Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Fighting Terror while Preserving Free Speech

by

Dr. Arthur J. Cockfield

of
Queen's University,
Faculty of Law

A discussion paper presented to the

Department of Justice Canada

The views expressed in this report are those of the author and do not necessarily represent the views of the Department of Justice

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Preface

This report was commissioned by the Department of Justice Canada as part of its ongoing efforts to canvas academic perspectives on targeted issues of anti-terrorism policy. An earlier draft was presented to Department of Justice Canada officials in Ottawa on March 17, 2009, and the author is grateful for the many helpful comments he received. The views expressed in this report are those of the author and do not necessarily represent the views of the Department of Justice Canada.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Executive Summary

This report explores the tension between efforts to counter violent extremism by regulating speech and efforts to preserve the right to freedom of expression. Certain countries such as the United Kingdom have adopted laws and policies that criminalize expressive activities that encourage, incite or glorify terrorism ('terrorist hate speech' laws). While Canada has legislated criminal laws and human rights laws that prohibit hate speech against members of identifiable groups, it has not yet adopted terrorist hate speech laws.

The analysis suggests that Canada's existing hate speech laws could be used to target, in certain circumstances, expression that encourages violent extremism against members of identifiable groups (for example, against Christians, Muslims or Jews). In addition, other criminal laws, including counseling and facilitating terrorist acts, could be used to investigate and prosecute certain expression that advocates the planning and execution of terrorist acts. Nevertheless, there are legislative gaps in Canada such as no prohibitions against speech that glorifies terrorism that could potentially be addressed through reform efforts.

Legislative and policy reforms that seek to develop terrorist hate speech laws must strive to protect against *Charter of Rights and Freedoms* violations, including possible infringements of the right to freedom of expression. To safeguard against possible *Charter* violations, any new terrorist hate speech laws should adopt some or all of the following elements:

(a) ensure there is a close connection between the expression and the risk of harm;
(b) ensure that the risk of harm is imminent;
(c) ensure that the restriction is the least intrusive and restrictive approach possible for protecting the public (by, for example, specifying speech that focuses on the planning and preparation of terrorist acts by specific individuals);
(d) ensure that the definition of terrorism does not capture lawful activities such as political dissent;
(e) avoid the usage of vague or overly-broad terms such as 'glorify' or 'encourage' by precisely defining these terms;
(f) adopt oversight mechanisms such as annual reporting to Parliament; and
(g) with respect to the usage of new investigatory or surveillance technologies, require technological systems of control and accountability as well as policies to govern information collection, use and exchange of a suspect's personal information.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

1. Introduction

This report explores the tension between potential efforts to counter violent extremism by regulating speech and efforts to preserve the right to freedom of expression. The analysis is directed at determining the merits and constitutional concerns surrounding possible new laws that would criminalize expression that encourages, incites, or glorifies terrorism ('terrorist hate speech').

Part 2 provides background by reviewing the first English legal efforts to deal with this tension as well as the ways that Canadian courts have tried to reconcile the tension surrounding the regulation of hate speech. The Part also reviews the similarities and differences between terrorist acts and 'ordinary' crimes to help discern whether expressive acts that encourage terrorism should be regulated in a different manner from ones that incite hatred against members of identifiable groups. Part 3 discusses whether Canada's existing hate speech laws can effectively counter terrorist activities, including potential reform efforts that could more directly prohibit speech that seeks to encourage, incite or glorify terrorism. This Part also reviews some of the free speech implications surrounding terrorist and government usage of new technologies. Part 4 overviews select developments in the United Kingdom and the United States to see how their governments are dealing with the tension between free speech and anti-terrorism laws, and relates these developments to recent survey views by Canadians on post-9/11 developments regarding national security and civil liberties. Part 5 concludes by noting some of the problematic aspects of terrorist hate speech laws in terms of their actual enforcement, and by summarizing the potential legal safeguards for freedom of expression should the government pursue reforms to link hate speech concepts to anti-terrorism laws.

2. Background: Exploring the Tension between Regulating Speech and Fighting Crime and Terrorism

In Canada, there is ongoing tension between efforts to criminalize hate speech while at the same time affording *Charter* protection to freedom of expression. This Part serves as background by examining this tension, and by teasing out the differences between 'ordinary' hate criminals and terrorists and forms of expression associated with both groups.

2.1. How the Tension was First Resolved by Law

The story of John Locke and the Glorious Revolution in 17th Century England highlights the historic tension between regulating speech and fighting criminals and terrorists. Locke's radical and illegal writings (under treason, sedition and heresy laws) helped foment the Glorious Revolution that led to the first laws in 1689 that protected free speech in a limited way, which lay the foundation to protect this freedom in Canada and elsewhere.

Locke is now considered one of the founders of the political philosophy of liberalism, which emphasizes democracy, individual rights, and a limited role for government. In the late 17th Century, he wrote in favor of social values that were contrary to the monarchical rule in England. The ruling monarchs and their supporters asserted that they were entitled to govern through

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

divine rule as the King and Queen were descendants of Adam and Eve and hence anointed by God (the so-called Divine Right of Kings). Locke claimed a political philosophy that defended monarchical absolutism was inappropriate in large part because God did not intend to place any man above another.[1]

As a result, Locke argued that the only legitimate (or moral) state was one where citizens would elect their rulers so that these rulers would follow the wishes of their constituents (especially with respect to the taxation and regulation of property).[2] In his view, a democratic state would best protect and promote an individual's 'natural right' to exercise individual autonomy, including the ability the express oneself without censorship from the state.

Before the Glorious Revolution, the freedom of speech in Parliament was generally unprotected with many individuals punished for statements that were not favorable to the king. In one famous case, the Speaker of the House of Commons was fined £10,000 for, in 1686, publishing writings against the King, which served to chill subsequent expression in Parliamentary debates.[3]

Locke's writings as well as those from other liberal theorists laid the foundation for the political view that individuals should have the right to freely express themselves without fear of state reprisal.[4] In particular, Locke and others argued that freedom of speech for these political debates was essential to promote the growth of democratic institutions. These views influenced other political actors and helped to foment the Glorious Revolution of 1688 where the authoritarian monarchy was overturned in favor of a bourgeois elite exercising its rights within a parliament.

The Glorious Revolution begat the English *Bill of Rights* of 1689, the earliest Western (formal) law to protect freedom of expression by providing: "That the freedom of speech and debates or proceedings in Parliament ought not to be impeached or questioned in any court or place out of Parliament."[5] Here we see the modern roots of the contemporary and far more expansive Canadian legal protections for freedom of expression.[6]

---

[1] Locke devotes an entire book to this topic as he argues against Filmer and the widely-held belief that the King was a descendant of Adam. See J. Locke, *Two Treatises of Government – Book I*, ed. M. Goldie (1996)(1690).

[2] See A.J. Cockfield, "Income Taxes and Individual Liberty: A Lockean Perspective on Radical Consumption Tax Reform," *South Dakota Law Review* 46 (2001): 8, 12-24.

[3] The Speaker of the House, Sir William Williams, was charged with seditious libel for publishing a pamphlet against James II before James had acceded to the throne. This charge proved influential in the subsequent drafting of the provision granting freedom of speech for Parliamentary debates in the English Bill of Rights. For discussion, see *Gravel v. United States,* 408 U.S. 606 (1972), n. 9.

[4] John Milton wrote a more influential defense of free expression in an essay called *Areopagitica* (1644) that argued against the English *Licensing Act*, which permitted the government to censor publications. After the Glorious Revolution, Parliament refused to renew the *Licensing Act* and it expired in 1695, which significantly curtailed government censorship of written expression.

[5] *An Act Declaring the Rights and Liberties of the Subject and Settling the Succession of the Crown, 1689* (U.K.), 1 William & Mary I, c. 2 s. 2 [the 'English Bill of Rights'].

[6] Earlier roots stretch back to the Ancient Persians where in 539 B.C. Cyrus the Great granted certain freedoms to exercise religious beliefs engraved on a cylinder that has been called the world's first declaration of human rights. See United Nations Press Release, *Statement by Secretary General U Thant at Presentation of Gift from Iran to United Nations* (Oct. 14, 1971).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To Locke and others this right to freedom of speech was a God-given right. While earlier political philosophers often brought religious interpretations into their views of natural rights, more recent philosophical attempts, including Rawlsian 'behind-the-veil' approaches, have reconstructed these views along secular lines to promote human rights, including the right to freedom of expression.[7]

2.2. Judicial Views on the Tension between Regulating Speech and Fighting Crime

As subsequently discussed, efforts to promote security and safety by regulating hate speech pose ongoing constitutional challenges.

Sections 318 and 319 make it a criminal offence to engage in certain forms of hate speech (or propaganda), namely: promoting genocide (s. 318); the incitement of hatred against an identifiable group when this incitement is likely to lead to a breach of the peace (s. 319(1)); and the willful promotion of hatred against an identifiable group (s. 319(2)).

While criminalizing hate speech, Canada also provides constitutional protection for freedom of expression via section 2(b) of the *Charter of Rights and Freedoms*: "Everyone has the following fundamental freedoms: …freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication." Freedom of expression is provided with *Charter* protection under the view that this right promotes the free flow of ideas that are essential within a liberal democracy such as Canada, protects against state abuse that would otherwise thwart or subvert other protected rights and freedoms.[8]

In other words, *Charter* protection for the right to freedom of expression acts as a kind of 'fence' against the exercise of arbitrary state power over expressive activities and so preserve fundamental freedoms for individuals. Consistent with Lockean views on the need to protect and promote individual autonomy, this right also permits individuals to freely express themselves and explore different aspects of their personalities for personal, religious or artistic reasons.

In *Keegstra*,[9] the first case to consider section 319(2)(the willful promotion of hatred provision), the majority of the Supreme Court of Canada (in a 4-3 split) recognized that the hate speech laws limit freedom of expression, but that this limit is reasonable and consistent with the values of a democratic society, and is hence constitutionally permissible. In particular, the majority accepted the Crown's argument that there is a rational connection between the hate speech laws and the objective or protecting target group members and of fostering harmonious social relations in a community dedicated to equality and multiculturalism.

Madame Justice (now Chief Justice) McLachlin dissented by indicating in part that section 319(2) did not effectively prevent the spread of hateful ideas and was overly intrusive into

---

[7] See, for example, C. Wellman, *An Approach to Rights: Studies in the Philosophy of Law and Morals* (Norwell, MA: Kluwer Academic Publishers, 1997), 15-16.

[8] For a discussion of the tension between freedom of expression and the regulations of hate speech, see, for example, R. Moon, *Report to the Canadian Human Rights Commission Concerning Section 13 of the Canadian Human Rights Act and the Regulation of Hate Speech on the Internet* (Oct. 2008), from http://www.chrc-ccdp.ca/pdf/moon_report_en.pdf (accessed February 27, 2009), 19-27.

[9] *R. v. Keegstra*, [1990] 3 S.C.R. 697.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

freedom of expression. In her view, it was unclear that section 319(2) provides an effective way to curb hate-mongers, and that the media coverage may even bring them sympathy. She noted that for the guarantee of free expression to be meaningful it must protect expression which challenges even the very basic conceptions about our society.

More recently, in *Mugesera* the Supreme Court narrowly construed section 319(2) so that the willful "promotion" of hate entails the active support or instigation and not mere encouragement. According to the Court, only the most intense forms of hate fall within the ambit of this offence although proof that the communication actually caused hatred was not required.[10]

Subsequent to the terrorist attacks of 9/11, the federal government implemented anti-terrorism reforms, including the *Anti-Terrorism Act* of 2001 (the 'Act') that promoted a number of different legislative amendments to a variety of federal statutes. With respect to anti-hate provisions, this Act amended the *Criminal Code* by adding section 430(4.1) to prohibit the defiling of a place of worship or an object associated with religious worship. The Act also added section 320.1 to allow courts to order the deletion of publicly available on-line hate propaganda from computer systems when it is stored on a server that is within the jurisdiction of the court (this new provision effectively tracks an older one that permitted courts to order the forfeiture of publications that constitute hate propaganda). In addition, the Act amended the *Canadian Human Rights Act* to clarify that computer communications, including the Internet, were included in the prohibited media to spread hate messages.

To safeguard against *Charter* rights violations the Act contained provisions, *inter alia*, that sought to exclude from the definition of 'terrorist activity' certain lawful activities such as "advocacy, protest, dissent or stoppage of work." In addition, the Department of Justice has ongoing efforts to study the impact of the Act and related legislation with a particular emphasis on the impact on ethno-cultural communities in Canada (including efforts such as the Cross-Cultural Roundtable on Security).

2.3. Similarities and Differences between 'Ordinary' Hate Crimes and Terrorism

The tension between regulating hate speech and fighting crime will persist with respect to any reform efforts that seek to criminalize expression that encourages, incites, or glorifies terrorism. There are both similarities and significant differences between traditional hate crimes (i.e., crimes that target individuals on the basis of their membership in identifiable groups, including hate speech crimes under sections 318 and 319 of the *Criminal Code*) and acts of terrorism (see also Sections 3.3. and 4.2).

There are essentially three views: (a) criminals and terrorists are the same and thus should be subjected to the same criminal law offences; (b) terrorists are different from criminals in that the former engages in violent acts that are motivated by political, religious, or ideological purposes; and (c) terrorists are different from ordinary criminals in that the former want to intimidate individuals or groups, other than the direct victims, to change their ways through their violent acts.

---

[10] See *Mugesera v. Canada (Minister of Citizenship and Immigration)*, 2005 SCC 40, [2005] 2 S.C.R. 100.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The first view maintains that there is no real difference between acts of terrorism and other violent crimes. In particular, home-grown terrorism in the West has been analogized with other violent youth movements.[11] Under this view, prior to the enactment of the Act terrorist activities were already covered by existing laws within the *Criminal Code*, including conspiracies and counseling the commission of various violent crimes, and hence no additional legislation was needed (see also Section 3.1).[12]

Perhaps the most cogent similarity between hate speech crimes and terrorist hate speech is that both forms of expression could potentially target members of identifiable groups such as members of religious groups. For instance, an individual could incite others to blow up a local mosque under the false view that Muslim Canadians are eroding Canadian democratic values.

In other words, hate crimes and terrorism are similar in that both acts are often directed not only toward an individual victim of a crime, but also toward similarly situated members of the victims' community: "[b]y inflicting harm on one victim, the perpetrators of these crimes often hope to intimidate those who are similarly situated to the victim. Both hate crime and terrorism are thus motivated in some way by an attempt to achieve socio-political ends outside of the legitimate political system."[13]

Under the second view, the terrorist has a political, religious or ideological agenda behind his or her actions. Studies of terrorists suggest these individuals actually believe they are accomplishing good deeds through their violent actions.[14] A terrorist, for instance, may want to target Canadians under the view that the Canadian government is inappropriately meddling in domestic political situations through actions such as the war in Afghanistan. Whether or not the belief is accurate is largely besides the point; the fact remains that such an individual holds an honest, if misguided, desire to promote political change through violent actions.

In contrast to hate criminals, terrorists may target broader groups such as individuals in countries associated with certain political values. Tim McVeigh, for example, bombed government buildings in Oklahoma as part of his political efforts to reduce the amount of government involvement in the lives of U.S. citizens. McVeigh and his associates did not respect traditional liberal democratic values that permit elected representatives to design laws and policies demanded by the majority of their constituents. Nor did he target an identifiable group, as would

---

[11] See Olivier Roy, Al Qaeda as a Youth Movement: The Power of a Narrative (MICROCON Working Paper 2, Brighton, United Kingdom).

[12] See D. Stuart, "The Dangers of Quick Fix Legislation in the Criminal Law: The Anti-Terrorism Bill C-36 Should be Withdrawn," in *The Security of Freedom: Essays on Canada's Anti-terrorism Bill*, ed. R. J. Daniels, P. Macklem and K. Roach (Toronto: University of Toronto Press, 2001), 205; K. Roach, "The Terrorism Offences and the Criminal Law," in *The Security of Freedom: Essays on Canada's Anti-terrorism Bill*, ed. R. J. Daniels, P. Macklem and K. Roach (Toronto: University of Toronto Press, 2001), 151.

[13] See E. Shimamoto, "Rethinking Hate Crime in the Age of Terror," *University of Missouri-Kansas City Law Review* 72 (2003-2004): 829, 838.

[14] See, for example, A. Chase, *A Mind for Murder: The Education of the Unabomber and the Origins of Modern Terrorism* (New York: Norton and Company, 2004); C. Reuter, *A Modern History of Suicide Bombing* (Princeton: Princeton University Press, 2004); R.A. Pape, "The Strategic Logic of Suicide Terrorism," *American Political Science Review* 97 (2003): 343-361. These studies typically recognize that political, religious, or ideological motives behind terrorist activities often serve to channel anti-social feelings into violent acts, and do not reflect concrete political agenda.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

have been necessary for his act to constitute a hate crime. Instead, he sought to further his political goals by striking symbolically. Rather than target individuals, McVeigh sought to change attitudes by attacking society as a whole. Such motivations are normally distinct from those underlying hate crimes.

As a result, the Act incorporates the need for political, religious, or ideological motivations as one of the necessary prerequisites for terrorism. Section 83.01(1)(b) of the Act defined "terrorist activity" in the *Criminal Code* to consist of three key elements: (i) an act or omission that intentionally causes one of the harms listed; (ii) a "political, religious or ideological purpose, objective or cause"; and (iii) "the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organisation to do or to refrain from doing any act." Similarly, a U.S. federal law defines terrorism as "premeditated, politically motivated violence perpetrated against noncombatants targets by subnational groups or clandestine agents."[15]

Under this second view, the inclusion of political, religious, or ideological motivations is necessary to accurately distinguish what is distinctively wrongful about terrorism when compared with other crimes.[16] The motive element is incorporated into terrorist offences because they are perceived to be more egregious when compared to ordinary crimes, including hate crimes: "The core premise is that political violence or violence done for some other public-oriented reason … is conceptually and morally different to violence perpetrated for private ends (such as profit, greed, jealousy, animosity, hatred, revenge, personal or family disputes and so on)."[17]

Because political, religious or ideological ideas are always in flux, the criminalizing of the espousing of these ideas is considered by many legal observers to be problematic. Some have challenged the need for motivations in this definition and, prior to passage, the law was modified to indicate "for greater certainty, the expression of a political, religious, or ideological thought, belief or opinion" will not constitute a terrorist activity unless the expression satisfies the other definition of terrorist activities.[18]

Despite this amendment, Justice Rutherford of the Ontario Superior Court in the *Khawaja* trial decision found that the motivation requirement in the Act was an unjustified violation of *Charter* rights to freedom of expression, association and religion.[19] In his view, the focus on political, religious, or ideological motives "will chill freedom protected speech … and therefore democratic life; and will promote fear and suspicion of targeted political or religious groups, and will result in racial or ethnic profiling."[20] Somewhat ironically, by striking down the motive requirement to protect the rights of the accused it will be easier to convict terrorists under the

---

[15] 22 U.S.C. § 2656f (d)(2) (2005) (outlining the role of foreign relations and intercourse).
[16] See S.A. Cohen, "Law in a Fearful Society: How Much Security?" *University of New Brunswick Law Journal* 54 (2005).
[17] See B. Saul, "The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient or Criminalising Thought? in A. Lynch et al., eds., *Law and Liberty in the War on Terror* (Federation Press, 2007), at 28, 29.
[18] See *Criminal Code*, R.S.C. 1985, c. C-46, s. 83.01(1.1).
[19] See *R. v. Khawaja* (2006), 214 C.C.C. (3d) 399 leave to appeal to S.C.C. denied [2006] S.C.C.A. No. 505..
[20] Id. at par. 73.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

two other branches of the test (i.e., the need for a wrongful act and the need for the intimidation of the public or the government).

In contrast, Justice Pattillo in the *Nadarajah* extradition application held that the inclusion of these motivations does not violate freedom of expression because terrorist acts are confined to acts of violence and s. 2 of the *Charter* does not protect expressive activities that constitute violence or threats of violence.[21] In his view, terrorist acts by their very nature are rooted in political, religious or ideological purposes or objectives.[22]

Under the third view, a distinguishing feature of terrorism is that its perpetrators target individuals with violence with the purpose of intimidating other individuals or governments so that they change their ways. As mentioned above, the definition of terrorism under the Act incorporates a requirement to intend to intimidate the public or compel a person or government to do or refrain from doing any act.

Certain judicial pronouncements in Canada have similarly not included a motive factor, but maintain the need for some form of political outcome that is intended or results from the terrorist act itself. For instance, the Supreme Court of Canada interpreted an undefined reference to terrorism in a Canadian immigration statute to be "acts intended to cause death or serious bodily injury to a civilian in order to intimidate a population or compel a government or an international organization to act."[23]

Yet without the political, religious or ideological motive element, intimidating acts could be motivated by purely private non-political goals. For instance, members of organized crime could extort payment from an individual or public official, which would constitute intimidation that would not be motivated by a political, religious or ideological purpose. For this reason, certain observers insist that motivation requirements are needed to recognize the distinct nature of terrorist acts.[24]

3. Linking Terrorism and Hate Speech Crimes

The Canadian federal government can potentially use existing criminal hate speech laws, human right laws or new terrorist hate speech laws to counter acts or potential acts of terrorism. This Part considers certain policy concerns for each possibility.

3.1. Using Existing Hate Speech Laws to Fight Terrorism

Some observers argue existing criminal law regime could be used to more effectively target violent extremists who wish to attack Canadians residing in Canada or elsewhere. For instance, Martin Rudner, an expert witness at the Air India hearing, suggested that hate speech criminal

---

[21] See *Attorney General (Canada) on Behalf of the U.S.A. v. Nadarajah*, Doc. No. CR-06-Ex32-00M0 (March 5, 2009), at pars. 29-30.
[22] Id. at par. 41.
[23] See *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1, [2002] 1 S.C.R. 3, at para. 98. The Supreme Court adopted the definition set out within the International Convention for the Suppression of the Financing of Terrorism.
[24] See Saul, supra note 17, at 30.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

laws should be used to prosecute terrorist propaganda and incitement.[25] In his view, the approach could have been deployed against Sikh extremists who had allegedly called for the murder of Hindus. According to his testimony, if authorities had intervened at an earlier point when these extremist elements were inciting and fomenting hatred it may have prevented the attack on Air India in 1985.

Hate crimes are more directly tailored to specific identifiable groups. Under sections 318 and 319 of the Criminal Code, "identifiable group" means "any section of the public distinguished by colour, race, religion, ethnic origin or sexual orientation." Accordingly, a suspect could presumably be investigated and charged under sections 319(1) or 319(2) for advocating or encouraging terrorist attacks against members of identifiable groups such as Christians, Jews or Muslims.

When the target of the hate speech is not a member of an identifiable group then reliance on the existing hate speech crime provisions may be less helpful. For example, terrorist hate speech generally directed at members of the Canadian public would not be captured by section 319. Finally, other criminal law provisions deal with threats of imminent violence against individuals or facilitating terrorist acts, and may be able to assist with prosecuting certain activities associated with terrorist hate speech.[26] In particular, the crime of counseling the commission of a terrorist act permits the police to investigate speech that advocates the preparation and planning of terrorist activities.

3.2. Human Rights Legislation

Section 13 of the *Canadian Human Rights Act* (CHRA) prohibits the communication of messages that are likely to expose a person to hatred or contempt on the basis of race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability or conviction for which a pardon has been granted. As a result, this section could potentially be used to investigate and counter acts of terrorist hate speech that targets members of the identifiable group. As with respect to the *Criminal Code* anti-hate speech laws, speech that more broadly targets Western values or members of the general public will not be covered by the CHRA.

Certain writings have focused on the problematic aspects of section 13 of CHRA. After noting that hate speech should only be banned if it explicitly or implicitly threatens, justifies or advocates violence against members of an identifiable group, Richard Moon suggests the current approach "does not fit easily or simply into a human rights law that takes an expansive view of discrimination and seeks to advance the goal of social equality through education and conciliation."[27] His principal recommendation was to repeal section 13. Other problematic aspects of section 13 surround the fact that defences to the charges do not include: truth; fair

---

[25] See K. Bolan, "Use hate laws against those who promote terrorism, inquiry hears," *National Post* (Dec. 10, 2007), from http://www.nationalpost.com/news/canada/mulroney/story.html?id=158814 (accessed February 28, 2009).
[26] See, for example, *Anti-terrorism Act*, S.C. 2001, c. 41, s. 83.19.
[27] R. Moon, *Report to the Canadian Human Rights Commission Concerning Sectoin 13 of the Canadian Human Rights Act and the Regulation of Hate Speech on the Internet* (Oct. 2008), at 31.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

comment on true facts; publication in the public interest; innocent intent or good faith expression; or that the expression followed accepted journalism practices.

Because allegations of hate speech can have a devastating impact on the reputation of the accused along with the potential for quasi-criminal sanctions, terrorist hate speech investigations and prosecutions should only occur under federal criminal proceedings where the accused can engage the full protection of the justice system. It would be arguably inappropriate for the government to support efforts by complainants to pursue terrorists or incitements of terrorism through the CHRA.

Importantly, certain other federal laws, including the *Broadcasting Act* and the *Immigration Act*, have provisions that deal with hate speech. A discussion of the impact of these provisions is beyond the scope of this report.

3.3. The Potential for New Terrorist Hate Speech Laws

As discussed, the Canadian criminal law regime currently does not specifically prohibit expressive activities that encourage, incite or glorify terrorism.

In 2005, the United Nations Security Council issued a Resolution, sponsored by the United Kingdom, that called upon states to take steps to prevent incitement to commit terrorist acts (see also Section 4.2.). The Resolution declared that governments "have obligations under international law to counter incitement of terrorist acts motivated by extremism and intolerance and to prevent the subversion of educational, cultural and religious institutions by terrorists and their supporters."[28]

A major challenge for laws that seek to criminalize terrorist speech is that they may unduly interfere with freedom of expression rights guaranteed by section 2(b) of the *Charter*.[29] In particular, because courts have generally recognized that the *Charter* affords greater protection over political and religious expression, any new laws that seek to increase police powers over terrorist hate speech will need to safeguard against potential violations. Accordingly, courts would closely scrutinize any such reforms to see whether they unduly intrude on freedom of expression and cannot be justified under *Oakes* proportionality analysis as a reasonable limit in a free and democratic society under section 1 of the *Charter* (see also Section 5.2).

Under the *Oakes* proportionality test: the means must be rationally connected to the objective; there must be minimal impairment of rights; and there must be proportionality between the infringement and objective.

Under the rational connection element of the *Oakes* test, the means used must be carefully designed to achieve the objective, and they must not be arbitrary, unfair or based on irrational

---

[28] *Threats to International Peace and Security (Security Council Summit 2005)*, SC Res. 1624, UN SCOR, 60th Sess., U.N. Doc. S/RES/1624 (2005).

[29] For background on the freedom of expression implications of hate speech laws, see, for example, R. Moon, *The Constitutional Protection of Freedom of Expression* (Toronto: University of Toronto Press, 2000), 126-148.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

considerations. Yet there does not appear be any significant social science evidence that hate speech leads to greater amount of hate crimes:

> "[W]e have here no aggregative studies looking for correlations between the availability of hate literature and the incidence of hate crimes, no retrospective studies attempting to determine whether perpetrators of hate violence have a history of differential consumption of such literature, no laboratory studies designed to determine whether exposure to hateful materials increases the likelihood of negative attitudes toward, or aggression against, members of the target groups, and no formal hearings with witnesses testifying about injuries which were incited or motivated by hate messages."[30]

Similarly, there appear to be no empirical studies that link terrorist hate speech to acts of terrorism, which calls into question the 'rational connection' between efforts to link hate speech concepts to acts of terrorism. While courts do not require empirical evidence to determine whether *Charter* violations have taken place, a lack of current social science evidence that terrorist hate speech harms important security interests in Canada weakens the case for limiting free expression through reform efforts that regulate this form of speech.[31]

Under the minimal impairment element of the *Oakes* test, courts ask whether the legislative means to achieve the objective impair the *Charter* protected right in question as minimally as reasonably possible, and whether there are alternative modes of promoting Parliament's objective that infringe the right to a lesser extent.

An area of concern would be that new terrorist hate speech laws could be been used to target individuals who may hold the same or similar views as terrorist groups, but who do not endorse the violent means to secure the desired outcomes of these groups. If the laws are overbroad or unduly vague, they could constrain various expressive activities that could be construed as encouraging, inciting or, in particular, glorifying terrorism so that others will emulate terrorists (see Section 4.2.). Consider the following hypothetical examples of the ways that lawful activities could potentially become ensnared in new terrorist hate speech laws:

(a) a Canadian resident circulates via email a link to a YouTube video of a foreign individual praising Hamas terrorists;

(b) an activist engages in an online chat room discussion criticizing Canadian government foreign policy and supporting those who resist this policy;

(c) a person shows at a public assembly a video of Osama Bin Laden praising suicide bombers;

(d) a researcher publishes a report on terrorism for a non-governmental organization that advocates the need for developed countries to redress historic inequities with developing countries, and that justifies violent retaliation if these inequities are not dealt with;

---

[30] See L.W. Sumner, *The Hateful and the Obscene: Studies in the Limits of Free Expression* (Toronto: University of Toronto Press, 2004), 158-159, 193.

[31] Id. at 203 (arguing that when no reliable evidence has been presented that certain expressions can significantly impair important interests then the case for limiting freedom of expression has not been demonstrated).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(e) a professor gives a public talk on pro-Palestinian policy and the need to financially support refugee organizations to resist human rights violations by violent means if needed;
(f) a religious figure argues that his religion historically taught that violence is a needed to resist the ways of non-believers; or
(g) a restaurant owner posts a picture of a convicted IRA terrorist, and toasts the terrorist every evening.

In fact, previous foreign government attempts to regulate certain forms of speech as part of anti-terrorism efforts have led to the partial or total restriction on freedom of opinion and expression, abuse of powers under such laws that have led to prolonged and short-term arbitrary detention, the closure of various media enterprises and the censorship of publications, and the banning and prohibition of organizations and groups that are not associated with terrorism.[32]

A major challenge for any Canadian reform efforts in this area arise from the fact that terrorist hate speech often emphasizes political, religious or ideological concepts, at least when compared to traditional forms of hate speech directed at members of identifiable groups (see Section 2.3. as well as the discussion of the *Khawaja* case).[33] Kent Roach discusses drawbacks with respect to Canadian reform efforts to criminalize expression with political, religious or ideological components, including the approach could inhibit intercultural dialogue, in particular if group members have been unfairly stigmatized as supporting terrorism in the past, and the approach could be counterproductive if it confirms or broadens the false perception that the war against terrorism is really a war against Islam.[34]

To guard against these constitutional violations, new laws could only seek to prohibit expressive activities that encourage the intimidation of a population or government through violent means (under the third view of the nature of terrorism set out in Section 2.3) without referring to political, religious, or ideological motives. Nevertheless, concerns may remain that the underlying reasons to intimidate a population or government spring from political, religious or ideological purposes hence implicating forms of speech that have traditionally attracted constitutional protection.

The third step under the *Oakes* test asks whether the objective is proportional to the effect of the law, including whether the benefit to be derived from the legislation outweighs the seriousness of the infringement.

Expressive activities that merely 'encourage' or 'glorify' terrorism may be characterized by a court as too passive to attract constitutional protection under the *Oakes* test because the possible harm to innocent individuals is too remote or indirect (unlike expressions of extreme hate that

---

[32] See, for example, Report of the Special Rapporteur, Inter-American Commission on Human Rights, E/CN/4/2005/64 (Dec. 17, 2004). For a discussion of censorious outcomes in Canada as a result of hate speech regulations, see S. Braun, *Democracy Off Balance: Freedom of Expression and Hate Propaganda Law in Canada* (Toronto: University of Toronto Press, 2004), 256-258.
[33] In *Keegstra*, supra note 9, the Supreme Court discussed how pre-*Charter* jurisprudence emphasized freedom of expression primarily in relation to political expression.
[34] See K. Roach, "Must We Trade Rights for Security? The Choice between Smart, Harsh, or Proportionate Security Strategies in Canada and Britain," *Cardozo Law Review 27* (2005-2006): 2183-2184.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

are willfully promoted to harm members of identifiable groups[35]). A narrowly tailored terrorist hate speech law that focused on expressive activities tied to the planning and commission of terrorist acts by specific individuals could address these constitutional concerns. In other words, reform efforts should only seek to ban expression that could be objectively interpreted to intend to directly cause a present or future harm.

3.4. A Note on Legal and Policy Challenges from New Technologies

As discussed elsewhere, recent technological change raise security concerns as well as concerns surrounding the erosion of individual rights such as the right to freedom of expression.[36]

On the one hand, calls for greater police powers over terrorist suspects can be traced to public fears surrounding weapons of mass destruction such as 'dirty' bombs, transportable nuclear bombs, or chemical poisoning of water sources. These technologies may permit terrorist to conduct devastating attacks that could lead to even greater fatality levels than the ones witnessed on September 11, 2001.

In addition, the Internet has facilitated the spread of hate propaganda through web sites, password-protected or public chat rooms and other online fora that can also serve as terrorist recruitment tools. To address this challenge, recent *Criminal Code* provisions seek to ensure that courts can order the deletion of online hate propaganda while a new CHRA provision prohibits online communications that spread hate messages (see Section 2.2.). Because of the global and decentralized nature of the Internet, it remains unclear whether governments can effectively enforce these sorts of provisions—web sites can be hosted on servers located anywhere in the world and, if necessary, transferred to other servers at the push of a computer button.

On the other hand, recent technological innovations can have a potentially significant impact on police investigatory practices along with the risk that important interests, including the right to free freedom of expression, may be inhibited. By way of a current example, new laws could force Internet Service Providers (ISPs) to maintain data records of all Internet communications then use a software filter to discern whether these communications may be encouraging terrorism (by, for instance, focusing on keywords such as 'Al Qaeda').

With respect to state efforts to monitor ISP or other online communications, information technological developments make it less costly and more efficient to gather personal information about suspects. First, information technologies facilitate the collection, use and disclosure of personal information that has been rendered into digital format (e.g., chat room emails). This personal information is often collected by the private sector then accessed by state agents.

---

[35] In *Keegstra*, supra note 9, Dickson, C.J., noted that the need for a 'wilful' promotion imposes a "stringent *mens rea* requirement, necessitating either an intent to promote hatred or knowledge of the substantial certainty of such" and that "[i]n "promotes" we thus have a word that indicates more than simple encouragement or advancement. The hate-monger must intend or foresee as substantially certain a direct and active stimulation of hatred against an identifiable group." See also *Mugesera*, supra note 10 (holding that promotion entails active support and instigation).

[36] See, for example, A. J. Cockfield and L. M. Austin, "Introduction: Overview of Technological Challenges to Privacy and Security," in *Technology, Privacy and Justice,* ed. L. Austin, A. J. Cockfield, and P. Molinari, (Montreal: Canadian Institute for the Administration of Justice, 2007), 1.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Second, these technologies facilitate the aggregation of personal information: digital personal information can be cross-indexed against different government databases (customs, tax, criminal records, social services, health records and so on) to provide a comprehensive profile of an individual's activities. Third, technological developments permit the state to gather information about suspects in a more surreptitious manner (e.g., a police officer can remotely monitor ISP records).

If Canadians believe their emails and web site visits could be monitored then they may be reluctant to freely express themselves, including engaging in peaceful political protest such as criticizing their government's military actions in foreign lands. Political dissent or other forms of expression may also be inhibited to the extent that the state maintains detailed records of its citizens.

A law and technology theoretical perspective informs the view that, for state searches to be constitutionally permissible and reasonable under section 8 of the *Charter*, police and intelligence agencies must develop reasonable policies and practices to govern the collection, use and transfer of a suspect's personal information.[37] This view is supported by the Supreme Court's decision in *Tessling* where the Court asked, as part of a test to determine the constitutional permissibility of a police search, "[w]as the use of the surveillance technology itself objectively reasonable?"[38]

Accordingly, with respect to monitoring ISP records or other online communications detailed regulations should govern the government's information collection practices, including how long records must be maintained by ISPs. New laws could also mandate the logging of all government database searches to create digital audit trails, which could serve to inhibit state abuses.

4. A Comparative Perspective on Hate Speech Crimes and Terrorism

By way of background, comparative legal analysis suggests that Canada was less aggressive with respect to deploying new anti-terrorism laws when compared to certain other countries such as the United States and the United Kingdom.[39] The reason for this may simply result from the practical reality that these two countries have been attacked by terrorists in recent years while Canada has so far emerged relatively unscathed (while recognizing that tragedies such as the Air India bombing have nevertheless had a devastating impact on many Canadian families). This Part briefly overviews a few U.S. and U.K. legal and policy struggles with respect to the tension between protecting freedom of expression and anti-terrorism initiatives. It also reviews recent relevant results from an international survey on Canadian and foreign attitudes concerning security initiatives and their implications for civil liberties.

---

[37] See A. J. Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies," *University of British Columbia Law Review* 40 (2007): 41-67; A. J. Cockfield, "Towards a Law and Technology Theory," *Manitoba Law Journal* 30 (2004): 383-415.

[38] See *R. v. Tessling*, 2004 SCC 67, at par. 56. Ibid., at 64-66.

[39] See, e.g., A. J. Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance," *Queen's Law Journal* 29 (2003): 364.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

4.1. United States

The United States is sometimes portrayed as a country that affords strong legal protection for freedom of expression. For instance, U.S. hate speech laws have normally been found to be constitutionally impermissible as they unduly intrude on the First Amendment of the U.S. Constitution that reads in part: "Congress shall make no law … abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." U.S. Supreme Court Justice Oliver Wendell Holmes Jr. suggested in his famed dissent in *Abrams v. United States*[40] that the First Amendment should be interpreted expansively to protect virtually every form of speech: "The best test of truth is the power of thought to get itself accepted in the competition of the market … I think that we should be eternally vigilant against attempts to check the expression of opinions that we loathe and believe to be fraught with death."

John Stuart Mill provided an earlier philosophical defence of this 'marketplace of ideas' concept: "But the peculiar evil of silencing the expression of an opinion is, that it is robbing the human race; posterity as well as the existing generation; those who dissent from the opinion, still more than those who hold it. If the opinion is right, they are deprived of the opportunity of exchanging error for truth: if wrong, they lose, what is almost as great a benefit, the clearer perception and livelier impression of truth, produced by its collision with error."[41]

Under this view, the most effective way to counter irrational hatred against identifiable groups (and hence to promote long term equality) is to try to refute the hate speech by showing the lack of critical or reasoned thinking behind these communications. Through this dialogue, it is hoped that greater insight will be derived concerning prejudiced thinking so that more enlightened (and accurate) perspectives will win out at the end of the day. In addition, the U.S. government may be in a better position to promote safety and security by tracking and countering violent extremism because hate speech laws do not force extremists to engage in covert forms of propaganda that are hard or impossible to detect.

Nevertheless, like all other legal systems the commitment to freedom of expression is not absolute. Most relevant for present purposes is the 'true threat' exception that permits a state to ban certain types of threatening speech (for example, laws that ban symbolic forms of speech such as cross burning). An observer notes that:

> A 'true threat' is defined as a statement where the speaker communicates a serious expression of his of her intent to commit a violent, unlawful act against a particular person or group of persons. Thus, the speech is unprotected if an objectively reasonable person would interpret the speech as a serious expression of an intent to cause a present or future harm. The … factors used to guide a court's decision on whether the contested speech falls within the true threats exception are the context in which the statement was made, the statement itself,

---

[40] *Abrams v. United States*, 250 U.S. 616 (1919).
[41] John Stuart Mill, *On Liberty* (1859)(J.M. Dent & Sons Ltd., 1987), at 85.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> and the reaction of listeners. [However,] mere advocacy of the use of force or violence is outside the realm of the true threat exception.[42]

As a very general proposition, U.S. constitutional protections provide broader protection for freedom of expression when compared with section 2(b) protection under *Charter* jurisprudence. As sometimes noted, this could be explained in part by the fact that First Amendment is not subject to a savings clause such as the one under the *Charter* that led to the development of *Oakes* proportionality analysis.[43]

Despite this apparent broad constitutional protection for freedom of expression, critics suggest that U.S. anti-terrorism policy inhibits free speech through legislation such as the *Patriot Act* that permits the seizure of personal information without traditional due process protections and government policies that include blacklists of academics, rendition of terrorist suspects to countries with humans right violations and expansive no-fly lists that inhibit political dissent.[44]

4.2. United Kingdom

Unlike Canada, the United Kingdom does not provide for constitutional protections for freedom of expression although expression is protected under a number of U.K. statutes. In the past, the United Kingdom used specifically-tailored criminal laws to fight terrorist activities in Northern Ireland. The United Kingdom more recently reformed certain criminal laws so that they would be more effective at disrupting terrorist networks (see also Section 3.3).

In 2006, the U.K. government introduced legislation to create several new offences, including the "direct or indirect encouragement or other inducement" of terrorism.[45] In addition, this legislation prohibits the "glorification" of terrorism if "members of the public could reasonably be expected to infer that what is being glorified is conduct that should be emulated by them in existing circumstances." The legislation indicates that it is irrelevant "whether any person is in fact enouraged or induced by the statement to commit, prepare or instigate" any terrorist acts.

A number of scholars and policy-makers have challenged the efficacy of certain U.K. anti-terrorism laws and practices, including the recent reforms. In a February 2009 report issued by the House of Lords, it was indicated that recent surveillance laws and practices create the risk that fundamental freedoms such as the right to privacy and the right to free speech will be undermined.[46] In particular, the report examined the potential misuse of new police powers by

---

[42] See Nina Petraro, "Harmful Speech and True Threats: *Virginia v. Black* and the First Amendment in an Age of Terrorism," *St. John's Journal of Legal Commentary* 20 (2006): 532, 546, 547.

[43] In *Keegstra*, supra note 9, the Supreme Court extensively reviewed U.S. jurisprudence with respect to free speech issues.

[44] See, e.g., International Commission of Jurists, *Assessing Damage, Urging Action, Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights* (Switzerland: International Commission of Jurists, 2009), 127-133.

[45] See *Terrorism Act 2006* (U.K.), 2006, c. 11.

[46] See House of Lords, Constitution Committee, *Surveillance: Citizens and the State* (2009). See also T. Hammarberg, Commissioner for Human Rights, *Protecting the Right to Privacy in the Fight against Terrorism*, CommDH/IssuePaper(2008)3, at 15 (asserting that anti-terrorism measures must not interfere with fundamental rights articulated by the European Convention on Human Rights).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

local authorities to deploy surveillance measures against activities outside of the scope of the initially intended criminal and/or terrorist activities. As a result, the report proposes a number of recommendations to promote state accountability and to ensure that new police powers are effectively regulated.

Advocacy groups have mounted a more direct challenge to U.K. anti-terrorism laws that have implications for the right to freedom expression guaranteed under European human rights laws. Under one view, the U.K. laws, including the recently-introduced offences of encouraging and glorifying terrorism "criminalise the legitimate exercise of freedom expression and have a real chilling effect on debate on matters of public interest" in part because the broad definition of terrorism captures many previously-lawful activities.[47]

Others suggest that the political, social, and other realities within the United Kingdom today justify attempts to link hate speech concepts to anti-terrorism policy. This country has been subjected historically and more recently (by Islamist radicals) to multiple devastating terrorist attacks. In addition, ongoing cases of terrorist hate speech in U.K. public spaces has been well-documented for over two decades, often resulting in the silencing and intimidation of individuals with opposing perspectives.[48]

4.3. Citizen Views in Canada on Post-9/11 Security Laws

Under one view, regulations of hate speech, including terrorist hate speech, should account for: (a) a country's history with ethnic, racial or religious violence and discriminatory practices; and (b) its jurisprudential history, including the hierarchy of its constitutional value choices.[49] While U.S. and U.K. developments may be relevant, Canadian historical and political developments as well as Charter jurisprudence must ultimately dictate the appropriate Canadian legal response with respect to regulating speech to counter violent extremism.

The views of Canadians also form an important consideration when contemplating reform to existing laws dealing with hate speech. In 2006 and 2007, the Surveillance Project, an inter-disciplinary research team at Queen's University, completed a survey of views of Canadians and the citizens of nine other countries (the United States, Mexico, Brazil, China, Japan, France, Hungary and Spain).[50] This survey was the first cross-national study to scrutinize attitudes and experiences with global flows of personal data, with a special focus on privacy and surveillance in the post-9/11 environment. In total, over 9,500 respondents were surveyed to help understand their views on these topics. While the survey questions did not directly address issues surrounding hate speech laws or freedom of expression, certain survey results are relevant as

---

[47] See Article 19, *The Impact of UK Anti-Terror Laws on Freedom of Expression, Submission to ICJ Panel of Eminent Jurists on Terrorism, Counter-Terrorism and Human Rights* (2006), from www.article19.org/pdfs/analysis/terrorism-submission-to-icj-panel.pdf (accessed February 28, 2009).

[48] See Ed Husain, *The Islamist* (Penguin Books, 2007)(providing a first-hand account of how U.K. teenagers can be drawn into the narrative of terrorism).

[49] See John C. Knechtle, "When to Regulate Hate Speech", *Penn St. L. Rev.* 110 (2005-2006): 539-578, 543.

[50] See The Surveillance Project, *The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance, Summary of Findings* (2008), from http://www.surveillanceproject.org/files/2008_Surveillance_Project_International_Survey_Findings_Summary.pdf (accessed February 28, 2009).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

they focused on understanding Canadian attitudes toward post-9/11 security and surveillance laws.

The survey results indicated that a majority (52%) of the Canadian respondents did not trust that their government had struck the right balance between security and individual rights when it comes to the privacy of personal information.[51] These results are comparable to certain countries such as the United States where 61.5% did not trust their government and France where 70.1% did not trust their government. In a related question, 47.7% of Canadians indicate that Canadian laws aimed at protecting national security are intrusive upon personal privacy, compared with 57.3% of Americans and 40.3% of French respondents.[52] Another survey question asked whether Canadians had ever had their personal information monitored by the federal government. 20.8% of Canadian respondents indicated that they had been monitored by the federal government compared with 22.3% in the United States and 7% in France.[53]

These survey results show that a significant portion of Canadians are worried that the government has not struck the right balance between security and the preservation of important liberties. Moreover, because Canada has a different historic experience with terrorism and has not (with the exception of the Air India and FLQ attacks) suffered significant terrorist attacks from home-grown or foreign terrorists, it calls into question the need for the Canadian government to pursue terrorist hate speech laws adopted by the United Kingdom and other countries. Finally, *Charter* protection for freedom of expression may signal a Canadian constitutional commitment to guarding against state scrutiny of speech with political, religious, or ideological aspects unless this speech is directly tied to threats of violence.

5. Canadian Anti-Terrorism/Hate Speech Laws and the Shadow of the Law

This final Part discusses policy concerns that new terrorist hate speech laws could upset the traditional balance between fighting crime and preserving free speech, potentially harming national security in the long run. It begins by reviewing the symbolic impact of anti-terrorism laws including, potentially, terrorist hate speech laws and the actual enforcement by the police or intelligence agencies of these laws, and concludes with a review of the safeguards that should be considered if the Canadian government tries to link anti-terrorism laws with hate speech concepts.

5.1. Symbolic Impact and Enforcement of Anti-Terrorism Laws

Legal and policy reform efforts should be guided in part by the ways that the law will likely be operationalized by state agents, including the possibility for rights violations. Have Canadian legislative efforts, including the *Anti-terrorism Act* (the 'Act'), significantly changed police or other government practices? In 2004, I conducted a survey of empirical research and

---

[51] Ibid., 13.
[52] Ibid., 26.
[53] Ibid., 17.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

government internal reports assessed government enforcement efforts with respect to the Act.[54] In roughly the two years following the 9/11 attacks, the preventative arrests and investigative hearings had not been used, the number of authorizations for interceptions of private communications had not increased, the amount of individuals detained for immigration-related offences had not gone up, and the number of complaints under the *Privacy Act* (which governs federal government personal information collection practices) had not appreciably risen.

There were anecdotal reports that expanded investigatory powers were used to conduct racial and religious profiling of Muslim Canadians.[55] Some of the stories involve fears that the police used their new powers to 'shake down' members of the targeted community by threatening to use these new powers (including the sunsetted preventative arrest provisions that have been recently re-introduced by Parliament) to coerce individuals within the community to cooperate with state agents. Ultimately, it was too soon to properly evaluate state practices due to the complex and ongoing legal and technological changes that followed the terrorist attacks of 9/11.

Whether or not more aggressive anti-terrorism laws, along with more aggressive enforcement of these laws, will make us more secure in the long run is a question that is much debated. Current social scientific research does not appear to offer definitive conclusions. A more conservative perspective would suggest that it is unwise to inhibit, on unproven assumptions, fundamental freedoms such as freedom of expression that have traditionally promoted a vibrant and secure democracy.

In particular, new laws to target terrorist hate speech carry important symbolic aspects. Individuals within identifiable groups may query whether the laws were designed to target individuals within the group. A climate of distrust may develop between the government and the group that feels it is being improperly scrutinized or investigated (as there may be no evidence of individual wrong-doing by the targeted group members).[56]

This distrust may make Canada less secure, at least in the long run, as members of the targeted community become more reluctant to assist government agents with their investigations. As Justice O'Connor noted in the Arar Commission, "[P]erceptions of unfair treatment, whether founded or not, can have a serious impact on the level of co-operation members of the communities give investigators."[57]

---

[54] See A. J. Cockfield, "The State of Privacy laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government," *University of Ottawa Law and Technology Journal* 1 (2004): 325-344.

[55] Ibid., 340-341. See also Maureen Webb, *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World* (San Francisco: City Lights, 2007), 9-45; Canadian Council on American-Islamic Relations, *Presumption of Guilt: A National Survey on Security Visitations of Canadian Muslims* (2005)(discussing racial profiling of young Arab males by state agents).

[56] Cockfield, Social Value of Privacy, supra note 37, at 52-53.

[57] Commission of Enquiry, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Works and Government Services Canada, 2006), at 357.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

In addition, criminalizing speech that has political, religious or ideological aspects may help to fuel terrorism by supporting the narrative—real or imagined—by alienated youth that they are being unfairly targeted and are hence 'heroes' that are defending the oppressed.[58]

A more effective anti-terrorism strategy could involve a multi-pronged approach that seeks to oppose the narrative of terrorism by countering radical extremist ideology, and empowering mainstream religious voices.[59]

5.2. Summary: Legal Safeguards for Free Speech

The tension that exists between efforts to regulate hate speech and efforts to preserve freedom of expression will persist with respect to reforms that seek to link hate speech concepts with efforts to counter violent extremism that threatens security. Current hate speech laws, as well as other criminal and anti-terrorism laws, arguably suffice to deal with potential expressive acts that could lead to terrorist acts. Due to *Charter* protection for the right to free speech, reform efforts that seek to criminalize expression that encourages, incites or glorifies terrorism ('terrorist hate speech') should seek to only ban expression that could be objectively interpreted to intend to directly cause a present or future harm, and should avoid prohibiting the passive encouragement or glorification of terrorism that could indirectly lead to violence.

In addition, to protect political, religious or ideological expressive activities, reform efforts that seek to criminalize terrorist hate speech should consider the adoption of some or all of the following safeguards:

(a) ensure there is a close connection between the expression and the risk of harm;
(b) ensure that the risk of harm is imminent;
(c) ensure that the restriction is the least intrusive and restrictive approach possible for protecting the public (by, for example, specifying speech that focuses on the planning and preparation of terrorist acts by specific individuals);
(d) ensure that the definition of terrorism does not capture lawful activities such as political dissent;
(e) avoid the usage of vague or overly-broad undefined terms such as 'glorify' or 'encourage';
(f) adopt oversight mechanisms such as annual reporting to Parliament; and
(g) with respect to the usage of new investigatory or surveillance technologies, require technological systems of control and accountability as well as policies to govern information collection, use and exchange of a suspect's personal information.

---

[58] See Roy, supra note 11, at 21-22.
[59] See Washington Institute for Near East Policy, Presidential Task Force, *Rewriting the Narrative: An Integrated Strategy for Counterradicalization* (Washington, D.C., March 2009).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Bibliography

Article 19. *The Impact of UK Anti-Terror Laws on Freedom of Expression, Submission to ICJ Panel of Eminent Jurists on Terrorism, Counter-Terrorism and Human Rights* (2006). Accessed February 28, 2009, from www.article19.org/pdfs/analysis/terrorism-submission-to-icj-panel.pdf.

Bolan, K. "Use hate laws against those who promote terrorism, inquiry hears," *National Post* (Dec. 10, 2007). Accessed February 28, 2009, from http://www.nationalpost.com/news/canada/mulroney/story.html?id=158814.

Braun, S. *Democracy Off Balance: Freedom of Expression and Hate Propaganda Law in Canada*. Toronto: University of Toronto Press, 2004.

Chase, A. *A Mind for Murder: The Education of the Unabomber and the Origins of Modern Terrorism*. New York: Norton and Company, 2004.

Cockfield, A.J. "Income Taxes and Individual Liberty: A Lockean Perspective on Radical Consumption Tax Reform." *South Dakota Law Review* 46 (2001): 8.

Cockfield, A.J. "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies." *University of British Columbia Law Review* 40 (2007): 41.

Cockfield, A.J. "The State of Privacy laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government." *University of Ottawa Law and Technology Journal* 1 (2004): 325.

Cockfield, A.J. "Towards a Law and Technology Theory." *Manitoba Law Journal* 30 (2004): 383.

Cockfield, A.J. "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance." *Queen's Law Journal* 29 (2003): 364.

Cockfield, A.J. and L.M. Austin. "Introduction: Overview of Technological Challenges to Privacy and Security." In *Technology, Privacy and Justice,* edited by L. Austin, A.J. Cockfield and P. Molinari, 1. Montreal: Canadian Institute for the Administration of Justice, 2007.

Cohen, S.A. "Law in a Fearful Society: How Much Security?" *University of New Brunswick Law Journal* 54 (2005): 143.

Hammarberg, T. *Protecting the Right to Privacy in the Fight against Terrorism*, (Commissioner for Human Rights) CommDH/IssuePaper(2008)3.

House of Lords, Constitution Committee, *Surveillance: Citizens and the State* (2009).

Husain E. *The Islamist: Why I Joined Radical Islam in Britain, What I Saw Inside and Why I Left.* Toronto: Penguin Books, 2007.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

International Commission of Jurists. *Assessing Damage, Urging Action, Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights.* Switzerland: International Commission of Jurists, 2009.

Knechtle, J.C. "When to Regulate Hate Speech." *Penn State Law Review* 110 (2005-2006): 539.

Locke, J. *Two Treatises of Government – Book I*, edited by M. Goldie (1996).

Mill, J.S. *On Liberty.* New York: Norton, 1975.

Moon, R. *The Constitutional Protection of Freedom of Expression.* Toronto: University of Toronto Press, 2000.

Moon, R. *Report to the Canadian Human Rights Commission Concerning Section 13 of the Canadian Human Rights Act and the Regulation of Hate Speech on the Internet* (Oct. 2008). Accessed February 27, 2009, from http://www.chrc-ccdp.ca/pdf/moon_report_en.pdf.

Pape, R.A. "The Strategic Logic of Suicide Terrorism." *American Political Science Review* 97 (2003): 343.

Petraro, N. "Harmful Speech and True Threats: *Virginia v. Black* and the First Amendment in an Age of Terrorism." *St. John's Journal of Legal Commentary* 20 (2006): 531.

Report of the Special Rapporteur, Inter-American Commission on Human Rights, E/CN/4/2005/64 (Dec. 17, 2004).

Reuter, C. *A Modern History of Suicide Bombing*. Princeton: Princeton University Press, 2004.

Roach, K. "Must We Trade Rights for Security? The Choice between Smart, Harsh, or Proportionate Security Strategies in Canada and Britain." *Cardozo Law Review 27* (2005-2006): 2151.

Roach, K. "The Terrorism Offences and the Criminal Law." In *The Security of Freedom: Essays on Canada's Anti-terrorism Bill*, edited by R. J. Daniels, P. Macklem and K. Roach, 151. Toronto: University of Toronto Press, 2001.

Roy, O. "Al Qaeda as a Youth Movement: The Power of a Narrative" (MICROCON Working Paper 2, Brighton, United Kingdom).

Shimamoto, E. "Rethinking Hate Crime in the Age of Terror." *University of Missouri-Kansas City Law Review* 72 (2003-2004): 829.

Stuart, D. "The Dangers of Quick Fix Legislation in the Criminal Law: The Anti-Terrorism Bill C-36 Should be Withdrawn." In *The Security of Freedom: Essays on Canada's Anti-terrorism*

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Bill, edited by R. J. Daniels, P. Macklem and K. Roach, 205. Toronto: University of Toronto Press, 2001.

Sumner, L.W. *The Hateful and the Obscene: Studies in the Limits of Free Expression.* Toronto: University of Toronto Press, 2004.

The Surveillance Project. *The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance, Summary of Findings* (2008). Accessed February 28, 2009, from http://www.surveillanceproject.org/files/
2008_Surveillance_Project_International_Survey_Findings_Summary.pdf.

Thant, U. United Nations Press Release, Statement by Secretary General U Thant, at Presentation of Gift from Iran to United Nations (Oct. 14, 1971).

Webb, M. *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World.* San Francisco: City Lights, 2007.

Wellman, C. *An Approach to Rights: Studies in the Philosophy of Law and Morals*. Norwell, MA: Kluwer Academic Publishers, 1997.

Zedner, L. "Pre-Crime and Post-Criminology." *Theoretical Criminology* 11 (2007): 261.

Legislation and Jurisprudence

22 U.S.C. § 2656f (2005).

Abrams v. United States, 250 U.S. 616 (1919).

An Act Declaring the Rights and Liberties of the Subject and Settling the Succession of the Crown, 1689 (U.K.), 1 William & Mary I, c. 2.

Anti-terrorism Act, S.C. 2001, c. 41.

Criminal Code, R.S.C. 1985, c. C-46.

Mugesera v. Canada (Minister of Citizenship and Immigration), 2005 SCC 40, [2005] 2 S.C.R. 100.

R. v. Keegstra, [1990] 3 S.C.R. 697.

R. v. Khawaja (2006), 214 C.C.C. (3d) 399 leave to appeal to S.C.C. denied [2006] S.C.C.A. No. 505.

R. v. Tessling, 2004 SCC 67, [2004] 3 S.C.R. 432.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Suresh v. Canada (Minister of Citizenship and Immigration), 2002 SCC 1, [2002] 1 S.C.R. 3, at para. 98.

Terrorism Act 2006 (U.K.), 2006, c. 11.

Threats to International Peace and Security (Security Council Summit 2005), SC Res. 1624, UN SCOR, 60th Sess., U.N. Doc. S/RES/1624 (2005).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(a)

Research Note

Glorification of Terrorism Leading to Terrorist Acts

Short-term Research Request for Rachel Fogl, CLPS

Prepared by Austin Lawrence and Melissa Northcott, RSD

July 7, 2009

Paraphrasing Rachel Fogl's research question:

"Statistically, what is a more likely course of action -- 1) a person engages in glorification-type activities (goes to meetings, rallies, etc.), then graduates to terrorist acts that are serious criminal offences, or 2) those who talk, go on talking, but those who end up doing serious stuff, do it quickly."

- In attempting to answer this question we focused on academic research into salafi jihadist terrorists, although we did look more broadly at other types of radicalization into violent extremism. The academic literature largely focuses on violent activities, not other crimes. Unfortunately, the published research we reviewed could not definitely answer your question.
    - This is mainly because the research method used was to examine identified terrorists and understand their progression into terrorism. The studies did not examine other individuals following the same progression that did not end up as terrorists.
- Friendship and family ties to violent extremists is much more important than simple exposure to messages of violent extremism (i.e. glorification-type activities).
    - Though, it is true that all people who acted on a violent extremist ideology (i.e. terrorists) either produced or consumed messages of violent extremism.
    - [redacted]
- The type of glorification-type message and how it is disseminated and consumed may make a difference in the radicalization process. It appears that the axiom "The more personal, the more effective." holds true.
    - It has been argued by Sageman and other analysts, that the Internet is a medium that leads to more radicalization. Thus, glorification of terrorism on the Internet may be more effective as a tool of radicalization than traditional media.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(a)

- This is because its' borderless reach instantly creates a stateless community of self-selected believers.
- Messages can to be reproduced by believers very easily, since there is no barrier to publication or dissemination.
- Internet software tools are designed to create virtual communities and foster social networks on single issues where much passing of information is personalized to a degree.
    - At the moment, by invitation-only Internet forums (and open forums to a lesser degree) are the main nucleus of radicalization. Not open websites. These sources are also some of the best sources for counter-terrorism intelligence.
    - Extremist messages (such as video recordings) passed hand-to-hand are personalized by friendship and kinship bonds, lending them greater validity. This type of personal dissemination is often cited as existing at the stage terrorist cells form.
- The time that it takes for someone to move from moderate to radical to violent extremist views to acting on violent extremist views appears to vary. We could find no empirical studies summarizing this progression temporally.
    - Case study overviews of salafi jihadists, by the likes of Sageman and Kreb, indicate that radicalization can take place very quickly. It may only take a span of several months to a year to move from being a moderate to espousing violent extremist views. However, it is a further several months of operational planning, etc. before an act of terrorist violence might be committed.
    - Further, the move along the continuum of radicalization is not a simple metric of the amount of exposure to violent extremist messaging (i.e. once a certain threshold is reached an individual decides to perpetrate terrorist acts), but is more correlated to other variables such as relationships with friends, relatives, events in foreign affairs and personal identity issues.
- People who went on to perpetrate terrorist acts themselves do not usually appear to be those who produce the most sophisticated violent extremist messages, although they do actively disseminate them.
    - However, as a caution, this may not support the hypothesis that "those who glorify just talk and those that listen do."
    - [redacted]

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.
s.21(1)(a)

- [redacted]

- The following is some quantitative information relevant to considerations of glorification of terrorism in the context of salafi jihadist terrorism in Canada:

    - In a 2006 poll of Muslim Canadians, 12% of respondents either somewhat or fully supported the goals of the alleged "Toronto 18" terrorist cell.

    - [redacted]

    - CSIS, meanwhile, has stated publicly that it is monitoring "several hundred" national security-related subjects of interest (among whom are radicalized individuals).

    - Using these numbers and some very rough assumptions we can do some mental estimation regarding glorification and radicalization in Canada.

        - Assumption A: [redacted]

        - Assumption B: [redacted]

            - Assumption B [redacted]

        - Estimate A: [redacted]

        - Assumption C: [redacted]

            - [redacted]

            - [redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Estimate B: [redacted]

- We are not aware of any kind of quantitative study of the types of glorification activities people engage in (rallies versus passing on print message versus passing on electronic communication versus producing messages versus attending lectures, etc.) and how that relates to radicalization into active violent extremism.

Core References

Environics Research Group. Focus Canada: The Pulse of Canadian Public Opinion, Report 2006-4. Ottawa, 2006.

[redacted]

National Security Criminal Investigations. Radicalization: A Guide for the Perplexed. Royal Canadian Mounted Police: Ottawa, June 2009.

Sageman, M. Leaderless Jihad: Terror Networks in the Twenty-First Century. University of Pennsylvania Press: Philidelphia, 2008.

Sageman, M. Understanding Terror Networks. University of Pennsylvania Press: Philidelphia, 2004.

Silke, A. "Holy Warriors: Exploring the Psychological Process of Jihadi Radicalization." *European Journal of Criminology*, 2008, 5(1): 99-123.

Other References

Bakker, E. Jihadi Terrorists in Europe: Their Characteristics and the Circumstances in Which They Joined the Jihad: An Exploratory Study. Netherlands Institute of International Relations, 2006.

Counter-Terrorism Implementation Task Force. First Report of the Working Group on Radicalism and Extremism that Lead to Terrorism: Inventory of State Programs. United Nations, 2008.

Davis, P. and Cragin, K., eds. Social Science for Counterterrorism: Putting the Pieces Together. RAND, National Defence Research Institute, 2009.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Hegghammer, T. Terrorist Recruitment and Radicalization in Saudi Arabia. Middle East Policy Council, 2006.

Home Office. Statistics on Terrorism Arrests and Outcomes, Great Britian. Home Office, United Kingdom, 2009.

Horgan, J. and Taylor, M. "The Making of a Terrorist." *Jane's Intelligence Review*, December 01, 2001.

Maghaddam, F. "The Staircase to Terrorism: A Psychological Exploration." *American Psychologist*, February-March 2005.

Moghadam, A. The Roots of Suicide Terrorism: A Multi-Causal Approach. Harvard University, 2006 (pre-published edition).

Ressler, S. "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research." *Homeland Security Affairs*, vol. 2, no. 2 (July 2006).

Shaunessy, M. "Praising the Enemy: Could the United States Criminalize the Glorification of Terror Under and Act Similar to the United Kingdom's Terrorism Act 2006?" Pen State Law Review, v. 113, no. 3 (Winter 2009).

Wiktorowicz, Q. Joining the Cause: Al-Muharjiroun and Radicalism. Rhodes College.

000031

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

TERRORIST LISTING PROCEDURES:

A Research Synthesis of Legislation, Cases and Literature on the UN 1267 Process, the European Union, the United Kingdom, the United States, Australia and New Zealand

October 2010

FINAL

Craig Forcese* and Kent Roach**

Table of Contents

Bibliographic Table of Legislation, Cases and Literature 3

Executive Summary 10

Introduction 13

Overview and Mandate 13

Structure 14

Part One: The UN 1267 Listing Process 14

A. Methodology 16

B. Findings 16

1. An Overview of the 1267 Listing Process 16
2. Court Decisions and the 1267 Listing Process 21
3. The Literature on the 1267 Listing Process 23

C. Discussion and Conclusions 35

1. Early Literature 36
2. Post-2006 Literature 36
3. Critique of the Literature 38
4. Due Process Reform Proposals 41
5. Conclusion 43

Part Two: European Union 44

A. Methodology 4444

B. Findings 44

1. Legislation 44
2. Court Decisions 48

a) Caselaw Concerning Implementation of the UN 1267 Listing Process 48

b) Caselaw Concerning the EU Unilateral Listing Process 56

* Associate Professor, Faculty of Law, University of Ottawa.
** Professor, Faculty of Law, University of Toronto.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

3. Literature 58
C. Discussion and Conclusions 71

Part Three: United Kingdom 72
A. Methodology 72
B. Findings 73
1. Legislation 73
a) Implementing the UN 1267 Process 73
b) Implementing UN Security Council Resolution 1373 73
c) Proscribed Organization Listing 74
2. Court Cases 7574
3. Literature 76
C. Discussion and Conclusions 77

Part Four: United States 77
A. Methodology 77
B. Findings 78
1. Legislation 78
a) Specially Designated Global Terrorist (SDGT) 78
b) Foreign Terrorist Organization Listing 78
2. Court Cases 79
3. Literature 81
C. Discussion and Conclusions 88

Part Five: Australia 89
A. Methodology 89
B. Findings 89
1. Legislation 89
2. Court Cases 90
3. Australian Law Reform Proposals 90
4. Literature 97
C. Discussion/Conclusions 101

Part Six: New Zealand 105
A. Methodology 105
B. Findings 105
1. The New Zealand Listing Process 105
2. Court Cases 107
3. The Literature 107
C. Discussion/Conclusions 110

Part Seven: Overall Conclusion 112

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

BIBLIOGRAPHIC TABLE OF LEGISLATION, CASES AND LITERATURE

UN RESOLUTIONS

Resolution 1267 ..... passim
Resolution 1333 ..... 16, 45
Resolution 1373 ..... passim
Resolution 1390 ..... passim
Resolution 1455 ..... 17, 45
Resolution 1526 ..... 17, 25, 68
Resolution 1617 ..... 17, 18
Resolution 1730 ..... 17, 18, 28, 31
Resolution 1735 ..... 17, 18, 31
Resolution 1822 ..... 17, 19, 31
Resolution 1904 ..... passim

UN LITERATURE

Boothe, Michael. "Security Council's Targeted Sanctions Against Presumed Terrorists," (2008) 6 *Journal of International Criminal Justice* 541. 31

Cameron, Iain. "UN Targeted Sanctions, Legal Safeguards and the European Convention on Human Rights" (2003) 72 *Nordic Journal of International Law* 159 23

Farrall, Jeremy Matam. *United Nations Sanctions and the Rule of Law* (Cambridge University Press, 2007). 28

Fassbender, Bardo. *Targeted Sanctions and Due Process* (March 2006) 25

Foot, Rosemary. "The United Nations, Counter-Terrorism and Human Rights: Institutional Adaptation and Embedded Ideas,"(2007) 29 *Human Rights Quarterly* 489 28

Godinho, Jorge. "When Worlds Collide: Enforcing UN Asset Freezes in EU Legal Order," (2010) 16 *European Law Journal* 67. 32

Gurule, Jimmy. "The Demise of the UN Economic Sanctions Regime to Deprive Terrorists of Funding," (2009) 41 *Case Western Reserve J. of Int. Law* 19 33

Gutherie, Peter. "Security Council Sanctions and the Protection of Individual Rights" (2004) 60 *NYY Annual Survey of American Law* 491. 24

Hudson, Andrew. "Not a Great Asset: The UN Security Council's Counter-Terrorism Regime: Violating Human Rights," (2007) 25 *Berkeley Journal of International Law* 203. 27

Johnstone, Ian. "Legislation and Adjudication in the UN Security Council: Bringing Down the Deliberative Deficit," (2008) 102 *American Journal of International Law* 275. 29

Kanetatke, Machiko. "Enhancing Community Accountability of the Security Council Through Pluralistic Structure: The Case of the 1267 Committee," (2008) 12 *Max Planck Yearbook of United Nations Law* 113.. 29

Keller, Helen and Andreas Fisher "The UN Anti-Terror Sanctions Regime under Pressure" (2009) 9 *Human Rights Law Review* 257. 34

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Lopez George A. et al, *Overdue Process: Protecting Human Rights while Sanctioning Alleged Terrorists,* A Report to Cordaid from the Fourth Freedom Forum and Kroc Institute for International Peace Studies at the University of Notre Dame (April 2009).....31
Meyers, Daniel. "The Transatlantic Divide over the Implementation and Enforcement of Security Council Resolutions," (2008) 38 *California Western International Law Journal* 255.....30
Michaelsen, Christopher. '*Kadi and Al Barakaat v Council of the European Union and Commission of the European Communities:* The Incompatibility of the United Nations Security Council's 1267 Sanctions Regime with European Due Process Guarantees' (2009) 10 *Melbourne Journal of International Law* 330...32
Michaelson, Christopher. "The Security Council Al Qaeda and Taliban Sanctions Regime: 'Essential Tool' or Increasing Liability in the UN's Counterterrorism Efforts?" (2010) 33 *Studies in Conflict and Terrorism* 448.....34
Reich, Johannes. "Due Process and Sanctions Targeted Against Individuals Pursuant to UN Resolution 1267(1999),"(2008) 33 *Yale J of Int Law* 505.....30
Rosand, Eric. "The Security Council's Efforts to Monitor the Implementation of the Al Qaeda/Taliban Sanctions" (2004) 98 A.J.I.L. 745.....23
van den Herik, Larissa. "The Security Council's Targeted Sanctions Regimes: In Need of Better Protection of the Individual," (2007) 20 *Leiden Journal of International Law* 797.....27
Watson Institute of Brown University *Addressing Challenges to Targeted Sanctions: An Update of the "Watson Report"* (October, 2009).....26
Watson Institute of Brown University, *Strengthening Targeted Sanctions Through Fair and Clear Procedures* (March 2006).....25

EU STATUTES

Common Position 1999/727/CFSP.....44
Common Position 2001/154/CFSP.....45
Common Position 2001/931/CFSP.....46, 64
Common Position 2001/932.....57
Common Position 2002/402/CFSP.....46, 47
Common Position 2003/140/CFSP.....47
Regulation No. 1190/2008.....51
Regulation No. 1286/2009.....48
Regulation No. 2580/2001.....passim
Regulation No. 337/2000.....45
Regulation No. 467/2001.....46
Regulation No. 501/2009.....57
Regulation No. 561/2003.....47
Regulation No. 881/2002.....passim
Treaty of Rome.....44, 46, 48, 49

EU CASES

Case C-229/05 *PKK and KNK*.....56
Case C-266/05 *Sison*.....56
Case C-340/08, *M & Others v. Her Majesty's Treasury* (ECJ Judgment), Apr. 29, 2010.....55

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Case C-354/04 *Gestoras Pro Amnisti´a* 56
Case T-135/06 *Al Bashir Al-Faqih* 54
Case T-136/06 *Sanabel Relief Agency* 54
Case T-137/06 *Ghunia Abdrabbah* 54
Case T-138/06 *Taher Nasuf* 54
Case T-228/02 *Organisation des Modjahedines du peuple d'Iran* 57
Case T-253/04, *KONGRA-GEL* 57
Case T-256/07 *People's Mojahedin Organization of Iran* 57
Case T-284/08 *People's Mojahedin Organization of Iran* 57
Case T-318/01, *Othman* 53
Case T-327/03, *Stichting Al-Aqsa* 56
Case T-341/07 *Sison* 57
Case T–47/03 *Sison* 57
Cases T-37/07 and T-323/07 *Mohamed El Morabit* 56
Joined Cases C-399/06 P and C-403/06 P, *Hassan v. Council and Commission*, ECJ Judgment, 3 December 2009 53
Joined Cases C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the EU and Commission of the EC* (ECJ Judgment), Sept. 3, 2008 48

EU LITERATURE

Almqvist, Jessica, "A Human Rights Critique of European Judicial Review: Counter-terrorism Sanctions," (2008) 57 International and Comparative Law Quarterly *303*. 59
Besson, Samantha, "European Legal Pluralism after *Kadi*," (2009) 5 *European Constitutional Law Review* 237. 60
Cameron, Iain, "European Union Anti-terrorist Blacklisting," (2003) 3(2) Human Rights Law Review 225. 58
Cananea, Giacinto della, "Global Security and Procedural Due Process of Law between the United Nations and the European Union: Yassin Abdullah Kadi & Al Barakaat International Foundation V. Council," (2009) 15 *Colum. J. Eur. L.* 511 60
Cardwell, Paul James, Duncan French and Nigel D. White, "European Court of Justice, Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council and Commission," (2009) 58 *International and Comparative Law Quarterly* 229. 61
Cremona, Marise, Francesco Francioni, Sara Poli (eds), *Challenging the EU Counter-Terrorism Measures through the Courts*, EU Working Papers, AEL 2009/10 (Academy of European Law) 62
d'Aspremont, Jean and Frederic Dopagne, "*Kadi:* The ECJ's Reminder Of The Elementary Divide Between Legal Orders," (2009) 5 *International Organization Law Review* 371 62
Draghici, Carmen, "Suspected Terrorists' Rights Between the Fragmentation and Merger of Legal Orders: Reflections in the Margin of the Kadi ECJ Appeal Judgment" (2009) 8(4) *Washington University Global Studies Law Review* 627. 63
Eckes, Christina, "A Test Case for the Resilience of the EU's Constitutional Foundations: International Sanctions," (2009) 15(3) *European Public Law* 351. 64
Eckes, Christina, "Sanctions against Individuals – Fighting Terrorism within the European Legal Order," (2008) 4(2) *European Constitutional Law Review* 205. 64

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Eckes, Christina. "Judicial review of European anti-terrorism measures - the Yusuf and Kadi judgments of the Court of First Instance," (2008) 14(1) *European Law Journal* 74. 63
Godinho, Jorge. "When worlds collide: enforcing United Nations Security Council asset freezes in the EU legal Order" (2010) 16(1) *European Law Journal* 67. 64
Harpaz, Guy. "Judicial Review by the European Court of Justice of UN Smart Sanctions against Terror in the Kadi Dispute," (2009) 14(1) *European Foreign Affairs Review* 65. 65
Johnston, Angus. "Freezing terrorist assets again: walking a tightrope over thin ice?" (2008) 67(1) *Cambridge Law Journal* 31. 66
Johnston, Angus. "Thawing out? The European courts and the freezing of terrorist assets," (2007) 66(2) *Cambridge Law Journal* 273. 65
Johnston, Angus. "The European Union, the ongoing search for terrorists' assets and a satisfactory legal framework: getting warmer or colder?" (2007) 66(3) *Cambridge Law Journal* 523. 66
Kunoy, Bjorn and Anthony Dawes. "Plate Tectonics in Luxembourg: The Menage a Trois between EC Law, International Law and the European Conventions on Human Rights Following the UN Sanctions Cases," (2009) 46(1) *Common Market Law Review* 73. 66
Menz, Simon and Tobias B. Scholz. "The Kadi Case or the Legal Protection of Persons Included in the European Union Anti-Terror List," (2009) 17(1) *European Journal of Crime, Criminal Law and Criminal Justice* 61 67
Michaelson, Christopher. "Kadi and Al Barakaat v Council of the European Union and Commission of the European Communities" (2009) 10 *Melbourne Journal of International Law* 330. 67
Payandeh, Mehrdad and Heiko Sauer, "European Union: UN sanctions and EU fundamental rights," (2009) 7(2) *International Journal of Constitutional Law* 306. 67
Porretto, Gabriele, *The European Union: Counter-Terrorism Sanctions Against Individuals and Human Rights Protection* (June 25, 2009). Transitional Justice Institute Research Paper No. 09-08. 68
Posh, Alberto, "The Kadi Case: Rethinking the Relationship between EU Law and International Law? (2009) 15 *Colum. J. Eur. L. Online* 1. 68
Simoncini, Marti "Risk Regulation Approach to EU Policy against Terrorism in the light of the ECJ / CFI jurisprudence," (2009) 10(11) *German Law Journal* 1526. 68
Spaventa, Eleanor, "Case T-256/07, People's Mojahedin Organization of Iran v Council" (2009) 46(4) *Common Market Law Review* 1239 69
Tridimas, Takis and Jose A. Gutierrez-Fons, "EU Law, International Law, and Economic Sanctions against Terrorism: The Judiciary In Distress?" (2009) 32 *Fordham Int'l L.J.* 660. 69
Tzanou, Maria. "Case-note on Joined Cases C-402/05 P & C-415/05 P *Yassin Abdullah Kadi & Al Barakaat International Foundation* v. *Council of the European Union & Commission of the European Communities*," (2009) 10(2) *German Law Journal* 123. 70
Weema, Christopher, "Kadi v. Council: Putting the United Nations in Its Place," (2009) 17 *Tul. J. Int'l & Comp. L.* 571 70
Zgonec-Rozej, Misa. "Yassin Abdullah Kadi & (and) Al Barakaat International Foundation v. Council & (and) Commission" (2009) 103(2) *American Journal of International Law* 305. 71

UK STATUTES

Al-Qaida and Taliban (Asset-Freezing) Regulations 2010, SI 2010/1197 73
European Communities Act 1972, c.68 73

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Terrorism (United Nations Measures) Order 2006, S.I. 2006/2657 73
Terrorism (United Nations Measures) Order 2009, S.I. 2009/1747 73
Terrorism Act, 2000, c.11 74
Terrorism Act, 2006, c.11 74
Terrorist Asset-Freezing (Temporary Provisions) Act 2010, c.2 74
United Nations Act 1946, c.45. 73

UK CASES

Her Majesty's Treasury v Ahmed and al-Ghabra (FC) [2010] UKSC 2 75
Lord Alton of Liverpool v. Secretary of State for the Home Department, [2008] EWCA Civ 443 76

UK LITERATURE

Middleton, Ben. "Terrorism Act 2000: seeking deproscription." (2008) 72 *Journal of Criminal Law* 270. 76

US STATUTES

18 U.S.C 2339B 78
3 U.S.C. 301 78
31 C.F.R. 594 78
Executive Order No. 13224 78
Immigration and Nationality Act (INA), 8 U.S.C. 1189(a) 79
International Emergency Economic Powers Act (IEEPA), 50 U.S.C.S. §§ 1701-1706 78
National Emergencies Act, 50 U.S.C. 1601 78
United Nations Participation Act of 1945, 22 U.S.C. 287c 78

US CASES

Al Haramain Islamic Foundation, Inc. v. U.S. Department of the Treasury, Civil Case No. 07-1155-KI (November 5, 2009) 80
Al-Aqeel v. Paulson, 568 F. Supp. 2d 64 (D.D.C. 2008) 80
Global Relief Found., Inc. v. O'Neill, 315 F.3d 748 (7th Cir. 2002) 80
Holy Land Found. for Relief & Dev. v. Ashcroft, 333 F.3d 156 (D.C. Cir. 2003) 80
Humanitarian Law Project v. *Mukasey*, 552 F.3d 916 (9th Cir., 2009) 80
Humanitarian Law Project v. U.S. Department of Treasury, 463 F. Supp. 2d 1049 79
Humanitarian Law Project v. U.S. Department of Treasury, 484 F.Supp.2d 1099 (C.D. Cal. 2007) 79
Humanitarian Law Project v. U.S. Department of Treasury, 578 F.3d 1133 (9th Cir. 2009) 79
Islamic American Relief Agency v. Gonzales, 477 F. 3d 728 (D.C. Cir. 2007) 80
KindHearts for Charitable Humanitarian Dev., Inc. v. Geithner, 647 F. Supp. 2d 857 (N.D. Ohio 2009) 79
National Council of Resistance of Iran v. Department of State, 251 F.3d 192 (DC Cir. 2001) 81
People's Mojahedin Org. v. Department of State, 327 F. 3d 1238 (D.C. Cir. 2003) 81

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

US LITERATURE

Chesney, Robert. "The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention," (2005) 42 *Harv. J. On Legis.* 1 81
Chugani, Sumeet H. "Benevolent blood money: terrorist exploitation of Zakat and its complications in the war on terror." (2009) 34 *North Carolina Journal of International Law and Commercial Regulation* 601..... 82
Cole, David. "The New McCarthyism: Repeating History in the War on Terrorism," (2003) 38 *Harvard Civil Rights-Civil Liberties Law Review* 1. 82
Donohue, Laura K. "Constitutional and legal challenges to the anti-terrorist finance regime," (2008) 43 *Wake Forest Law Review* 643 82
Folendorf , Carrie. "Breaking Terror's Bank Without Breaking the Law: A Comment on the USA Patriot Act and the United States Financial War on Terrorism" (2003) 23 J. NAALJ 481. 83
Furst III, Joseph. "Guilt By Association and the AEDPA's Fund Raising Ban," (1999) 16 N.Y.L. Sch. J. Hum. Rts. 475..... 83
Gurule, Jimmy. *Un-Funding Terror: The Legal Response to the Financing of Global Terrorism* (Edward Elgar Publ. 2008)..... 84
Hardister, Angela D., "Can We Buy Peace On Earth?: The Price of Freezing Terrorist Assets in a Post-September 11 World," (2003) 28 *North Carolina Journal of International Law and Commercial Regulation* 605. 85
Jonkait, Randolph. "A Double Due Process Denial: The Crime of Providing Material Support or Resources to Designated Foreign Terrorist Organizations," (2003-2004) 4a8 N.Y.L. Sch. L. Rev. 125. 85
Nice-Petersen, Nicole. "Justice for the 'Designated': The Process that is Due to Alleged U.S. Financiers of Terrorism," (2005) 93 Geo. L.J. 1387. 85
O'Leary, Robert E., "Improving the Terrorist Finance Sanctions Process," (2010) 42 N.Y.U. J. Int'l L. & Pol. 549. 86
Ortblad, Vanessa, "Criminal prosecution in sheep's clothing: the punitive effects of OFAC freezing sanctions," (2008) 98 *Journal of Criminal Law and Criminology* 1439. 86
Piers, Matthew J. "Malevolent destruction of a Muslim charity: a commentary on the prosecution of Benevolence International Foundation," (2005) 25 *Pace Law Review* 339. 86
Roth, John, Douglas Greenberg, Serena Willie, "National Commission on Terrorist Attacks Upon the Untied States: Monograph on Terrorist Financing," Staff Report to the Commission (2004). 86
Shapiro, Julie B. "The politicization of the designation of foreign terrorist organizations: the effect on the separation of powers," (2008) 6 *Cardozo Public Law, Policy & Ethics Journal* 547. 87
Stampley, Danielle. "Blocking Access to Assets: Compromising Civil Rights to Protect National Security Or Unconstitutional Infringement On Due Process And The Right To Hire An Attorney?" (2008) 57 Am. U.L. Rev. 683..... 87
Wyatt, Micah, "Designating Terrorist Organizations: Due Process Overdue" (2008-2009) 39 Golden Gate U. L. Rev. 221. 87

AUSTRALIA STATUTES

Charter of the United Nations Act, 1945 90
Criminal Code Act 1995, Act No. 12 of 1995..... 89
Suppression of the Financing of Terrorism Act, 2002, No. 66 of 2002 90

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

AUSTRALIA LITERATURE

Gani, Miriam and Gregor Urbas "Alert or Alarmed? Recent Legislative Developments Aimed at Terrorist Organizations and Persons Supporting or Assisting in Terrorist Acts" (2004) 8 Newcastle L.Rev. 23. ..99
Hocking, Jenny. "Counter-terrorism and the Criminalization of Politics: Australia's New Security Powers of Detention, Proscription and Control" (2003) 49 *Australian J of Politics and History* 355. 97
Hogg, Russell. 'Executive Proscription of Terrorist Organisations in Australia: Exploring the Shifting Border between Crime and Politics' in Miriam Gani and Penlope Mathew (eds) *Fresh Perspectives on the 'War on Terror'* (ANU Press, 2008). 100
Joseph, Sarah. "Australian Counter-Terrorism Legislation and the International Human Rights Framework" [2004] 27 *University of New South Wales* 428. 98
Lynch, McGarrity and Williams "The Proscription of Terrorist Organizations in Australia" (2009) 37 *Federal Law Review* 1. 101
McGarrity, Nicola. "Review of the Proscription of Terrorist Organizations: What Role for Procedural Fairness? (2008) 16 *Australian J. of Admin Law* 45. 100
National Security Legislation Discussion Paper on Proposed Amendments (July 2009).....94
Parliamentary Joint Committee on Intelligence and Security *Inquiry into the proscription of 'terrorist organizations' under the Australian Criminal Code* (September 2007).....93
Report of the Security Legislative Review Committee (June 2006).....91
Ruddock, Phillip. "Australia's Legislative Response to the Ongoing Threat of Terrorism" (2004) 27 U.N.S.W.L.Rev. 254.....98
Tham, Joo-Cheong. "Possible Constitutional Objections to the Powers to Ban 'Terrorist' Organisations" [2004] UNSWLawJl 31; (2004) 27(2) University of New South Wales Law Journal 482.....99

NZ STATUTES

Terrorism Suppression Act, 2002 No. 34.....105
UN Sanctions (Afghanistan) Regulations 105
United Nations Act, 1946 No. 7.....105

NEW ZEALAND LITERATURE

Conte, Alex. *Counterterrorism and Human Rights in New Zealand* (New Zealand Law Foundation, 2007)..107

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

EXECUTIVE SUMMARY

This research paper examines the procedures used to compile lists of individuals and organizations believed to be associated with terrorist activities under UN Security Council 1267 and in the European Union, the United Kingdom, the United States, Australia and New Zealand. It focuses on court cases that have challenged listings and the legal literature about the listing procedures. It describes the methodologies used to survey the court cases and the literature.

The literature about the 1267 process and one relevant decision of the UN Human Rights Committee are reviewed. In the decision, the Committee held that a 1267 listing did not amount to a criminal sanction triggering fair trial requirements but that it did affect the right to travel and reputation. Belgium was held in breach of its obligations under the ICCPR for proposing a listing and being unable to obtain the delisting of the affected individuals after domestic processes had not confirmed culpable association with al Qaeda.

Much of the literature by legal experts on the 1267 listing process is critical of the process used by the 1267 Committee and its failure to comply with the judicial right to a remedy. The consensus among the experts is that reforms to the 1267 process such as the creation of a Focal Point and subsequently an Ombudsperson for delisting requests do not provide affected individuals with a right to a judicial remedy. Most commentators suggest that only a tribunal or court at the UN level could provide such remedies. Some note that domestic judicial remedies could interact with the 1267 process, but other legal experts stressed that domestic remedies for listing could put countries in breach of their mandatory obligations under the 1267 process and Chapter VII of the UN Charter.

Two more or less constant themes emerge from the legal literature on the 1267 process that is almost uniformly critical of the fairness of the process. The first theme is the difficulty of providing affected individuals with a meaningful opportunity to challenge the basis of listing within the intergovernmental and generally confidential process used by the 1267 Committee and to seek a remedy for wrongful listings.

The second theme is the dilemma of allowing states to maintain the confidentiality of the information that is said to justify the listing while also using that secret information as a basis for such a listing. It is not clear that reforms to the 1267 process such as the provision of narrative summaries for the basis for listing resolve this dilemma or provide affected individuals with a meaningful opportunity to challenge their listing. Narrative summaries appear to feature unsourced conclusions and assertions. Although such an approach can preserve the confidentiality of intelligence sources and methods, it also makes it impossible to judge the reliability of the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

underlying intelligence and the conclusions that are drawn that the individual or group is actually associated with al Qaeda or the Taliban. Thus even if the affected person could challenge the listing before an independent body capable of acting judicially, he or she might not be able to make a meaningful challenge in the absence of full disclosure or some other equivalent mechanism.

Many of these themes animate the literature concerning the EU system. Of note in relation to the EU is the now sizable number of cases successfully challenging either the EU regulations implementing the 1267 process or the EU "unilateral" listing system on due process grounds. The most notable decision is the recent holding of the European Court of Justice in *Kadi*. EU commentators for the most part view that decision favourably and see it as presenting serious challenges to the viability of the 1267 process. The long term implications of *Kadi* remain unclear, however. While the EU has introduced due process standards requiring notice, opportunity to comment and reasons surrounding EU listing of persons designated by the 1267 Committee, the adequacy of these due process reforms remains disputed, and new cases are underway in the EU legal system.

The United Kingdom, as a member of the EU, incorporates the EU listing process into its law. In some respects, therefore, its listing process is a double-derivative: implementation of EU rules that implement the UN list. However, the UK does have its own unique unilateral listing rules allowing for the listing of individuals and entities above and beyond those designated by the supranational and international bodies of which the UK is a part.

The UK listing process has attracted relatively little court or scholarly attention until recently. In the last year or so, however, a number of key decisions questioning the legal basis for the UK implementation and application of the 1267 list (among others) have been delivered by the UK Supreme Court and the European Court of Justice. These decisions have sparked reform efforts, although no real scholarship to date.

The United States literature departs from the trends observed with other jurisdictions in being largely indifferent to the international context in which listing is undertaken. The literature focuses almost exclusively on domestic legal issues, and in particular the due process shortcomings of the US designation rules. Once again, notice and comment issues figure in this discussion, but so too concerns about use of classified information and the role of the executive in rendering decisions in the absence of effective judicial oversight. Court challenges to the US rules have produced mixed outcomes, but seem increasingly to be imposing more robust due process expectations on the listing process.

Although no cases were discovered challenging the list of terrorist groups or individuals under the *Australian Criminal Code* or its *Charter of the United Nations Act*, a

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

wealth of critical literature about the Australian listing processes exists. A number of commentators have criticized listing for its adverse effects on political freedoms and for allowing the executive to exercise what are in essence judicial powers in making determination about an individual's involvement with terrorism. A range of law reform proposals in Australia are examined including those that would allow the judiciary to make listing determinations and the creation of an advisory body of experts who could review listings and hear requests for delisting. The Australian experience with listing is also noteworthy because of the role played by Parliamentary review in terms of briefings of the Leader of the Opposition before terrorist groups are listed and review by a Joint Parliamentary committee of listing after they have occurred.

As in Australia, no court cases challenging the listing process were discovered in New Zealand. The reasons for this finding are speculative but could involve various disincentives in challenging listing in relatively small jurisdictions as well as concerns about associating oneself with a group or individual listed as a terrorist for the purposes of judicial review. The New Zealand experience is noteworthy because of the central role of the Prime Minister in listing. From 2002-2007, New Zealand had an interesting provision that required judicial review and approval of a listing once the initial listing had expired after three years. The provisions for judicial review made allowance for the preservation of confidential information but were in any event abandoned in 2007 in preference to allowing the executive in the form of the Prime Minister to decide to re-list an individual or a group. Academics have, however, argued that the present regime (including provisions designed to protect intelligence from disclosure) does not accord with natural justice and fair trial rights. They have proposed that the Inspector General with expertise in intelligence conduct reviews of listing.

The New Zealand experience brings us full circle to the themes discussed in relation to the 1267 process. The first theme is the great challenge presented by the use of secret intelligence to support listing decisions and the difficulties of allowing such information to be challenged and its reliability determined. There are no simple solutions to the dilemmas of secret evidence that are seen not only in the listing process but other anti-terrorism activities. Although it is possible to imagine and propose creative reforms that will improve the listing process by allowing review of listing decisions by outside experts, courts or tribunals both before and after listing, such reforms may flounder if those who presently have the power to make listing decisions are unwilling to give up decision-making power over the listing process. The listing of terrorists is a procedure that is woven deeply into counter-terrorism regime at the international, supranational and regional levels. At the same time, it is one that is difficult to reconcile with the values of transparency and effective challenge and remedies for any errors made in the listing process.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTRODUCTION

Overview and Mandate

This research paper examines the procedures used to compile lists of individuals and organizations believed to be associated with terrorist activities. Our focus is on court cases that have challenged such listing procedures and the literature that has been written by legal experts about the listing process. Much of the legal literature focuses on the lack of safeguards and in particular the lack of hearings before and sometimes after an individual or an organization is added to a terrorist list. The consequences of being placed on a terrorist list are often severe and can involve sanctions such as the freezing of assets, travel bans and the criminalization of various forms of support and association with an individual or organization on the list. In keeping with some of these criticisms, there is a growing number of court cases that have resulted in successful direct or indirect challenges to listing decisions.

We have also examined responses to court cases and other criticisms of the listing process that have added safeguards to the listing process and survey the views expressed by legal experts in the literature about the adequacy of such safeguards.

An important caveat is that we have only been able to identify cases and literature that exist at this point of time. We are struck by the dynamic nature of the listing process and the changes that have occurred particularly in relation to the listing process first created by United Nations Security Council Resolution 1267 (1999). In 2006, a well regarded report on the 1267 process reported that it was aware of no domestic judicial decisions challenging listing[1], but a 2009 update of that original report noted that it was aware of 30 challenges decided or pending in domestic courts to the 1267 process.[2]

Both challenges and changes to listing regimes have accelerated in recent years and will continue to accelerate in the foreseeable future. We are also struck by the many legal experts who have expressed deep pessimism about the ability to reform the listing process to conform to satisfactory standards of fairness even while the United Nations, European Union and each of the domestic jurisdictions studied maintain that the listing of terrorist groups and individuals and associated sanctions and prohibitions are a vital part of modern counter-terrorism regimes.

---

[1] Watson Institute of Brown University *Strengthening Targeted Sanctions Through Fair and Clear Procedures* March 2006 available at http://watsoninstitute.org/pub/Strengthening_Targeted_Sanctions.pdf

[2] Watson Institute of Brown University *Addressing Challenges to Targeted Sanctions: An Update of the "Watson Report"* October, 2009 at 7 available at http://www.watsoninstitute.org/pub/2009_10_targeted_sanctions.pdf

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Structure

The first part of this paper will examine the listing process created under Resolution 1267 of the Security Council. It is appropriate to start with this process conducted under the mandatory provisions of Chapter VII of the UN Charter both because it applies to all states and because it created the impetus for much of the subsequent listing carried on at the supranational or national levels. A large and often critical literature has also developed discussing this process and some court cases at the supranational and domestic level provide indirect challenges and comments on the 1267 listing regime.

The next part of the paper will examine the listing process used by the European Union and a variety of court cases that have challenged that listing process; most notably the decision of the European Court of Justice in the *Kadi* case. There are, however, many other cases in the EU judicial bodies dealing with the EU listing processes, and a substantial legal literature.

The third part of the paper will examine listing processes and legal challenges in the United Kingdom, as a member state of the European Union. These court cases are recent, and have yet to generate a response in the legal literature.

The jurisdictions examined in the remainder of the paper will be the United States, Australia and New Zealand. As might be expected, there are a number of court cases – and a substantial legal literature – addressing the US process. In Australia and New Zealand, we have not been able to identify court cases challenging the listing systems, but we have found useful information about proposed and actual changes that have been made to the listing process.

In each jurisdiction examined we have provided an account of the methodology used to search legal databases, an account of the findings in the form of court cases and legal literature and then a more analytical discussion of the findings and conclusions.

PART ONE: THE UN 1267 LISTING PROCESS

We begin with a terminological note: As discussed, the UN terrorist listing process originated with UN Security Council Resolution 1267 in 1999, but it has been amended periodically since then by other resolutions. Despite these amendments, we shall refer to the process simply as "1267 listing" or use analogous descriptions. At present, the UN body overseeing the process is known as the "the Al-Qaida and Taliban Sanctions Committee". We, however, shall refer to it simply as the "1267 Committee".

In order to understand both the process for listing individuals and organizations associated with terrorist activities in domestic jurisdictions, it is necessary to understand the process created by UN Security Council Resolution 1267 and related Security Council Resolutions. An outline of this process is, of course, also necessary to

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

understand and analyze the views of legal experts in regards to the terrorist listing regime created by the 1267 Committee.

We do not discuss Security Council Resolution 1373 (2001), obliging states to criminalize terrorism and terrorism financing in detail. There is no UN-based 1373 listing system. Note, however, that some of the jurisdictions examined in this report pointed to resolution 1373 as justification for establishing separate domestic listing systems (which we typically refer to as "unilateral" listing systems).

A word about the overall purposes of both Security Council Resolution 1267 and 1373 is in order at this preliminary juncture. Both resolutions were enacted by the Security Council under Chapter VII of the United Nations Charter that provides for mandatory measures to protect international peace. As such, they place mandatory international obligations of all member states to follow those resolutions. In particular they impose mandatory obligations on states in an attempt to prevent acts of terrorism. These obligations include those relating to preventing funds that will finance acts of terrorism and the operations of terrorist groups and as such are congruent with the 1999 Convention for the Suppression of Terrorism Financing.

Security Council Resolution 1267 was in part a response to the terrorist bombings of American embassies in Africa in 1998. Its preamble strongly condemns "the continuing use of Afghan territory, especially areas controlled by the Taliban, for the sheltering and training of terrorists and planning of terrorist acts" and reaffirms the Security Council's "conviction that the suppression of international terrorism is essential for the maintenance of international peace and security." The preamble also notes bin Laden's indictment for the embassy bombings and deplores that the Taliban provided safe haven for bin Laden.

Security Council Resolution 1373 was in part a response to the terrorist attacks of September 11, 2001 on the United States. Its preamble reaffirms the Security Council's "unequivocal condemnation" of those attacks and the need "to combat by all means, in accordance with the Charter of the United Nations, threats to international peace and security caused by terrorist attacks". Moreover, that resolution decides that states shall "prevent and suppress the financing of terrorist acts" including the criminalization of the willful or knowing provision of funds to carry out terrorist attacks and the freezing of funds and other financial assets of those who commit or attempt to commit or facilitate terrorist acts. It also calls on states to prohibit those within their territories from providing funds and other financial assets to benefit terrorists. Lists of terrorists, terrorist groups and entities owned or controlled directly or indirectly by such persons, are a means used by many states to prevent terrorism and its financings and to comply with the mandatory directives of Security Council Resolutions 1267 and 1373.

In what follows, the methodology used for the literature review of the view of experts will be briefly described. Next under the heading of findings, a brief review of

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the UN 1267 listing regime will be provided followed by a more extensive review of the legal literature that was found on that process. This will be followed by a discussion/conclusion section reflecting on the themes and challenges raised by the 1267 list and the views of legal experts on the listing regime.

A. Methodology

General searches of the following electronic data bases were conducted under the words "1267 Committee" "United Nations Security Council listing of terrorists" and "terrorist listings", "terrorist proscriptions" and "individual sanctions" and the United Nations. The data bases searched included Social Science Research Network,[3] Hein Online,[4] the Legal Journals index (UK), and Legal Trac as well as searches using Google and Google scholar on the web. The decisions of the United Nations Human Rights Committee were also searched under similar terms in the CCPR data base.[5]

B. Findings

1. An Overview of the 1267 Listing Process

UN Security Council Resolution 1267 was issued by the Security Council on October 15, 1999 under Chapter VII of the United Nations Charter relating to the maintenance of international peace. The resolution recalled that Usama bin Laden and his associates had been indicted in the United States for the 1998 bombings of American embassies in Kenya and Tanzania and demanded that the Taliban as the *de facto* government of Afghanistan hand over bin Laden. It required sanctions against the Taliban in the form of denying permission for landing rights for aircraft operated on behalf the Taliban and for the freezing of funds directly or indirectly controlled by the Taliban as designated by a committee created by the resolution. It was also contemplated that the 1267 Committee could decide humanitarian exceptions to the travel ban and asset freezes provided by the resolution. Countries were required to report to the 1267 Committee within 30 days and to make periodic reports to the committee. The resolution also called on states to take proceedings against those who violated the prohibitions in the Resolution.

In 2000, the Security Council issued Resolution 1333 reaffirming the call for the Taliban to surrender bin Laden and imposing other measures directed at Afghanistan. For our purposes, the importance of this resolution was its extension of the sanction and freezing of assets regime from the Taliban as the *de facto* government of Afghanistan to

---

[3] Available at http://www.ssrn.com/lsn/index.html

[4] Available at http://heinonline.org.myaccess.library.utoronto.ca/HOL/Welcome?collection=journals

[5] Available at http://sim.law.uu.nl/SIM/CaseLaw/CCPRcase.nsf/(Article)/$Searchform?SearchView

000047

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

"Usama bin Laden and individuals and entities associated with him as designated by the Committee, including those in the Al-Qaida organization". This provision also mandated that the 1267 Committee "maintain an updated list, based on information provided by States and regional organizations, of the individuals and entities designated as being associated with Usama bin Laden, including those in the Al-Qaida organization".[6] As a consequence, it contemplated the maintenance of a list of terrorists associated with Al-Qaida based on information provided by states and regional organizations and extended the sanctioning regime to individuals.

A number of other Security Council Resolutions including Resolution 1390 (2002), Resolution 1455 (2003), Resolution 1526 (2004), Resolution 1617 (2005), Resolution 1730 (2006), Resolution 1735 (2006), Resolution 1822 (2008) and Resolution 1904 (2009) have subsequently been issued, all under Chapter VII, and have reaffirmed and modified the original listing regime. This activity makes the listing regime a moving and dynamic target. This also has meant that some of the legal literature evaluating the 1267 listing process has become out of date. As will be seen, however, much of the literature evaluated a number of reform options for the 1267 listing and in this sense can be useful even if the 1267 listing process has changed since the literature was written and published.

A number of earlier resolutions were designed to strengthen the listing regime in the sense of enhancing its effectiveness. For example, Resolution 1455 (2003) asked states to submit names of those associated with the Taliban and Al Qaeda for consideration by the committee and to enact domestic measures to "to prevent and punish"[7] violations of the bans in the primary resolution. Resolution 1526 (2004) asked the committee to monitor domestic compliance with the regime in member countries and created a monitoring team with expertise in Al Qaeda, terrorism financing, arms embargos, charities, alternative remittance systems and banking to assist in such monitoring. Resolution 1617 (2005) provided a broad definition of what would constitute association with bin Laden, Al Qaida or the Taliban.[8]

---

[6] UN Security Council Resolution 1333 para 8 (a).

[7] UN Security Resolution 1455 para 5.

[8] Paragraph 2 provides that the Security Council:

Further decides that acts or activities indicating that an individual, group, undertaking, or entity is "associated with" Al-Qaida, Usama bin Laden or the

Taliban include:

– participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of;

– supplying, selling or transferring arms and related materiel to;

– recruiting for; or

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

In the last half-decade several resolutions have included measures designed to remedy complaints about the unfairness of the 1267 process. Thus, Resolution 1617 (2005) requested relevant states to inform those on the Consolidated List "to the extent possible"[9] and made clear that states could provide the 1267 Committee with confidential information or intelligence that would only be released with the state's consent.[10]

Resolution 1735 (2006) decided that all states when proposing names to be added to the list "should provide as much detail as possible on the basis(es) for the listing, including: (i) specific information supporting a determination that the individual or entity meets the criteria above; (ii) the nature of the information and (iii) supporting information or documents that can be provided; States should include details of any connection between the proposed designee and any currently listed individual or entity" and indicate what part of this information can be publicly released either to the listed entity or to interested states.[11] These provisions can be seen as attempts to increase the information that informs listing decisions while at the same time respecting the idea that information submitted by member states to the 1267 Committee would not be released without the state's permission.

Resolutions 1730 and 1735 (2006) dealt specifically with delisting by deciding that the 1267 Committee should adopt delisting guidelines that would consider whether listing was a result of a mistake of identity, whether the listed individual was deceased and whether the criteria for listing still applied, for example in a case of those who had been affirmatively shown to have severed all associations with Al Qaeda, bin Laden and the Taliban.[12] Resolution 1730 adopted a delisting procedure that created a focal point to receive requests for delisting from entities on the consolidated list. This process was in addition to the process where a listed person could approach their state of citizenship or residence and the state could hold bilateral consultations with the state that had first proposed that the entity be listed. Resolution 1730 provided that once a delisting request had gone before the 1267 Committee then the request for delisting shall be deemed rejected if no Committee member recommends delisting.

– otherwise supporting acts or activities of;

Al-Qaida, Usama bin Laden or the Taliban, or any cell, affiliate, splinter group or derivative thereof

UN Security Council Resolution 1617 (2005).

[9] Ibid para 5

[10] Ibid para 6

[11] UN Security Council Resolution 1735 (2006) paras 5 and 6.

[12] UN Security Council 1822 (2008) paras 13-14.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Resolution 1822 (2008) directed the 1267 Committee to provide a narrative summary of the reasons for the listing and make these available on the committee's website. Member states were also requested to identify those parts of the reasons for listing that could be publicly identified in the narrative summaries.[13] This represents an attempt both to provide public reasons for the listing but also to protect secret intelligence that may lie behind the listing.

This resolution also contemplated that the Committee would promptly inform member states of listings and that the states would communicate the fact of listing to the affected individuals in their jurisdictions including information about the narrative summary, delisting procedures and applications for humanitarian exemptions. Member states were also required to notify individuals of any delisting by the 1267 Committee. Designating states and states of citizenship were urged to co-operate with the Focal Point process and to consider delisting petitions in a timely manner and indicate whether they supported or opposed the petition. [14] The 1267 Committee was also to review all names on the Consolidated list by 30 June 2010 and thereafter review the names that had not been reviewed in the last three years.[15] This resolution demonstrated a concern about enhancing the accuracy and reasons for listing but also contained provisions for the continued protection of confidential information and the nature of listing and delisting as a process decided by the governments on the 1267 Committee.

Resolution 1904 (2009) was adopted on 17 December 2009. Like many of the other resolutions it affirms the Security Council's commitment to the individual sanctions in Resolution 1267 and calls on Member states to forward names to be considered for listing by the 1267 Committee. It also confirms the broad definition of those who should be listed as including those financing, participating, recruiting for or "otherwise supporting acts or activities of Al-Qaida, bin Laden or the Taliban or any cell, affiliate, splinter group or derivative thereof".[16]

Resolution 1904 also encourages member states to provide a detailed statement of the case when proposing listing. The onus is placed on member states to identify information (including in some cases the identity of the designating state) that should be kept confidential and not placed on the narrative summaries of the listing made public by the 1267 Committee. [17] This resolution also "*Encourages* Member States and relevant international organizations to inform the Committee of any relevant court

---

[13] Ibid at paras 14 and 15

[14] Ibid at para 20

[15] Ibid at paras 25 and 26

[16] UN Security Council Resolution 1904 (2009) at para 2.

[17]Ibid at paras 11 and 12

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

decisions and proceedings so that the Committee can consider them when it reviews a corresponding listing or updates a narrative summary of reasons for listing". [18] This demonstrates an awareness by the 1267 Committee that listing decisions are being challenged at least indirectly at the domestic level.

The most important change in Resolution 1904 is the replacement of the Focal Point process with a new process where an Ombudsperson described as "an eminent individual of high moral character, impartiality and integrity with high qualifications and experience in relevant fields, such as legal, human rights, counter-terrorism and sanctions" [19] will be appointed to consider requests for delisting. In addition to delisting requests from states, the Ombudsperson can make delisting recommendations to the 1267 Committee and the committee is encouraged "to give due consideration to the opinions of designating State(s), and State(s) of residence, nationality or incorporation when considering delisting requests" and committee members are called upon "to make every effort to provide their reasons for objecting to such delisting requests."[20]

Annex 2 of this resolution outlines the manner in which the new Ombudsperson will operate. Upon receiving a valid request for delisting, the Ombudsperson shall inform and conduct dialogue with the 1267 Committee, the designating state(s), states(s) of residence, relevant UN bodies including the 1267 monitoring committee and other states deemed relevant by the ombudsperson for a 2 month period to determine their opinion on their petition. A 2 month period of engagement with the petitioner is to follow followed by the Ombudsperson's preparing a report for the 1267 Committee laying out the information obtained and "the principal arguments concerning the delisting request". [21] The Ombudsperson then presents this report to the 1267 Committee. In the end, the 1267 Committee decides the delisting request through its normal procedures. The Ombudsperson then informs the petitioner of the decision, providing to the extent possible publicly releasable information, but also respecting "the confidentiality of Committee deliberations and confidential communications between the Ombudsperson and Member States. "[22]

The guidelines for the work of 1267 Committee contained on its website and updated as of December, 2008 provide that the committee will generally work in closed session, is open to any member state with relevant information and works by consensus with disputes being referred to the Security Council where presumably at least nine

---

[18] Ibid at para 15

[19] Ibid at para 20

[20] Ibid at para 25

[21] Ibid at Annex 2 para 7 (c)

[22] Ibid at Annex 2 para 14

000051

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

members would have to agree and the five permanent members would have a veto. It contemplates that delisting requests will come through the former Focal Point or through the state of residence or nationality.[23]

A December 2009 annual report from the 1267 Committee indicates there were at the end of 2009, 503 individuals and entities on the list. In 2009, 7 entities were added to the list and 10 were delisted, 9 as a result of the ongoing comprehensive review to be completed by June 2010 and 1 as a result of the Focal Point process. Six delisting petitions were still under consideration and 13 such delisting petitions had been denied during the year.[24]

2. Court Decisions and the 1267 Listing Process

A number of court decisions such as the European Court of Justice's *Kadi* decision indirectly comment and review on the 1267 listing process and are reviewed elsewhere in this paper.[25] One decision within the UN system was identified that is relevant and constitutes an indirect challenge to the 1267 process. It is the decision in *Sayadi and Vinck v Belgium*, (1472/2006), CCPR/C/94/D/1472/2006 (2008), of the UN Human Rights Committee. The decision involved Belgian nationals who were added to the 1267 list at Belgium's request in 2002 because of their alleged associations with a convicted al Qaeda member and role in the Global Relief Foundation, a listed group. They were not given the evidence said to support their listing and petitioned the Belgium courts which after three years of investigation declared their innocence of criminal activity. In 2005, Belgium requested that the 1267 Committee delist the individuals but no action had been taken as of the time if the Committee's decision in late December 2008.

The Committee held the petition under the optional protocol to the ICCPR was admissible and that the petitioners were not required to apply to the 1267 Committee for humanitarian exemptions as a means of exhausting domestic remedies.[26] The Committee held that the petitioners were not denied an effective remedy domestically.[27] It also held that the 1267 sanctions regime did not constitute a criminal penalty that triggered the fair trial and legality of penalties provisions of Articles 14 and 15 of the

---

[23] 1267 Committee Guidelines available at http://www.un.org/sc/committees/1267/pdf/1267_guidelines.pdf

[24] S/2009/ 676 at para 11 available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/656/62/PDF/N0965662.pdf?OpenElement

[25] See also *Abdelrazik v. Canada* 2009 FC 580 which is outside of the scope of our terms of reference.

[26] Ibid at 7.4

[27] Ibid at 10.9

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

International Covenant on Civil and Political Rights[28]. It did, however, find Belgium in violation of Article 12 of the ICCPR relating to freedom to travel and Article 17 relating to reputation on the basis that Belgium had initially proposed that the plaintiffs be listed by the 1267 Committee but had later unsuccessfully attempted to have the plaintiffs removed from the list after a criminal investigation resulted in no terrorism prosecution against them. In such circumstances the travel ban was not necessary for national security or public order.[29]

This decision does not directly hold the 1267 process in violation of the ICCPR because it focused on Belgium's conduct and not that of the 1267 Committee or the Security Council. Nevertheless it provides indirect scrutiny of the effects of listing on rights protected under the ICCPR. It suggests that even if listing in the 1267 process is found not to amount to a criminal sanction, triggering the fair criminal trial rights, it can nevertheless affect other rights relating to freedom to travel and reputation.

This decision also featured dissents that concluded that Belgium should not be held in violation of the ICCPR because it was acting pursuant to the mandatory 1267 process. One of these dissents by Sir Nigel Rodney[30], however, expressed some strong criticisms about the fairness of the 1267 listing process as executive action by the Security Council that lacks "the consultation and checks and balances" that would be available at the national level.

---

[28] Ibid paras 10.11. The Committee's reasoning is brief: "Although the sanctions regime has serious consequences for the individuals concerned, which could indicate that it is punitive in nature, the Committee considers that this regime does not concern a "criminal charge" in the meaning of article 14, paragraph 1."ibid at 10.11.

[29] Ibid at para 10.8. The reasoning is again brief: "The Committee therefore finds that, in the present case, even though the State party is not competent to remove the authors' names from the United Nations and European lists, it is responsible for the presence of the authors' names on those lists. The Committee concludes that the facts, taken together, disclose that, as a result of the actions of the State party, there has been an unlawful attack on the authors' honour and reputation. Consequently, the Committee concludes that there has been a violation of article 17 of the Covenant." Ibid at 10.13

[30] Sir Nigel Rodney stated that Belgium "has done what it could to secure the authors' de-listing. In so doing it has provided the only remedy within its power. Accordingly, unless the Committee believes that the State party's mere compliance with the Security Council listing procedure (in the absence of bad faith by the State party or of manifest abuse or overstepping of the Security Council's powers) is capable of itself of violating the Covenant, it is not clear how the authors can still be considered victims, under article 1 of the Optional Protocol, of violations of the State party's obligations under the Covenant. *We acknowledge, of course, that the authors may have been unjustly harmed by operation of the extravagant powers the Security Council has arrogated to itself, including the obstacles it has created to the correction of error. It is more than a little disturbing that the executive branches of 15 Member States appear to claim a power, with none of the consultation or checks and balances that would be applicable at the national level, to simply discard centuries of States' constitutional traditions of providing bulwarks against exorbitant and oppressive executive action.* However, the Security Council cannot be impleaded under the Covenant, much less the Optional Protocol." (emphasis added)

000053

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

3. The Literature on the 1267 Listing Process

Much of the published literature on the 1267 listing process predates recent resolutions and especially Security Council Resolution 1904 reforming the listing process by introducing an Ombudsperson. Nevertheless, this literature still provides some important insights into the listing process and criticisms of this process. In what follows we provide an analysis of legal articles that have examined the 1267 regime. The more recent of these articles also considers recent legal challenges to these process, most notably the European Court of Justice's decision in *Kadi* and analysis of the effects of such judgments on the listing process including the responses of governments to the court decisions. Common themes that emerge from the literature will be discussed below under the heading Discussion/Conclusions.

Cameron, Iain. "UN Targeted Sanctions, Legal Safeguards and the European Convention on Human Rights" (2003) 72 *Nordic Journal of International Law* 159.

This article criticizes the 1267 listing regime as a form of rubber stamping of listing decisions made by individual states often on the basis of intelligence that does not satisfy legal standards of proof. It also expresses concerns that requirements for consensus for delisting will allow states to block legitimate delisting attacks. The author concludes that the listing process violates various domestic fair trial rights but only after examining a number of arguments in favour of the process including the existence of political safeguards and the ability to grant humanitarian exemptions. The author examines the variety of potential challenges to listing decisions noting that most of them except cases of simple mis-identity may require access to intelligence that may be said to support the listing. He suggests that one possible approach is for the 1267 Committee not to list a person unless they face criminal proceedings at the domestic level and then use the domestic forum as a vehicle to allow the listed person to challenge the basis of the listing. One problem, however, is that many listing decisions originate from American sources and the ability to review listing decisions in American courts especially for non-Americans is quite restricted. Another alternative is to allow three judges with experience in intelligence and selected with input from the parties to review listing decisions within the UN framework. Governments, and in particular the American government, might still, however, be unwilling to reveal sensitive intelligence to such a body. A final alternative is simply to allow individual sanctions to be applied and challenged at the domestic level.

Rosand, Eric. "The Security Council's Efforts to Monitor the Implementation of the Al Qaeda/Taliban Sanctions" (2004) 98 A.J.I.L. 745.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

This 20 page article examines the 1267 Committee in the context of other counter-terrorism work by the Security Council. It suggests that the committee work has focused on issues of compliance. It describes how names with little supporting information were added to the list and accepted by other members of the Security Council on the basis of "political trust"[31] as well as the need to protect intelligence from disclosure. It describes how almost 200 names were added to the list in the aftermath of 9/11 and largely at the request of the United States. It describes the attempts of the Swedish government to have citizens associated with Al Barakaat removed from the list. Concerns are raised about the listing of people who are not associated with Al Qaeda and a reluctance to list those associated with Al Qaeda for political reasons at the domestic level of member states. The criticisms made by a monitoring team about the failure of some states to freeze assets of those on the list without domestic judicial findings are reviewed as is Resolution 1526 which called for increased vigilance with respect to terrorist financing through charities and informal banking systems. It also noted that the monitoring team advocated greater distribution of the 1267 list to increase the effectiveness of its arms embargo, travel ban and asset freeze. It also discusses attempts to encourage states to report to the 1267 Committee and possibilities for combining the reporting and monitoring work of the Counter-terrorism committee created by Resolution 1373 and the 1267 Committee. The article characterizes the task of increasing co-operation of the states as "perhaps the committee's biggest challenge".[32] A second challenge identified is the need to maintain the credibility of the list by requiring states to both list individuals and to provide supporting information as well as to respond with due process to requests for removal from the list.

Gutherie, Peter. "Security Council Sanctions and the Protection of Individual Rights" (2004) 60 *NYY Annual Survey of American Law* 491.

This article suggests that the 1267 regime does not accord with fair trial norms including those relating to property and due process. It suggests that the only parallel to the individual sanctions in the 1267 regime are the courts created for Rwanda and the former Yugoslavia. The 1267 regime, however, unlike those courts does not apply judicial procedures before imposing the individual sanctions which may amount to criminal punishment. It notes that when the listing of three Somali were challenged by Sweden, the United States produced material in an unsuccessful attempt to support the

---

[31] Eric Rosand "The Security Council's Efforts to Monitor the Implementation of the Al Qaeda/Taliban Sanctions" (2004) 98 A.J.I.L. 745 at 748

[32] Ibid at 759

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

listing that contained 27 pages, 23 of which were news reports.[33] It also suggests that the 1267 Committee cannot provide a full or impartial review of listing decisions it originally made.[34] It discusses but ultimately rejects the idea of dismantling the regime and leaving listing and freezing of assets to domestic jurisdiction as not effective enough in preventing terrorism financing. It also discusses and ultimately dismisses the prospect of creating an international body under UN auspices to review listing decisions as politically implausible given the reluctance of governments, especially the American government, to share the secret intelligence that often lies behind the listing decisions. It favours a third process where the 1267 Committee becomes more sensitive to decentralized review of listing decisions at the domestic and regional level. This would allow sensitive intelligence to be dealt with domestically while also subjecting listing decisions to adversarial challenge.

Fassbender, Bardo. *Targeted Sanctions and Due Process* (March 2006).

This 32 page report was commissioned by the UN Office of Legal Counsel. This study stresses the need for the Security Council to adopt fair procedures given the absolute immunity of the Security Council from domestic challenge under Article 105 of the UN Charter. It argues that there are legitimate expectations that a listed person will be heard and have a right to an effective remedy when being listed in the 1267 regime even if the UN Security Council is not directly subject to human rights norms.[35] It argues that the Security Council has an obligation to ensure that the listing process is necessary and proportionate to the important ends it pursues. [36] It outlines competing conceptions of the listing process as either legislation or penalties and outlines a variety of methods including independent judicial review, Ombudsperson, committee of experts, an inspection panel and a commission of inquiry to ensure better fairness in the listing and delisting process.

Watson Institute of Brown University, *Strengthening Targeted Sanctions Through Fair and Clear Procedures* (March 2006).

This 60 page report accepts the use of targeted sanctions against individuals by the UN and situates the 1267 regime in the context of other targeted sanctions used by

---

[33] Peter Gutherie "Security Council Sanctions and the Protection of Individual Rights" (2004) 60 NYY Annual Survey of American Law 491 at 512

[34] Ibid at 514

[35] Bardo Fassbender *Targeted Sanctions and Due Process* March 2006 at para 1.17

[36] Ibid at 11.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the Security Council including in respect to Sierra Leon, Iraq, Liberia, Congo, Lebanon/Syria and Cote de Ivoire. Nevertheless, the report argues for several reforms to improve the fairness of the 1267 listing regime and in particular its compliance with the right to a fair trial and the right to an effective judicial remedy. These reforms include providing where possible notice to listed individuals including a redacted version of the reasons for the listing. It also proposed a focal point, time limits and greater transparency for the delisting process as well as biennial reviews of the 1267 listing. It also examines the options for review of listing decisions including a monitoring team, an advisory review panel of experts, an Ombudsperson, a binding arbitration panel and direct judicial review of listing by a UN administrative tribunal or court. It concluded that only the last two options of direct review by a UN administrative tribunal or court would satisfy concerns about a fair trial and a right to an effective remedy.[37] This 2006 report noted that no domestic or regional court had yet invalidated a listing decision, but warned of this possibility if reforms to the listing and delisting process were not made.

Watson Institute of Brown University *Addressing Challenges to Targeted Sanctions: An Update of the "Watson Report"* (October, 2009).

This 58 page update of the 2006 report predicts that without change the ability of the 1267 Committee to issue targeted sanctions "will be severely compromised"[38] by various human rights challenges. It notes that while the Security Council has imposed individual sanctions in other contexts that the 1267 Committee has by far targeted the most individuals of all Security Council bodies. It reports that 30 legal challenges have been made in various domestic courts around the world with 16 pending cases as of the time of the writing of the report.[39] It concludes that while the 1267 regime attempts to deter and prevent terrorism that "the growing negative reaction to targeted sanctions for counter-terrorism purposes, however, risks the further erosion of the credibility and future utility of the instrument of multilateral sanctions in general."[40] The report provides helpful descriptive chapters outlining both the changes to the 1267 process and the various legal challenges to it to date. It concludes that the reforms to date still "do not deal with the need for an effective remedy in the case of a wrongful application

---

[37] Watson Institute of Brown University *Strengthening Targeted Sanctions Through Fair and Clear Procedures* March 2006 at 49.

[38] Watson Institute of Brown University *Addressing Challenges to Targeted Sanctions: An Update of the "Watson Report"* October, 2009 at 5

[39] Ibid at 7

[40] Ibid at 11

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

of a targeted sanction."[41] In terms of remedy, the report draws distinctions between those that will improve the listing and delisting procedure itself, those that will respond to national or regional review of listing decisions and those that will provide independent review within the UN of listing decisions. With respect to the later, the report suggests that while an ombudsperson would be easier to implement, a panel of impartial advisors "would likely be perceived as more independent".[42]

van den Herik, Larissa. "The Security Council's Targeted Sanctions Regimes: In Need of Better Protection of the Individual," (2007) 20 *Leiden Journal of International Law* 797.

This 11 page article examines the 1267 listing process in light of various decisions by European courts of first instance involving the listing of those associated with al Qaeda and the Taliban. It examines the rise of UN sanctions targeted against individuals and argues that effective judicial review of such sanctions is required. The appropriate forum for such review, it is suggested, would by the International Court of Justice applying *jus cogens* norms, but that such review is precluded by the fact that individuals do not have standing before the International Court of Justice. Debates about whether the 1267 sanctions are administrative sanctions or criminal sanctions are noted. Reforms to the 1267 process are examined with the author suggesting that they still fail to provide the wrongly listed with an effective remedy. It is suggested that if the Security Council wishes to continue to use targeted sanctions against individuals, it must accommodate a degree of due process that will allow secret intelligence to be disclosed to those challenging listing decisions.

Hudson, Andrew. "Not a Great Asset: The UN Security Council's Counter-Terrorism Regime: Violating Human Rights," (2007) 25 *Berkeley Journal of International Law* 203.

This article argues that the 1267 listing process violates fair trial rights as contained in the purposes of the UN Charter and *jus cogens*. It focuses on the lack of a hearing before either listing or delisting. It proposes a variety of reforms including requiring countries to forward all delisting requests to the 1267 Committee and providing a UN tribunal to decide delisting applications. It concludes that "in reality, it is unlikely that the Security Council would approve an independent tribunal with the

---

[41] Ibid At 22

[42] Ibid at 32

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

binding powers to de-list individuals."[43] It then focuses on various advisory bodies such as an ombudsperson and inspection panels.

Foot, Rosemary. "The United Nations, Counter-Terrorism and Human Rights: Institutional Adaptation and Embedded Ideas,"(2007) 29 *Human Rights Quarterly* 489.

This article suggests that both the initial work of the 1267 Committee as well as the Counter-Terrorism Committee created by Security Council Resolution 1373 neglected human rights concerns. It then suggests, however, that both committees have become more sensitive to human rights concerns in part because of various criticisms of their neglect of human rights both within and outside the UN. With respect to the 1267 Committee, the author notes the work of various European governments and the prospects of successful domestic due process challenges.[44] She concludes that even Security Council committees can become more sensitive to human rights despite the fact that three of the permanent members of the Security Council, China, Russia and the United States, have not been overly sympathetic to human rights concerns in these areas.

Farrall, Jeremy Matam. *United Nations Sanctions and the Rule of Law* (Cambridge University Press, 2007).

This book examines the broad range of UN Sanctions against states and individuals. It argues that the transparency of sanctions committees should be increased as should their commitment to the rule of law. With respect to the 1267 Committee, the author concludes that while recent attempts to clarify the process "is welcome" that what is striking about the delisting procedure is that listed individuals have no capacity to address the relevant committee directly to present their concerns and protest their innocence. They must rely upon a sponsor government, which, if it can be convinced to proceed with the case, must then effectively rely upon the good will of the state that originally suggested the individual be listed, in order for the matter to proceed to the committee." He thus concludes that reforms to the listing process contained in SC Resolution 1730 seem "to provide a recipe for how to reject rather than take seriously any requests for delisting."[45]

---

[43] Andrew Hudson "Not a Great Asset: The UN Security Council's Counter-Terrorism Regime: Violating Human Rights" (2007) 25 Berkeley Journal of International Law 203 at 226

[44] Rosemary Foot "The United Nations, Counter-Terrorism and Human Rights: Institutional Adaptation and Embedded Ideas" (2007) 29 Human Rights Quarterly 489 at 505

[45] Jeremy Matam Farrall *United Nations Sanctions and the Rule of Law* (Cambridge University Press, 2007) at 222

000059

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Johnstone, Ian. "Legislation and Adjudication in the UN Security Council: Bringing Down the Deliberative Deficit," (2008) 102 *American Journal of International Law* 275.

Drawing on various theories of deliberative democracy, this article argues that the 1267 listing regime which allows listing in the absence of objection from member states and allows member states to object and effectively veto a delisting request fails to foster deliberation about listing or delisting decisions. It suggests that the failure to engage in deliberation can adversely affect the accuracy of the decision or full consideration of the impact of a particular listing decision on affected individuals. The author suggests that "support the for the 1267 regime is continuing to erode" [46] despite some reform efforts and can be seen in a reluctance to create a larger terrorist list pursuant to Resolution 1566 adopted in response to acts of terrorism in Beslan, Russia. He proposes increased consultation with non-members of the Security Council, an individual right to be heard by the 1267 Committee[47] and more public justification of listing decisions as a means of increasing deliberation and accuracy in the work of the 1267 Committee.

Kanetatke, Machiko. "Enhancing Community Accountability of the Security Council Through Pluralistic Structure: The Case of the 1267 Committee," (2008) 12 *Max Planck Yearbook of United Nations Law* 113.

This article surveys the accountability gap within the Security Council with special attention to the 1267 Committee. It notes the various changes including the creation of a Focal Point for delisting petitions but concludes that there are still normative and pragmatic grounds for enhanced accountability. The author concludes that decentralized review through the increasing number of court cases is problematic because many countries will be unwilling to share secret intelligence used to justify listing with other states and domestic courts may not have adequate abilities to examine and safeguard such intelligence. The author favours centralized accountability in the UN including the use of an expert arbitration panel to decide delisting cases, but also notes that countries may still object to the sharing of secret information with such a body.

---

[46] Ian Johnstone "Legislation and Adjudication in the UN Security Council: Bringing Down the Deliberative Deficit" (2008) 102 American Journal of International Law 275 at 296

[47] Ibid at 305

000060

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Meyers, Daniel. "The Transatlantic Divide over the Implementation and Enforcement of Security Council Resolutions," (2008) 38 *California Western International Law Journal* 255.

This article examines the 1267 process as enacted under Chapter VII of the United Nations. It then contrasts a monist European approach which the author suggests renders the 1267 process difficult if not impossible to challenge in European courts with a dualist American approach where any domestic implementation of 1267 listing would depend on an independent act of the executive that could be challenged under American due process norms. The author examines three ongoing cases where such due process challenges had been made in the United States, but had not been successful. He suggests that while improvements to the 1267 listing process such as a right to be heard, to be represented by counsel and to an effective remedy will improve the chances of the listing surviving due process domestic challenges, no improvement will preclude the ability of individuals to challenge the implementation of the listing under domestic systems that have a dualist approach to domestic and international law.

Reich, Johannes. "Due Process and Sanctions Targeted Against Individuals Pursuant to UN Resolution 1267(1999),"(2008) 33 *Yale J of Int Law* 505.

This short note traces the development of the 1267 process as a "barely checked supranational administrative agency".[48] It notes, that while listing is understood as a preventive as opposed to a punitive or criminal process, listing in specific cases can have dramatic effects on individuals that are the equivalent of house arrest. It describes the Focal Point reforms to the delisting process as one that simply informs governments of a request for delisting and facilitates intergovernmental bargaining but does not engage "in fact-finding nor in applying laws."[49] It argues that domestic refusal to apply the 1267 listing would infringe the supremacy of the UN Charter and inhibit the ability to take collective measures against terrorism. It then argues that it is necessary for the 1267 process to be reformed both by independent review by independent experts within the UN framework and by placing time limits on any listing so as to justify "the listing decision being based upon prima facie evidence not necessarily meeting the standards of criminal proceedings" and to "provide incentives to launch formal criminal investigations and criminal proceedings in absentia if unavoidable."[50]

---

[48] Johannes Reich "Due Process and Sanctions Targeted Against Individuals Pursuant to UN Resolution 1267 (1999)" (2008) 33 Yale J of Int Law 505 at 505

[49] Ibid at 507

[50] Ibid at 511

000061

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Boothe, Michael. "Security Council's Targeted Sanctions Against Presumed Terrorists," (2008) 6 *Journal of International Criminal Justice* 541.

This article argues that the lack of a formal judicial mechanism within the UN to hear challenges to individual sanctions is a fundamental problem for the UN system. The article stresses the need to allow listed persons to know and challenge the basis for the listing. It examines various means of improving the listing process such as inspection panels used by the World Bank and suggests that such a procedure might provide a basis for individual and transparent review of the 1267 process.

Lopez George A. et al, *Overdue Process: Protecting Human Rights while Sanctioning Alleged Terrorists*, A Report to Cordaid from the Fourth Freedom Forum and Kroc Institute for International Peace Studies at the University of Notre Dame (April 2009).

This 30 page report argues that the 1267 listing process and other related processes have led to "serious concerns about violations of human rights and limitations on the work of civil society groups". [51] It characterizes the reforms made by Resolutions 1730 (2006), 1735 (2006) and 1822 (2008) as "modest improvements" that "still do not meet fundamental human rights standards which include the right to judicial review, the right to procedural fairness, the right to be heard and the right to judicial remedy."[52] It concludes that the focal point for review "does not constitute an independent review mechanism"[53]. It concludes that reform of the listing process is a quandary because reforms that would satisfy the requirements for judicial review such as a binding arbitration review are not likely to be accepted by Permanent Members of the Security Council while more incremental reforms such as advisory review or an advisory Ombudsperson are not likely to satisfy human rights requirements or provide effective judicial review. The report identifies both the need to protect sensitive intelligence and a desire to preserve the Security Council's powers to make listing decisions as almost insurmountable obstacles to meaningful reforms that would make the process compliant with human rights standards. This report contains helpful appendices outlining the main changes made to the listing process and the main reports on the 1267 process.

---

[51] George A Lopez et al, *Overdue Process: Protecting Human Rights while Sanctioning Alleged Terrorists* (April 2009) at 1

[52] Ibid at 2

[53] Ibid at 5

000062

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Michaelsen, Christopher. '*Kadi and Al Barakaat v Council of the European Union and Commission of the European Communities:* The Incompatibility of the United Nations Security Council's 1267 Sanctions Regime with European Due Process Guarantees' (2009) 10 *Melbourne Journal of International Law* 330.

This 18 page case note examines the European Court of Justice's *Kadi* decision in light of the 1267 listing regime. It argues that the focal point in the committee does not provide listed persons with the right to be heard and "does not operate as an independent review mechanism."[54] The author concludes that the listing process still violates rights to judicial review, procedural fairness and an effective remedy that form "the very basis of due process of law" as guaranteed by the Universal Declaration, the ICCPR, the African Charter and the American Convention on Human Rights.[55] *Kadi* is interpreted as confirmation that the intergovernmental and diplomatic nature of the delisting process does not provide a real opportunity to assert rights.[56] The article predicts that *Kadi* will be influential legally and politically and that it will support increased challenges to the 1267 process.

Godinho, Jorge. "When Worlds Collide: Enforcing UN Asset Freezes in EU Legal Order," (2010) 16 *European Law Journal* 67.

This article examines the 1267 regime and suggests that sanctions against individuals as opposed to states constitutes a "mutation"[57] of the UN sanctioning regime and the development of "an ad hoc criminal procedure".[58] It stresses that judicial review of listings under the 1267 process is not possible in the UN regime because of limits on jurisdiction of the International Court of Justice and characterizes present procedures for delisting as "diplomatic" in nature and reforms as "relatively minor"[59]. It also criticizes the permanent nature of the listing process and argues that it constitutes a confiscation of property. It proposes that all listing be made temporary for a period of a year so as to allow domestic judicial process to ensure due process with respect to the final confiscation of the assets that are frozen.

---

[54] Christopher Michaelsen, '*Kadi and Al Barakaat v Council of the European Union and Commission of the European Communities:* The Incompatibility of the United Nations Security Council's 1267 Sanctions Regime with European Due Process Guarantees' (2009) 10 *Melbourne Journal of International Law* 330 at 333

[55] Ibid at 334

[56] Ibid at 342

[57] Jorge Godinho "When Worlds Collide: Enforcing UN Asset Freezes in EU Legal Order" (2010) 16 European Law Journal 67 at 73

[58] Ibid at 77

[59] Ibid at 83

000063

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Formuth, Peter. "The European Court of Justice Decision in Kadi and the Future of UN Counterrorism Sanctions," (2009) 13(20) ASIL Insights.

This article characterizes the *Kadi* decision as a major challenge to the 1267 regimes use of sanctions against individuals. It notes that in light of the European Court of Justice's decisions, a narrative summary of reasons was provided to the plaintiffs in *Kadi* and they were again listed commencing new litigation in the Court of First Instance. It suggests that while the 1267 regime has added procedural protections over the years that its reliance on secret intelligence limits the degree to which major powers will be willing to accept more significant reforms that would give listed persons a meaningful right to contest their listing. It suggests that European proposals to make the 1267 listing provisional and allow rescinding of listing if they were successfully challenged would run afoul of the mandatory nature of the 1267 regime. It suggests the need for fundamental reforms to the 1267 regime such as making listings provisional and subject to in camera review and ratification by jurists within the UN system.

Gurule, Jimmy. "The Demise of the UN Economic Sanctions Regime to Deprive Terrorists of Funding," (2009) 41 *Case Western Reserve J. of Int. Law* 19.

This article suggests the 1267 regime is at a critical juncture and is "failing"[60] because of due process challenges such as the *Kadi* litigation and the declining number of individuals being added to the list since the immediate aftermath of 9/11. It criticizes a reluctance by domestic states to take steps to implement the listing even while both Al Qaeda and the Taliban remain a terrorist threat. It notes that the asset freeze imposed in Security Council Resolution 1373 is broader than the 1267 regime because it applies to all terrorists and is administered domestically without the keeping of a UN list. The author suggests that listing can be justified as a preventive measure on reasonable grounds to believe as opposed to proof to guilt beyond a reasonable doubt and that the Consolidated 1267 list reads as a "Who's Who of Islamic terrorists."[61] He also notes the ability of the 1267 Committee to grant humanitarian exemptions from asset freezes suggests that listing should be viewed as preventive and not as punishment.[62] It also notes the practice of joint submissions by member states for listing such as the actions of Australia, Indonesia, Philippines, Singapore and the United States in their joint

---

[60] Jimmy Gurule "The Demise of the UN Economic Sanctions Regime to Deprive Terrorists of Funding" (2009) 41 Case Western Reserve J. of Int. Law 19 at 55

[61] Ibid at 39

[62] Ibid at 44

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

designation of Jemaah Islamiyah after the Bali bombings.[63] The author concludes that the failure of the 1267 regime to lead to more listings and freezing is largely a failure of political will as opposed to concerns about capacity or due process.

Keller, Helen and Andreas Fisher "The UN Anti-Terror Sanctions Regime under Pressure" (2009) 9 *Human Rights Law Review* 257.

This article notes improvements in the 1267 regime such as the Focal Point and review process but still concludes that it violates fairness standards whether listing is characterized as administrative, civil or criminal in nature. It then examines *Sayadi and Vinck v Belgium*[64] a decision of the Human Rights Committee holding that Belgium's actions in listing the plaintiffs violated both freedom of travel and reputation guarantees under the ICCPR even though it did not constitute criminal sanctions. It notes the dilemma caused by states that can be in breach of human rights guarantees by complying with the 1267 process but also in breach of Chapter VII of the United Nations Charter if they do not comply with the regime.

Michaelson, Christopher. "The Security Council Al Qaeda and Taliban Sanctions Regime: 'Essential Tool' or Increasing Liability in the UN's Counterterrorism Efforts?" (2010) 33 *Studies in Conflict and Terrorism* 448.

This article examines both the 1267 regime and the effects of the *Kadi* decision. It highlights the preventive role of 1267 listing while concluding that the freezing of assets has a punitive effect on individuals and for that reason has attracted due process challenges such as that in *Kadi*. It indicates that as of January 2010, 256 individuals were listed as associated with al Qaeda and 137 were listed as associated with the Taliban. It concludes that while the best reform to 1267 reform would be one based on independent review that such a reform "appears almost impossible to achieve"[65] because of concerns about preserving Security Council decision-making power and the confidentiality of intelligence used by nations to support the listings. It suggests that closed proceedings with security cleared counsel would be necessary to protect the confidentiality of intelligence. The article also examines Security Council Resolution 1904 which replaces the focal point approach with an independent and impartial

---

[63] Ibid at 40

[64] (1472/2006), CPR/C/94/D/1472/2006 (2008); 16 IHRR 427 (2009). This case is examined above.

[65] Christopher Michaelson "The Security Council Al Qaeda and Taliban Sanctions Regime: 'Essential Tool' or Increasing Liability in the UN's Counterterrorism Efforts?" (2010) 33 Studies in Conflict and Terrorism 448 at 455

000065

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Ombudsperson to assist applicants and to submit confidential recommendations to the committee. The author concludes that the Ombudsperson "constitutes a significant improvement" but one that is unlikely to fulfill "international obligations of effective due process" because the Ombudsperson depends on a state's volunteering the intelligence that lies behind the listing decision and because it only makes recommendations to the 1267 Committee, thus failing to provide effective remedies for those who are wrongfully listed.

C. Discussion and Conclusions

Categorization of the Literature

The literature on the 1267 listing process suggests that legal experts who have written in the area are generally critical of the listing process and some are pessimistic about the possibility that reforms to the listing process can satisfy international or domestic fair trial process. Most of the authors take the listing system as a given and few address the question of whether listing in any form is a bad idea. A few authors such as Rosand and Gurule can be seen as supportive of listing to the extent that they focus on lack of domestic compliance with the listing regime and its accompanying asset and travel bans. A number of authors such as Fassbender, Van den Herik, Reich, and Keller and Fisher stress that despite concerns about the lack of due process in listing, that listing still imposes mandatory obligations on states because Resolution 1267 was enacted under the mandatory provisions of Chapter VII of the United Nations Charter. Hudson considers but rejects the idea that the UN should withdraw from listing. A few authors such as Cameron and Meyers seem skeptical about whether there will ever be satisfactory reforms and stress that domestic challenges to listings will still continue. Much of this literature proposes various reforms to the listing processes and it is perhaps possible to infer from such reform proposals that the authors conclude that listing is salvageable. A number of authors such as Hudson, Foote, Farrall and Johnstone either note that the listing regime has improved over the years or is capable of improvement, but others such as Lopez and Michaelson seem skeptical about whether the Security Council and the 1267 Committee would give an independent adjudicatory body the power or access to secret intelligence that in their view would be necessary to provide due process to those who are listed.

1. Early Literature

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The earlier literature on the listing process, like the process itself, focused on compliance issues. Many of the earlier articles placed the 1267 listing process in the context of an increased use by the Security Council of targeted sanctions against individuals. The original 1267 resolution targeted only the Taliban as the *de facto* government of Afghanistan, but this focus was changed as subsequent resolutions included those associated with bin Laden and Al Qaeda. They also defined the criteria for being associated with Al Qaeda broadly. The early literature was aware that the 1267 list had been dramatically expanded at the request of the United States in the wake of 9/11 and that some countries were unwilling to propose that people be added to the list in part because of concerns about the fairness of the process used to compile the list.[66]

2. Post-2006 Literature

Starting in 2006, there was a definite trend as the literature on the 1267 listing process increasingly focused on due process concerns. [67] Notable here is the Fassbender report commissioned by the UN Office of Legal Counsel and the first report by the Watson Institute of Brown University. This literature noted that no domestic or regional court had at that time directly or indirectly invalidated a listing decision, but clearly contemplated the possibility of such successful challenges. This literature also surveyed a variety of reforms that could (and in some cases have subsequently) been made to the 1267 process. These reforms included greater use of monitoring teams or inspection or advisory panels or Ombudspersons as well as direct review of listing decisions by an independent tribunal or court.

The 2006 Watson Institute report is important for its conclusion that only direct review by a tribunal or court within the UN process would satisfy domestic or international standards of a fair trial and a right to an effective remedy. Many other experts have subsequently agreed with such a conclusion and this accounts for a great degree of the pessimism in the literature about the possibility of reforming the 1267 listing process. Most experts recognize the ability of reforms such as the Focal Point or Ombudsperson processes to make the delisting process more transparent, but the

---

[66] Eric Rosand "The Security Council's Efforts to Monitor the Implementation of the Al Qaeda/Taliban Sanctions" (2004) 98 A.J.I.L. 745. For a more recent article that also focuses on compliance issues see Jimmy Gurule "The Demise of the UN Economic Sanctions Regime to Deprive Terrorists of Funding" (2009) 41 Case Western Reserve J. of Int. Law 19.

[67] A notable exception before that time was Iain Cameron "UN Targeted Sanctions, Legal Safeguards and the European Convention on Human Rights" (2003) 72 Nordic Journal of International Law 159 which was prescient in its recognition of the flaws in the 1267 listing process and the difficulties of reforming a process based in large part on secret intelligence and intergovernmental diplomacy. See also Peter Gutherie "Security Council Sanctions and the Protection of Individual Rights" (2004) 60 NYY Annual Survey of American Law 491 raising similar concerns and arguing that the 1267 Committee should become receptive to domestic challenges of listing decisions.

000067

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

consensus of experts is that such processes will not provide a listed person or entity with a fair hearing because it does not allow them to make representations before the 1267 Committee as the decision-maker or to see and challenge the information that the 1267 Committee uses to make its decision to list the person. These concerns emerge as the "bottom line" in much of the literature. In addition, most commentators also conclude that members of the Security Council will be unwilling to cede either decision-making power over listing or disclose all the secret intelligence that may lie behind the listing to an independent tribunal or court.

One notable alternative to the idea that the UN itself must be able to devise some new structure that allows a fair hearing when a listing is challenged is a strand of thought that focuses on the interaction between the 1267 listing processes and those of domestic jurisdictions. Iain Cameron first proposed such an approach when he contemplated in 2003 that UN listings could be subject to review in domestic courts and that domestic courts could develop their own procedures for reconciling the need to treat a listed person fairly with the need to ensure the confidentiality of sensitive intelligence.[68] Cameron, however, expressed some reservations about the ability of American courts to provide effective review of listing provisions. Nevertheless, the idea that the 1267 Committee should become attentive to domestic challenges and that domestic challenges may be better suited than UN processes to reconcile the competing interests in secrecy and effective challenge of listing decisions is an important strand in the literature.

There have, however, been some criticisms of the idea that domestic proceedings could be used to challenge the 1267 listing process. As noted above, Professor Cameron expressed reservations about whether some states would allow a full challenge to the listing decision and especially the secret intelligence that might support the listing. The capacities of domestic states to fulfill this challenge function will vary and both home and foreign governments may resist attempts to have intelligence disclosed in such proceedings.[69]

Others criticized the prospect of relying on domestic challenges to the 1267 listing process on a more formalist basis that stresses the mandatory nature of the 1267 process enacted under Chapter VII of the UN Charter. Such an approach has also been criticized by some as contemplating that domestic and regional courts would annul

---

[68] Iain Cameron "UN Targeted Sanctions, Legal Safeguards and the European Convention on Human Rights" (2003) 72 Nordic Journal of International Law 159 ; See also Peter Gutherie "Security Council Sanctions and the Protection of Individual Rights" (2004) 60 NYY Annual Survey of American Law 491.

[69] Machiko Kanetatke "Enhancing Community Accountability of the Security Council Through Pluralistic Structure: The Case of the 1267 Committee" (2008) 12 Max Planck Yearbook of United Nations Law 113

000068

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

listings, thereby arguably placing that nation in nonconformity with 1267 international obligations.[70]

One possible response to such objections would be that the UN 1267 listing process could be made temporary to allow various domestic authorities time to investigate a listed person and to take various domestic actions against the listed person that could accord with domestic fairness standards in a manner not found in the 1267 process.[71] Implicit in this would be that the 1267 listing would expire or be repealed should the domestic process find that the grounds for listing as a terrorist had not been validated by some domestic prosecution or asset freeze or forfeiture proceeding. Such an approach might allow the 1267 process to retain its mandatory character but it would make listings temporary.

There is one school of thought, as represented in the Fassbender report, that stresses that the work of the 1267 Committee is immune from domestic challenge because it was pursued under Chapter VII of the UN Charter. Even those who maintain such positions, however, concede that the 1267 Committee is bound by *jus cogens* and other fairness norms. In any event, the literature after the *Kadi* decision seems to be less concerned about these questions. Another theme inspired by international law is the idea that dualist systems may allow more domestic court challenges to 1267 listings than monist systems.[72] Again, this distinction is much less important after the *Kadi* decision, a judgment arising in a European context where monism is more common.

3. Critique of the Literature

There are some shortcomings in the literature on the 1267 process. Most of the literature focuses on fairness concerns and the issue of the effectiveness or lack thereof of listing is under-researched. For example, we found no research that examines the 1267 listing process in light of the changing nature of Al Qaeda or that provides case studies of 1267 listing that have facilitated successful enforcement efforts. The literature thus does not grapple with the oft-noted observation that Al Qaeda's central structure has eroded and that Al Qaeda has become something akin to an ideology. We have found no discussion of the reference in Resolution 1904 that the 1267 process should be applied to those "otherwise supporting acts or activities of Al-Qaida, bin Laden or the

[70] Peter Formuth "The European Court of Justice Decision in Kadi and the Future of UN Counterrorism Sanctions" (2009) 13(20) ASIL Insights available at http://www.asil.org/insights091030.cfm

[71] Johannes Reich "Due Process and Sanctions Targeted Against Individuals Pursuant to UN Resolution 1267 (1999)" (2008) 33 Yale J of Int Law 505.

[72] Daniel Meyers "The Transatlantic Divide over the Implementation and Enforcement of Security Council Resolutions" (2008) 38 California Western International Law Journal 255; Andrew Hudson "Not a Great Asset: The UN Security Council's Counter-Terrorism Regime: Violating Human Rights" (2007) 25 Berkeley Journal of International Law 203.

000069

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Taliban or any cell, affiliate, splinter group or derivative thereof".[73] There is some discussion in the literature of cases of those who have been delisted under the 1267 process,[74] but again there is a need for more detailed case studies. We also found no literature that dealt with the effects of attempts to provide public narrative summaries to justify the listing.

Another shortcoming in the literature is that with a few exceptions it does not examine how the desire of states to keep intelligence secret places limits on what information can be disclosed to a listed person either through the narrative summary of listings that are placed on the 1267 Committee's website or in response to a petition for delisting. An examination of the narrative summaries that have been posted on the 1267 Committee's website suggest that listings are typically justified in conclusory and unsourced terms.[75] Without more disclosure of the reasons for listing including the

---

[73] UN Security Council Resolution 1904 (2009) at para 2 available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/656/62/PDF/N0965662.pdf?OpenElement

[74] See for example E. Alexandra Dosman "For the Record: Designating 'Listed Entities' for the Purpose of Terrorist Financing Offences in Canada" (2004) 62 U.T.Fac.L.Rev. 1

[75] The first narrative summary of a person listed as an Al Qaeda associate provides as follows:

QI.A.15.01. MAHFOUZ OULD AL-WALID

Date on which the narrative summary became available on the Committee's website: 08.07.2009

Mahfouz Ould al-Walid was listed on **6 October 2001**, pursuant to paragraph 8 (c) of resolution 1333 (2000) as being associated with Al-Qaida, Usama bin Laden or the Taliban for "participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of" Al-Qaida (QE.A.4.01).

Additional information:

Mahfouz Ould al-Walid was a senior Al-Qaida (QE.A.4.01) leader who followed Usama bin Laden (QI.B.8.01) from Sudan to Afghanistan in the late 1990s. He has performed several roles within Al-Qaida: spiritual leader, legal scholar and operational planner. In 2001, Mahfouz Ould al-Walid was a close associate and strong supporter of the Taliban.

The last summary provides:

QI.A.282.10. QASIM YAHYA MAHDI AL-RIMI

Date on which the narrative summary became available on the Committee's website: 11 May 2010

Qasim Yahya Mahdi al-Rimi was listed on **11 May 2010** pursuant to paragraph 2 of resolution 1904 (2009) as being associated with Al-Qaida, Usama bin Laden or the Taliban for "participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of ", "supplying, selling or transferring arms and related materiel to", " recruiting for", and "otherwise supporting acts or activities of " Al-Qaida (QE.A.4.01) and Al-Qaida in the Arabian Peninsula (QE.A.129.10).

Additional information:

Qasim Yahya Mahdi al-Rimi is Al-Qaida in the Arabian Peninsula's (AQAP) (QE.A.129.10) senior leader for terrorist operations. He was sentenced to five years in prison in 2005 after being convicted in Yemen

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

human sources and methods used to obtain the information, the ability of a listed person to challenge the listing before either the 1267 Committee or even some independent body might be illusory. Without such information, there is no way to evaluate the reliability of the information that is used to justify the listing. For example, it would be extremely relevant to reliability whether a person was identified as associated with Al Qaeda by multiple or single sources and under what circumstances, including the possibility of torture, mistreatment or even reward, that the sources provided the information. There is simply no way of gleaming that information from the narrative summaries. The countries that supply the information may, of course, have important reasons for not disclosing the methods and sources used to obtain the information.

The literature that we have identified on the 1267 process only engages with the secrecy versus disclosure dilemma with respect to the intelligence and grounds for the listing in a superficial manner. For example, there have been assertions that effective challenge of listing will require full disclosure of the basis for the listing,[76] but this is not likely to be viable given the desire of states to protect some of the sources and methods used to obtain the information. Alternatively, there has been a suggestion that any effective proceeding for challenging listings or for hearing delisting procedures would

---

of plotting to assassinate the United States Ambassador to Yemen. He, along with AQAP's current emir, Nasir 'abd-al-Karim 'Abdullah al-Wahishi (QI.A.274.10), escaped from prison in Yemen in 2006.

Since his escape, Al-Rimi has played a key role in reviving the regional node of Al-Qaida (QE.A. 4.01). In 2007, he and Al-Wahishi announced the emergence of Al-Qaida in Yemen (AQAP's predecessor) and carried out a July 2007 attack on a convoy of Spanish tourists in Mareb province, Yemen that killed nine people.

Since its creation, AQAP has claimed responsibility for the March 2009 suicide bombings that killed four Korean tourists in Yemen, and is reportedly responsible for the kidnapping of nine foreigners in Yemen, and the execution of three of them, in June 2009. Additionally, AQAP has claimed responsibility for the 25 December 2009 attempted bombing of a Northwest Airlines flight traveling between Amsterdam and Detroit by Umar Farouk Abdulmutallab.

Al-Rimi has played a key operational role and held positions of authority in AQAP and formerly Al-Qaida in Yemen, both of which have publicly claimed responsibility for planning and carrying out assassinations, suicide bombings, and attacks against critical infrastructure with targets including the United States Embassy in Sanaa, tourists, aid workers, Yemeni counterterrorism officials, and oil facilities. Al-Rimi has planned and directed such acts of terrorism. Al-Rimi has also played an important role in recruiting the current generation of militants making up the Yemen-based AQAP.

Available at http://www.un.org/sc/committees/1267/NSQI01501E.shtml

[76] Larissa van den Herik, 'The Security Council's Targeted Sanctions Regimes: In Need of Better Protection of the Individual' (2007) 20 *Leiden Journal of International Law* 797.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

require security-cleared counsel to act on behalf of the listed person.[77] This may be so, but we would note that this raises larger and contested issues about the fairness of the special advocate/security cleared counsel process.

4. Due Process Reform Proposals

In the literature examined, we have found no unqualified defence of the 1267 listing process. Most of this literature predates Security Council Resolution 1904 issued in late 2009 replacing the Focal Point for delisting requests with an Ombudsperson. Nevertheless, the literature that discussed the option of the Ombudsperson before 2009, as well as the literature which takes note of Resolution 1904, still maintains that improvements to the delisting process does not ensure compliance with fairness requirements that would presumptively give the listed person access to an impartial decision-maker and a fair opportunity to know and challenge the basis for a listing. The literature examines the range of options both within and outside of the UN that could provide a fair hearing, but it almost universally expresses reservations about states being willing to reveal confidential intelligence and information that may have supported the listing.

Some of the literature raises the prospect that the 1267 listing could be made temporary or provisional contingent to challenges to listing at the domestic and regional level.[78] The idea here is that the listed individuals or groups may have greater opportunities in domestic courts to challenge listings than are available in the 1267 process. Such proposals are intriguing particular in their conception of complementary roles for UN and domestic review, but they would require some change from the mandatory requirements of the 1267 prospect with respect to freezing the assets and other sanctions on individuals and entities associated with the Taliban, bin Laden and Al Qaeda. The domestic review option, however, is not without its problems. Domestic courts will have varying abilities to hear such challenges and reconcile the competing interests in disclosure and fairness. If the 1267 process does not respond promptly to domestic challenges, a listed person might have concerns about the near impossible task of challenging listing in multiple jurisdictions. In this respect, our inability to find court cases challenging listings in Australia and New Zealand may be significant because they underline the difficulties faced by a person bringing a domestic challenge to listing especially in a small jurisdiction where the government may bring secrecy claims and might oppose delisting requests and appeal successful first instance challenges, if only because of concerns about the need to comply with the 1267 process. Another issue is

---

[77] Christopher Michaelson "The Security Council Al Qaeda and Taliban Sanctions Regime: 'Essential Tool' or Increasing Liability in the UN's Counterterrorism Efforts?" (2010) 33 Studies in Conflict and Terrorism 448

[78] Johannes Reich "Due Process and Sanctions Targeted Against Individuals Pursuant to UN Resolution 1267 (1999)" (2008) 33 Yale J of Int Law 505.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

that domestic challenges will depend on the liability rule established by domestic law which will often be the criminal law relating to terrorism financing in each jurisdiction. The *Sayadi* case decided by the UN Human Rights Committee is notable because the petitioners were able to petition the Belgian courts to determine whether they were criminally liable and that domestic court essentially declared the petitioners to be innocent of involvement in terrorism. Other courts, including those in the Anglo-American world, typically do not make determinations of criminality in the absence of a public prosecutor proceeding with charges and also typically do not make declarations of innocence. The domestic review process will be slow. In some cases, it will require listed individuals to associate themselves with a listed terrorist group in order to establish that the group was not involved in terrorism. In other cases, a person may want to establish that they are not associated with a group without challenging that the particular group is or has been involved in terrorist activities.

Nevertheless, there is a broad consensus in the literature that the 1267 response should become more responsive to domestic challenges and to this end Resolution 1904 asks nation states to inform the 1267 Committee of relevant domestic court decisions.

Review of listing within the 1267 process has the potential to be more efficient for both listed individuals and other nations. It has the potential to nip or correct errors in the bud so to speak and a number of commentators have clearly expressed a preference for a centralized approach that would reform the 1267 process and not rely on decentralized domestic challenges. [79] That said, the consensus in the literature is that the 1267 process has yet to have a review process that will allow the listed person effectively to challenge a listing. Even with the contemplated meetings that would occur between the new Ombudsperson and a person or group seeking delisting under Resolution 1904, the 1267 listing process still remains one that is based on decision-making by governments who themselves may not have full access to the information that is said to support listing a person as associated with Al Qaeda or the Taliban. As many commentators have stressed, those who are listed do not have a judicial remedy within the 1267 process in the sense that they are able to know and challenge the basis for the listing before an independent and impartial decision-maker.

Only one quasi-judicial proceeding has been identified within the UN system that has indirectly challenged the 1267 process. This is not surprising given that individuals or organizations challenging listing decisions would not have standing in the International Court of Justice. The one case identified and decided by the UN Human Rights Committee[80], however, suggests that indirect challenges can be made to

---

[79] Machiko Kanetatke "Enhancing Community Accountability of the Security Council Through Pluralistic Structure: The Case of the 1267 Committee" (2008) 12 Max Planck Yearbook of United Nations Law 113; Johannes Reich "Due Process and Sanctions Targeted Against Individuals Pursuant to UN Resolution 1267 (1999)" (2008) 33 Yale J of Int Law 505.

[80] *Sayadi and Vinck v Belgium* (1472/2006), CCPR/C/94/D/1472/2006 (2008); 16 IHRR 427 (2009),

000073

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the 1267 process. The committee in this case held that listing did not amount to a criminal sanction requiring fair trial rights, but that a listing did, however, violate the petitioner's rights under the ICCPR in relation to travel and reputation. The Committee's holding that the 1267 sanction process does not amount to a criminal sanction might be questioned given the severe consequences of listing that are inherent in the 1267 regime and might be revisited in domestic forums that might play less deference to the mandatory nature of the 1267 process. In any event, Belgium was held in breach of its ICCPR obligations even though it has unsuccessfully attempted to persuade the 1267 Committee to delist the petitioners that it had originally proposed be listed, after a domestic investigation in Belgium had revealed no basis for prosecution of the individuals listed as associated with Al Qaeda. This decision suggests that even the actions of the designating state may not necessarily result in delisting. Moreover, it accepts that listing can have adverse consequence on at least some legal rights even if it does not amount to a criminal sanction. It also reveals the mismatch between the intergovernmental nature of the 1267 Committee and the attempts by individuals to challenge their listing and have their rights protected.

5. Conclusion

In conclusion, two main themes and dilemmas arise from an examination of the large literature on the 1267 process and cases that have challenged the listing process. The first dilemma is the discrepancy between using an intergovernmental and generally confidential process to list and delist individuals and groups as associated with Al Qaeda and the Taliban and the inability of those who are listed to seek a judicial remedy in the process that allows them to know and challenge their listing before an impartial decision-maker. The consensus of the experts in the literature is that only an independent court or tribunal within the UN system can provide such a judicial remedy and that reforms such as the creation of a Focal Point or Ombudsperson may improve the process but will not provide a judicial remedy. Although judicial remedies may be available at the domestic level, the implementation of such domestic remedies could put individual nations in breach of their mandatory obligations under the 1267 process.

The second theme that is apparent in the literature is the dilemma of allowing states to maintain the confidentiality of the information that is said to justify the listing while also using that secret information as a basis for such a listing. It is not clear that reforms to the 1267 process such as the provision of narrative summaries for the basis for listing resolve this dilemma or provide affected individuals with a meaningful opportunity to challenge their listing. Narrative summaries appear to feature unsourced conclusions and assertions. Although such an approach can preserve the confidentiality of intelligence sources and methods, it also makes it impossible to judge

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the reliability of the underlying intelligence and the conclusions that are drawn that the individual or group is actually associated with Al Qaeda or the Taliban.

The two main shortcomings of the 1267 process- the institutional problem of intergovernmental and nonjudicial decision-making and the dilemmas of secret evidence- combine to present formidable obstacles to reforming the 1267 process to respond to the growing number of indirect challenges to this process. In other words, even if the affected person could challenge the listing before an independent body capable of acting judicially, he or she might not be able to make a meaningful challenge in the absence of full disclosure or some equivalent mechanism.

PART TWO: EUROPEAN UNION

A. Methodology

General searches of the following electronic data bases were conducted under the words "listing of terrorists" and "terrorist listings", "terrorist proscriptions" and "individual sanctions" and the EU as well as more specific terms such as "Kadi" and "European Court of Justice" and "terrorism". The databases searched included Social Science Research Network,[81] Hein Online,[82] the Legal Journals index (UK), and Legal Trac as well as searches using Google and Google scholar on the web.

B. Findings

1. Legislation

In the wake of UN Security Council Resolution 1267, the Council of the European Union (EU Council) adopted Common Position 1999/727/CFSP[83] imposing sanctions measures against the Taliban. Article 2 of that instrument specified that "Funds and other financial resources held abroad by the Taliban under the conditions set out in UNSCR 1267 (1999) will be frozen". Subsequently, in February 2000, the EU Council promulgated Regulation No. 337/2000[84], implementing the asset freeze. It did so on the basis of Articles 60 and 301 of the Treaty establishing the European Community (Treaty of Rome). Articles 60 and 301 read, in part:

Article 60

---

[81] Available at http://www.ssrn.com/lsn/index.html

[82] Available at http://heinonline.org.myaccess.library.utoronto.ca/HOL/Welcome?collection=journals

[83] OJ 1999 L 294, p. 1.

[84] OJ 2000 L 43, p. 1

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> 1. If, in the cases envisaged in Article 301, action by the Community is deemed necessary, the Council may, in accordance with the procedure provided for in Article 301, take the necessary urgent measures on the movement of capital and on payments as regards the third countries concerned.

Article 301

> Where it is provided, in a common position or in a joint action adopted according to the provisions of the Treaty on European Union relating to the common foreign and security policy, for an action by the Community to interrupt or to reduce, in part or completely, economic relations with one or more third countries, the Council shall take the necessary urgent measures. The Council shall act by a qualified majority on a proposal from the Commission.

Also of relevance is Article 308:

> If action by the Community should prove necessary to attain, in the course of the operation of the common market, one of the objectives of the Community, and this Treaty has not provided the necessary powers, the Council shall, acting unanimously on a proposal from the Commission and after consulting the European Parliament, take the appropriate measures.

After Security Council Resolution 1333 (2000) (extending the UN sanctioning measures to "Usama bin Laden, his associates or any entities owned or controlled, directly or indirectly, by Usama bin Laden or individuals and entities associated with him including the Al-Qaeda organization"), the EU Council adopted Common Position 2001/154/CFSP,[85] applying additional measures against the bin Laden and his associates and organization and the Taliban and amending Common Position 96/746/CFSP. Article 4 of that document reads:

> Funds and other financial assets of Usama Bin Laden and individuals and entities associated with him as designated

[85] OJ 2001 L 57, p. 1

000076

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> by the UN Sanctions Committee, will be frozen, and funds or other financial resources will not be made available to Usama Bin Laden and individuals or entities associated with him as designated by the UN Sanctions Committee, under the conditions set out in UNSCR 1333 (2000).

Subsequently, and again with reference to Articles 60 and 301 of the Treaty of Rome, the EU Council introduced Regulation No. 467/2001[86] implementing the Common Position. That regulation ultimately included an annex listing persons, entities and bodies named by the UN sanctions committee, under resolution 1267, as amended. The EU Council was empowered to amend this list, in keeping with changes at the UN level, and did so amend on several occasions between its introduction and 2002.

After 9/11 and UN Security Council resolution 1373, the EU Council adopted a further Common Position – Common Position 2001/931/CFSP -- and then regulation -- Regulation No. 2580/2001. These instruments directed financial sanctions and freezing requirements at persons, groups and entities *not* listed by the UN 1267 Committee process. We will refer to this system as the "unilateral" listing process, to distinguish it from the implementation of the UN 1267 Committee sanctioning regime.

After the Security Council adopted resolution 1390 (2002), the EU Council deemed it necessary to align its own legal instruments with the modified UN sanctions regime. It therefore repealed its prior Common Positions on Taliban and Al-Qaeda sanctions, and adopted instead Common Position 2002/402/CFSP. This instrument, and the subsequent Regulation No. 881/2002, continued the financial asset freeze implementing the UN 1267 Committee listing process. Article 2 of the Regulation provides:

> 1. All funds and economic resources belonging to, or owned or held by, a natural or legal person, group or entity designated by the Sanctions Committee and listed in Annex I shall be frozen.
>
> 2. No funds shall be made available, directly or indirectly, to, or for the benefit of, a natural or legal person, group or entity designated by the Sanctions Committee and listed in Annex I.

---

[86] OJ 2001 L 67, p. 1

000077

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> 3. No economic resources shall be made available, directly or indirectly, to, or for the benefit of, a natural or legal person, group or entity designated by the Sanctions Committee and listed in Annex I, so as to enable that person, group or entity to obtain funds, goods or services.

After UN Security Council resolutions 1452 (2003), permitting certain exemptions from asset freezes, the EU Council adopted Common Position 2003/140/CFSP,[87] permitting derogations from the measures imposed by Common Position 2002/402. The EU Council then introduced Regulation No. 561/2003[88] incorporating amendments governing these exceptions into Regulation No. 881/2002. Article 2a of the latter instrument reads, in part:

> 1. Article 2 shall not apply to funds or economic resources where:
>
> (a) any of the competent authorities of the Member States, as listed in Annex II, has determined, upon a request made by an interested natural or legal person, that these funds or economic resources are:
>
> (i) necessary to cover basic expenses, including payments for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums, and public utility charges;
>
> (ii) intended exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services;
>
> (iii) intended exclusively for payment of fees or service charges for the routine holding or maintenance of frozen funds or frozen economic resources; or
>
> (iv) necessary for extraordinary expenses; and
>
> (b) such determination has been notified to the Sanctions Committee; and
>
> (c) (i) in the case of a determination under point (a)(i), (ii) or (iii), the Sanctions Committee has not objected

---

[87] OJ 2003 L 53, p. 62

[88] OJ 2003 L 82, p. 1

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

to the determination within three working days of notification; or (ii) in the case of a determination under point (a) (iv), the Sanctions Committee has approved the determination.

Regulation No. 881/2002 was most recently amended by Regulation No. 1286/2009[89] in December 2009 to include new due process standards in the decision to list persons, groups and entities. This amendment followed the *Kadi* case described below. These due process protections are also discussed below.

The most recent consolidated version of Regulation No. 881/2002 (the 1267 Committee implementation measure) is dated 26-12-2009. The most recent consolidated version of Regulation No. 2580/2001 (the unilateral listing process) is dated 22-12-2007.

2. Court Decisions

a) Caselaw Concerning Implementation of the UN 1267 Listing Process

The legality of Regulation No. 881/2002 was examined by the European Court of Justice in Joined Cases C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the EU and Commission of the EC* (ECJ Judgment), Sept. 3, 2008. These cases were challenges by Mr Kadi and Al Barakaat to their listing under Regulation No. 881/2002. The applicants were unsuccessful in the Court of First Instance.

The European Court of Justice reversed this lower court decision.[90] It held: First, that Articles 60 and 301 of the Treaty of Rome "concern the adoption of measures vis-à-vis third countries, since that concept may include the rulers of such a country and also individuals and entities associated with or controlled, directly or indirectly, by them".[91] The articles do not, however, authorize measures addressed at persons without "any link to the governing regime of a third country. Following the collapse of the Taliban regime, those measures were aimed directly at Usama bin Laden, the Al Qaeda network and the persons and entities associated with them, as they appear in the summary list. They do not, therefore, as such, fall within the ambit of Articles 60 EC and 301 EC."[92]

---

[89] OJ 2009 L 346, p. 42.

[90] In so doing, it also effectively reversed other Court of First Instance cases that had rendered decisions in keeping with *Kadi*, such as Case T-253/02, *Chafiq Ayadi v Council and Commission*, July 12, 2006 and Case T-49/04 *Hassan v Council*, July 12, 2006.

[91] *Kadi* at para. 167.

[92] *Ibid.*

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

On the other hand, the measures did fall within the ambit of Article 308 of the Treaty of Rome. That provision reads: "If action by the Community should prove necessary to attain, in the course of the operation of the common market, one of the objectives of the Community, and this Treaty has not provided the necessary powers, the Council shall, acting unanimously on a proposal from the Commission and after consulting the European Parliament, take the appropriate measures."

Second, the fact that the 1267 listing process constituted an obligation on state parties to the UN Charter was immaterial to the assessment of whether Regulation No. 881/2002 complied with EU law. In the ECJ's words: "the obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness which it is for the Court to review in the framework of the complete system of legal remedies established by the Treaty."[93] The ECJ further held that

> the Charter of the United Nations does not impose the choice of a particular model for the implementation of resolutions adopted by the Security Council under Chapter VII of the Charter, since they are to be given effect in accordance with the procedure applicable in that respect in the domestic legal order of each Member of the United Nations. The Charter of the United Nations leaves the Members of the United Nations a free choice among the various possible models for transposition of those resolutions into their domestic legal order. … It follows from all those considerations that it is not a consequence of the principles governing the international legal order under the United Nations that any judicial review of the internal lawfulness of the contested regulation in the light of fundamental freedoms is excluded by virtue of the fact that that measure is intended to give effect to a resolution of the Security Council adopted under Chapter VII of the Charter of the United Nations.[94]

---

[93] *Ibid* at para. 285.

[94] *Ibid* at paras. 298-299.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Third, Regulation No. 881/2002 did not comply with the fundamental rights protected by EU law, in large measure because of the due process shortcomings of the 1267 listing process:

> 346 It has next to be pointed out that the Council at no time informed the appellants of the evidence adduced against them that allegedly justified the inclusion of their names for the first time in Annex I to the contested regulation and, consequently, the imposition of the restrictive measures laid down by the latter.
>
> ...
>
> 348 Because the Council neither communicated to the appellants the evidence used against them to justify the restrictive measures imposed on them nor afforded them the right to be informed of that evidence within a reasonable period after those measures were enacted, the appellants were not in a position to make their point of view in that respect known to advantage. Therefore, the appellants' rights of defence, in particular the right to be heard, were not respected.
>
> 349 In addition, given the failure to inform them of the evidence adduced against them ..., the appellants were also unable to defend their rights with regard to that evidence in satisfactory conditions before the Community judicature, with the result that it must be held that their right to an effective legal remedy has also been infringed.
>
> 350 Last, it must be stated that that infringement has not been remedied in the course of these actions. Indeed, given that, according to the fundamental position adopted by the Council, no evidence of that kind may be the subject of investigation by the Community judicature, the Council has adduced no evidence to that effect.
>
> 351 The Court cannot, therefore, do other than find that it is not able to undertake the review of the lawfulness of the contested regulation in so far as it concerns the appellants, with the result that it must be held that, for that reason too,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the fundamental right to an effective legal remedy which they enjoy has not, in the circumstances, been observed.

352 It must, therefore, be held that the contested regulation, in so far as it concerns the appellants, was adopted without any guarantee being given as to the communication of the inculpatory evidence against them or as to their being heard in that connection, so that it must be found that that regulation was adopted according to a procedure in which the appellants' rights of defence were not observed, which has had the further consequence that the principle of effective judicial protection has been infringed.

353 It follows from all the foregoing considerations that the pleas in law raised by Mr Kadi and Al Barakaat in support of their actions for annulment of the contested regulation and alleging breach of their rights of defence, especially the right to be heard, and of the principle of effective judicial protection, are well founded.

The ECJ also held that in the "circumstances of the case, the imposition of the restrictive measures laid down by the contested regulation in respect of Mr Kadi, by including him in the list contained in Annex I to that regulation, constitutes an unjustified restriction of his right to property."[95]

As applied against Messieurs Kadi and Al Barakaat, Regulation No. 881/2002 was, therefore annulled, although that annulment was suspended for three months to avoid "seriously and irreversibly prejudicing the effectiveness of the restrictive measures imposed by the regulation and which the Community is required to implement".[96]

Subsequently, the EU Council adopted Regulation No. 1190/2008,[97] relisting these individuals, but only after the process described in that instrument as follows:

> In order to comply with the judgment of the Court of Justice, the Commission has communicated the narrative summaries

---

[95] *Ibid* at para. 370.

[96] *Ibid* at para. 373.

[97] 2008 O.J. (L 322/25).

000082

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> of reasons provided by the UN Al-Qaida and Taliban Sanctions Committee, to Mr Kadi and to Al Barakaat International Foundation and given them the opportunity to comment on these grounds in order to make their point of view known.
>
> …The Commission has received comments by Mr Kadi and by Al Barakaat International Foundation and examined these comments.
>
> …After having carefully considered the comments received from Mr Kadi in a letter dated 10 November 2008, and given the preventive nature of the freezing of funds and economic resources, the Commission considers that the listing of Mr Kadi is justified for reasons of his association with the Al-Qaida network.
>
> …After having carefully considered the comments received from Al Barakaat International Foundation in a letter dated 9 November 2008, and given the preventive nature of the freezing of funds and economic resources, the Commission considers the listing of Al Barakaat International Foundation is justified for reasons of its association with the Al-Qaida network.
>
> … In view of this, Mr Kadi and the Al Barakaat International Foundation should be added to Annex I.

Messieurs Kadi and Al Barakaat then commenced challenges in the European Court of First Instance to this second listing.[98] By the time of writing, the *Al Barakaat* matter had been removed from the Court of First Instance's register, while *Kadi* was pending. The *Kadi* applicant urges that:

> …the contested regulation lacks a sufficient legal basis because it appears to amend Regulation 881/2002 without relevant determination by United Nations which, in the applicant's opinion, is precondition for the amendment of that regulation.
>
> Second, the applicant claims that the contested regulation violates his rights of defence, both the right to an

[98] Action brought on 30 January 2009 — Al Barakaat International Foundation v Commission (Case T-45/09); Action brought on 26 February 2009 — Kadi v Commission (Case T-85/09).

000083

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

effective hearing and the right to effective judicial protection, and fails to remedy the infringements of those rights as found by the Court in joined cases C-402/05 and C-415/05. He further contends that the contested regulation provides no procedure for communicating to the applicant the evidence on which the decision to freeze his assets was based, or for enabling him to comment meaningfully on that evidence.

Third, the applicant submits that the Commission failed to provide compelling reasons for maintaining the asset freeze against the applicant, in violation of its obligation under Article 253 EC.

Fourth, it claims that the Commission failed to undertake an assessment of all relevant facts and circumstances in deciding whether to enact the contested regulation and therefore manifestly erred in its assessments. Fifth, the applicant contends that the contested regulation constitutes an unjustified and disproportionate restriction on his right to property which is not justified by compelling evidence.[99]

Meanwhile, the ECJ's decision in *Kadi* has sparked other challenges to listing under Regulation 881/2002. In Joined Cases C-399/06 P and C-403/06 P, *Hassan v. Council and Commission*, ECJ Judgment, 3 December 2009, the ECJ followed its *Kadi* holding in annulling, effective immediately, the original listing under Regulation 881/2002 in relation to two other listed applicants. (The two applicants had also subsequently been listed pursuant to the notice and comment approach described above in relation to the post-ECJ response to the *Kadi and Al Barakaat* matters, but that second listing was not before the Court).

In Case T-318/01, *Othman v. Council and Commission* (June 11, 2009), the Court of First Instance followed *Kadi* in relation to yet another person listed under the 1267 listing process, holding that "the contested regulation [881/2002], in so far as it concerns the applicant, was adopted without any guarantee being given as to the communication of the inculpatory evidence against him or as to his being heard in that connection, so that it must be found that that regulation was adopted according to a procedure in

---

[99] *Ibid.*

000084

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

which the applicant's rights of defence were not observed, which has had the further consequence that the principle of effective judicial protection has been infringed".[100] The regulation, as applied to Mr. Othman, was annulled, effective immediately.

Other, similar cases were pending at the Court of First Instance by the time of this writing. These included: Case T-135/06 *Al Bashir Al-Faqih*, Case T-136/06 *Sanabel Relief Agency*, Case T-137/06 *Ghunia Abdrabbah*, and Case T-138/06 *Taher Nasuf* before the Court of First Instance.

Notably, in the wake of the ECJ's decision in *Kadi*, the EU Council amended Regulation No. 881/2002 to include due process standards for implementation of the 1267 listing process analogous to those already existing under its unilateral listing system in Regulation No. 2001/2580. Article 7a includes the most important new standards:

> 1. Where the United Nations Security Council or the Sanctions Committee decides to list a natural or legal person, entity, body or group for the first time, the Commission shall, as soon as a statement of reasons has been provided by the Sanctions Committee, take a decision to include such person, entity, body or group in Annex I.
>
> 2. Once the decision referred to in paragraph 1 has been taken, the Commission shall without delay communicate the statement of reasons provided by the Sanctions Committee, to the person, entity, body or group concerned, either directly, if the address is known, or following the publication of a notice, providing him, her or it an opportunity to express his, her or its views on the matter.
>
> 3. Where observations are submitted, the Commission shall review its decision referred to in paragraph 1 in the light of those observations and after following the procedure referred to in Article 7b(2) [incorporating general rules on Council regulation-making]. Those observations shall be forwarded to the Sanctions Committee. The Commission shall communicate the result of its review to the person, entity, body or group concerned. The result of the review shall also be forwarded to the Sanctions Committee.

---

[100] *Othman*, at para. 89.

000085

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> 4. If a further request is made, based on substantial new evidence, to remove a person, entity, body or group from Annex I, the Commission shall conduct a further review in accordance with paragraph 3 and after following the procedure referred to in Article 7b(2).
>
> 5. Where the United Nations decide to de-list a person, entity, body or group, or to amend the identifying data of a listed person, entity, body or group, the Commission shall amend Annex I accordingly.

A final EU case of note in relation to Regulation 881/2002 is Judgment of the ECJ in Case C-340/08, *M & Others v. Her Majesty's Treasury* (ECJ Judgment), Apr. 29, 2010. At issue in that case were proceedings in UK court concerning the reach of the asset freeze, and specifically whether the EU rules barred the provision of social security and assistance benefits to listed persons and their spouses. That question was referred to the European Court of Justice as a reference case by the then-UK House of Lords. Interpreting the resolutions establishing the UN 1267 regime and the EU regulation, the ECJ held that "the measure freezing economic resources applies only to those assets that can be turned into funds, goods or services capable of being used to support terrorist activities."[101] The Court then observed that "it is hard to imagine how those funds could be turned into means that could be used to support terrorist activities, especially because the benefits at issue are fixed at a level intended to meet only the strictly vital needs of the persons concerned" and concluded that

> …the benefit in kind that a designated person might indirectly derive from the social payments made to his spouse cannot, therefore, compromise the objective pursued by Regulation No 881/2002 which, as stated …, is to stop designated persons gaining access to economic or financial resources of any kind that they could use to support terrorist activities. …In consequence, having regard to the variations found to exist in the language versions of Article 2(2) of Regulation No 881/2002, that provision must, in the light of its object, be construed as meaning that it does not apply to the payment of social security or social assistance benefits in

---

[101] *M & Others*, at para. 56.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> circumstances such as those in issue in the main proceedings.[102]

b) Caselaw Concerning the EU Unilateral Listing Process

Listed persons have also challenged the EU's unilateral listing process; that is, the system established by Regulation No. 2580/2001 for the listing for persons not named in the UN listing system. These cases include several before the European Court of Justice. Case C-354/04 *Gestoras Pro Amnisti´a v Council*, Case C-355/04 *Segi v Council*, Case C-266/05 *Sison v Council* concern questions of competence, jurisdiction and certain disclosure practices under EU law, tied to the unilateral listing system. Case C-229/05 *PKK and KNK v Council* affirms the ECJ's competence to hear judicial review of listing decisions under the unilateral listing mechanism.

The European Court of First Instance has delivered more substantive court holdings. In Cases T-37/07 and T-323/07 *Mohamed El Morabit v Council*, Judgment of the Court of First Instance, 2 September 2009, the Court rejected claims that the unilateral listing process violated presumptions of innocence and held that the consequences of freezing assets were proportional to the objective of the measure in combating terrorism. However, in the earlier Case T-327/03, *Stichting Al-Aqsa v Council and Commission*, 11 July 2007, the CFI annulled the asset freeze imposed on the applicant, holding that the latter had not been provided with sufficient reasons for their listing. This was also the holding in Case T-253/04, *KONGRA-GEL v. Council*, 3 April 2008. Likewise, in Case T-47/03 *Sison v Council*, 11 July 2007, the European Court of First Instance declared regulation 2580/2001 annulled in relation to the applicant because of violation of, in essence, due process guarantees. In the Court's words, at para. 219:

> The applicant has not only been unable effectively to make his views known to the Council but also, given the lack of any statement, in the decision originally challenged or in the contested decision, of the actual and specific grounds justifying those decisions, has not been placed in a position to make good use of his right of action before the Court, given the aforementioned links between the guarantees of the rights of the defence, of the obligation to state reasons and of the right to an effective legal remedy. It is to be borne in mind that the possibility of regularising the total lack of a

[102] *Ibid* at paras. 61-63.

000087

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> statement of reasons after an action has been brought is now considered in the case-law to be prejudicial to the rights of the defence and is therefore prohibited …

In the wake of that decision, the EU Council relisted Sison, and provided reasons for doing so (a practice it then universalized for all listed persons, per Regulation No. 501/2009). This decision prompted a further round of judicial review, culminating in Case T-341/07 *Sison v Council*, September 30, 2009. In that matter, the European Court of First Instance again annulled Sison's listing, this time for failing to meet requirements under Common Position 2001/932, as incorporated by regulation 2580/2001, specifying that the list "shall be drawn up on the basis of precise information or material in the relevant file which indicates that a decision has been taken by a competent authority in respect of the persons, groups and entities concerned, irrespective of whether it concerns the instigation of investigations or prosecution for a terrorist act, an attempt to perpetrate, participate in or facilitate such an act based on serious and credible evidence or clues, or condemnation for such deeds."

A second series of cases have concerned the listing of the People's Mojahedin Organization of Iran (called OMPI in the jurisprudence). In Case T-228/02 *Organisation des Modjahedines du peuple d'Iran* v *Council*, 12 December 2006, the Court of First Instance annulled the listing of OMPI on the basis that the listing did not contain adequate reasons and that the procedure leading to the listing did not comport with the applicant's right to a fair hearing. Subsequently, the applicant was relisted by the Council, following the provision of reasons, and a request for any comments. The applicant submitted comments and a request for access to the Council's files. The Council provided certain files to the applicant. The applicant continued to request, however, the full set of files. The Council decided, however, to relist, prompting renewed judicial review and the Court of First Instances decision in Case T-256/07 *People's Mojahedin Organization of Iran* v *Council*, October 23, 2008. There, the Court held "in the light of all the relevant information and having regard to the particular circumstances of the case, proper and sufficient reasons have not been adduced for the continued freezing of the applicant's funds" (at para. 185).

Also of note, is Case T-284/08 *People's Mojahedin Organization of Iran* v *Council*, December 4, 2008. In that matter, the applicant had been relisted on the basis of new information said to be in the possession of the Council. The applicant was not informed of this new information or provided with the new material on the file. The Court of First Instance annulled the new listing, holding (at para. 47) that "the continued freezing of the applicant's funds by the contested decision was the result of a procedure during which the applicant's rights of the defence were not respected. That finding

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

cannot but lead to the annulment of the contested decision, in so far as it concerns the applicant."

3. Literature

Cameron, Iain, "European Union Anti-terrorist Blacklisting," (2003) 3(2) *Human Rights Law Review* 225.

This article provides an overview of the UN targeted sanctions regime, with an emphasis on counter-terrorism measures. It then focuses on the EU unilateral listing system, tracing the EU's reaction to Security Council resolution 1373 (2001) and the resulting EU Council Common Position and regulation 2580/2001. The article describes the legal authority for regulation 2580/2001, its content and describes its workings, with a particular emphasis on the complex and (as the author notes) relatively opaque manner in which groups and persons are listed under the unilateral system.

Since much of the mechanics by which persons and entities are listed is "shrouded in secrecy", the author infers how a listing decision is actually undertaken, focusing on the respective roles of the EU member states and the EU apparatus itself. The author's key conclusion in this discussion is to note that discrepancies between the end EU list as compared to those of individual EU member national lists suggests that member states can and do object to some inclusions at the EU level – that is, that some listings that individual member states have made in their national lists have been vetoed by other member states at the EU level.

The author notes that the exact evidentiary basis for a listing decision is "not publicly known". He reports, on the basis of personal information, that groups have been included "where the 'terrorist' nature of the group is 'notorious'" (at 236). The system "leaves considerable space for political considerations, such as political pressure from friendly states, such as Turkey, to blacklist an organization" (at 236), or to decline to blacklist an organization. The absence of clear listing criteria means that groups have been listed who have not recently committed acts of terrorism and who have, indeed, renounced terrorist tactics (an example being the listing of the PKK in 2002).

Subsequently, the article focuses specifically on the implementation and legal effects of the EU listing system in Sweden, noting the domestic constitutional environment in which implementation must take place. He points, among other things, to the constraints on Swedish foreign policy imposed by EU-mandated listing, and the inclusion of groups that Sweden itself might not chose to list.

The balance of the article discusses procedures and grounds for challenging EU listing under EU law. The author focuses in particular on the prospect that challenges could be lodged with reference to the guarantees found in the European Convention on

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Human Rights. Possible grounds for complaint canvassed by the author include: Art. 6 (access to court); Art. 6 (fair trial and presumption of innocence); Art. 11 (freedom of association); and Art. 1, Protocol 1 (property rights and sanctions). The author concludes that there is "little concrete guidance in the case law, and so the ECHR standards are still rudimentary" in the area of counter-terrorism (at 256).

Almqvist, Jessica, "A Human Rights Critique of European Judicial Review: Counter-terrorism Sanctions," (2008) 57 *International and Comparative Law Quarterly* 303.

This article examines post-listing judicial review of listing mechanisms, with a principle focus on EU law. It approaches the question from the perspective of effective access to justice, a core human rights principle. The article begins with an overview of the UN listing mechanisms, and the critiques thereof, before then looking at the implementation of listing mechanisms in the EU. The article compares the UN listing mechanism with the EU unilateral system, noting that the latter suffered initially from many of the shortcomings afflicting the latter in terms of disclosure, fair hearing and judicial review and remedies. (The EU unilateral system always included more precision than its UN counterpart in the criteria for inclusion of names and a definition of the concept of terrorist acts guiding the listing decisions).

The article discusses how the EU unilateral system changed in the wake of the Court of First Instance's decision in Case T-228/02 *Organisation des Modjahedines du Peuple d'Iran* v *Council*. In that ruling – delivered at the end of 2006 – the Court held that the unilateral listing process was unacceptable, prompting the EU Council to provide statement of reasons to all listed entities and persons, as well as providing notice to persons and entities on how, e.g., to obtain this statement of reasons and seek reconsideration of a listing decision.

Despite the obvious impact of this decision, the author has clear doubts as the efficacy of judicial review through EU judicial bodies in counter-terrorism matters. Some of the failed EU court challenges to listings have stemmed from poor legal strategy and reliance on doubtful arguments and the inherent complexity of EU law.

There are also doubts and uncertainties about the competency of the EU judicial bodies to conduct full judicial review of the listing measures under the relevant EU laws and treaties, although the EU courts have shown a willingness to review the actual implementation of the listing process (for example, the provision of information and reasons).

EU judicial institutions may also be constrained in their review competence when it comes to implementation of the UN lists under the 1267 process, where the EU mechanism is designed simply to give effect to the UN list. [This article pre-dates the ECJ decision in *Kadi*, focusing instead on the Court of First Instance decision].

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The author also examines at length the challenge to judicial oversight posed by secrecy surrounding the material motivating and justifying listing either under the UN process or the EU unilateral system.

Besson, Samantha, "European Legal Pluralism after *Kadi*," (2009) 5 *European Constitutional Law Review* 237.

This largely theoretical article focuses on the significance of the *Kadi* decision for understanding the relationship between EU law and international law. Highlighting its arguments with a discussion of *Kadi*, the article proposes a theory on this question that it calls "European legal pluralism". This article is, in other words, mostly a work on EU law and not a critique of listing or counter-terrorism practices per se.

Cananea, Giacinto della, "Global Security and Procedural Due Process of Law between the United Nations and the European Union: Yassin Abdullah Kadi & Al Barakaat International Foundation V. Council," (2009) 15 *Colum. J. Eur. L.* 511.

The case comment examines the *Kadi* decision. It notes that the Court of First Instance decision in *Kadi* showed deference to political choices made at the international level. The European Court of Justice did not adopt that position on appeal. The latter emphasized the autonomy of the European legal order, rather than uncritical subordination to the Security Council, and superimposed respect for human rights as a condition on the lawfulness of measures taken by EU bodies. The fundamental procedural safeguards invoked by the ECJ extended, not just to EU citizens, but to everyone, aliens included. The author concludes that "what emerges from *Kadi* is that when confronted with issues of power, the ECJ is reluctant to follow the traditional ideal of constitutionalism, restraining government. Rather, it uses procedural due process of law as a form of proxy. Of course, this instrumental use of procedural safeguards has at the same time the effect of strengthening its role as the constitutional court of the EU. Whether the ECJ will be capable of mediating these kinds of conflicts between collective interests and individual rights in the new post-September 11, 2001 context remains to be seen" (at 530).

Cardwell, Paul James, Duncan French and Nigel D. White, "European Court of Justice, Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council and Commission," (2009) 58 *International and Comparative Law Quarterly* 229.

This brief case comment on the *Kadi* case begins with a summary of the facts; specifically, a brief history of the implementation of Security Council resolution 1267

000091

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

and its successors into EU law. It then describes the decision of the Court of First Instance and summarizes the decision of the ECJ, on appeal. The balance of the article comprises commentary on the decision, describing the ICJ decision as a "significant—though perhaps not a ground-breaking—decision in understanding the relationship between EU law and public international law" (at 233). In the author's views, "The approach of the ECJ is ultimately premised upon three key understandings, namely the autonomy of the EU legal system, the constitutionality of the EU legal system and the centrality of fundamental rights to the operation of that legal system" (at 233), none of which constitutes a radical new departure for the ECJ.

In its subsequent discussion, the note focuses on the relationship between the EU legal sphere and the UN Charter, and particularly the working of Articles 25 and 103 of the UN Charter. It regards the *Kadi* decision as a rejection of the ill-founded view that these provisions override domestic constitutional rights. The authors argue that the Security Council is not empowered by the Charter, and Article 103 does not operate, to vitiate human rights principles. In the authors' words, "the targeted sanctions against Kadi created overriding obligations for member states only to the extent that they were consistent with 'promoting and encouraging respect for human rights'", itself a purpose and principle of the UN under the UN Charter. "Member states are obliged to apply them within their legal orders as far as they are consistent with respect for human rights" (at 237). Compliance with fundamental human rights obligations – such as a right to a fair hearing – does not conflict with the Article 103 obligation to implement Security Council resolution 1267 and its successors.

Cremona, Marise, Francesco Francioni, Sara Poli (eds), *Challenging the EU Counter-Terrorism Measures through the Courts*, EU Working Papers, AEL 2009/10 (Academy of European Law).

This 168-page compilation of papers on the *Kadi* case focuses on issues such as:

- The scope of the Rome Treaty and its relationship with the UN Charter;
- The perceived existence of a conflict between the UN and EU legal orders, and the *Kadi* decision's assertion of primacy of EU norms over global standards;
- The extent to which fair hearing rights must be observed by the Security Council sanctioning system, and how challenges before domestic courts may cure a failure to observe these standards;
- Whether the ECJ should properly have assessed the legitimacy of the EU regulations implementing the 1267 process with an eye to customary international law or UN Charter obligations, rather than confining its analysis on EU law;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- The implications of *Kadi* in positioning fundamental rights at the top of the hierarchy of EU norms; and
- A discussion of the respective roles of the European Court of Justice and the European Court of Human Rights in protecting fundamental human rights.

The document also includes a bibliography of articles concerned with UN smart sanctions that strategically target individuals or sectors as opposed to whole countries and the EU legal order (including those by political scientists), many of which are reproduced in the bibliography for this report but also including articles in languages other than English and French.

d'Aspremont, Jean and Frederic Dopagne, "*Kadi:* The ECJ's Reminder Of The Elementary Divide Between Legal Orders," (2009) 5 *International Organization Law Review* 371.

This brief and largely theoretical comment examines the *Kadi* decision as reflecting a particular perspective on the European constitutional order and its relationship with the international legal order. It discusses how the interplay between regional and global legal orders is understood by legal scholars and sees *Kadi* as reminding scholars that these regional and international "legal orders are naturally and inextricably estranged from each other".

de Burca, Grainne, "The European Court of Justice and the International Legal Order After Kadi," (2010) 51 Harv. Int'l L.J. 1.

This discussion of the *Kadi* case argues that *Kadi* represents a strongly "pluralist" or "dualist" view of the relationship between EU and international legal orders, one that is inconsistent with the EU's traditional approach to international law (and earlier more deferential approaches adopted by the European Court of Human Rights in relation to UN Security Council resolutions). The ECJ's departure from this stance carries risks to the EU's image as an entity strongly committed to international law.

Draghici, Carmen, "Suspected Terrorists' Rights Between the Fragmentation and Merger of Legal Orders: Reflections in the Margin of the Kadi ECJ Appeal Judgment" (2009) 8(4) *Washington University Global Studies Law Review* 627.

This article examines the ECJ's decision in the *Kadi* case. It begins with an overview (and critique) of the UN 1267 listing process and argues that its nature (and the consequence it visits on a listed individual) demands prior determination of guilt by

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

a tribunal. The article then examines (and critiques) the Court of First Instance's approach in *Kadi* before then turning to the ECJ decision. The author concludes that "[a]t first glance, the moderate finding that procedural guarantees have to be added to the mechanism in the implementation phase at the EC level does not clash, in principle, with EC States' superior obligation, deriving from U.N. membership, to freeze the funds of listed individuals. Yet, if the evidentiary burden is not met for the EC review body, and individuals are de-listed at the EC rather than at the U.N. level, the collision between obligations becomes unavoidable. In that event, the primacy of U.N. commitments, which the ECJ attempts to leave undisputed, largely remains a mere theoretical concession" (at 657).

Eckes, Christina. "Judicial review of European anti-terrorism measures - the Yusuf and Kadi judgments of the Court of First Instance," (2008) 14(1) *European Law Journal* 74.

This article pre-dates the ECJ's decision in *Kadi* and has, therefore, been superseded by events. Its focus is on the ultimately overturned Court of First Instance decision. The article is highly critical of this lower court decision, arguing that it left "the individual without effective legal protection exposed to SC decisions vested with the powers of Community law" and predicting (correctly as it turns out) that the ECJ would reverse this holding.

Eckes, Christina, "Sanctions against Individuals – Fighting Terrorism within the European Legal Order," (2008) 4(2) *European Constitutional Law Review* 205.

This article focuses on the EU unilateral listing process, and the decision of the European Court of First Instance dealing with it. It concludes that in "*OMPI*, *Sison* and *al-Aqsa* the CFI identified fundamental flaws in the autonomous listing procedure and developed convincing guidelines for a different approach" (at 222). As summarized by the author, "[r]estrictive measures adopted by the EU must, as a minimum, comply with the safeguards outlined by the CFI in *Sison*. Those affected must have at least *after* the initial listing the opportunity to make their views know on the allegations raised against them. The statement of reasons must indicate the decision identified to satisfy the criteria in Article 1(4) of Common Position 2001/931/CFSP; this would – barring exceptional circumstances – include the author, date and content of that decision. While security concerns might justify the non-disclosure of certain information to the parties, the EU Courts must be able to access sufficient information to carry out full judicial review of the law and the facts of the case brought before them" (at 223).

Eckes, Christina, "A Test Case for the Resilience of the EU's Constitutional Foundations:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

International Sanctions," (2009) 15(3) *European Public Law* 351.

This article discusses the ECJ's decision in *Kadi*, providing a background and summary of the case, an analysis of the EU's jurisdictional competence to adopt smart sanctions, and an examination of the relationship between EU law and UN Security Council resolutions. The author concludes that "[i]nstead of allowing the Security Council to set aside fundamental principles of European law within the European legal order the Court increased the pressure on the Security Council to reconsider its course. This could lead to further reaching procedural rights within the UN listing procedure, or ultimately to the finding that the UN cannot actually meet the necessary standards" (at 378).

Godinho, Jorge. "When worlds collide: enforcing United Nations Security Council asset freezes in the EU legal Order" (2010) 16(1) *European Law Journal* 67.

This article examines UN Security Council asset freezing sanctions and the difficulties it creates for the legal institutions of the EU. It begins by describing the evolution of the UN 1267 regime. It then highlights the problem of how to implement this regime faced by the EU and the difficult conundrum of reconciling the UN system with the fundamental rights protected by the EU legal order. In the author's view, "asset freezes against suspected terrorists are an ad hoc (para-)criminal procedure measure" (at 90), and should, therefore, attract legal safeguards, including judicial review. Such review is not, however, available at the international level. In the author's view, "[t]he solution is not to simply add the possibility of judicial review, for *asset freezing with standard judicial review would substantially amount to a sort of abbreviated criminal process where the accuser is the executive branch and where there is a reversal of the burden of proof* (given that the person who has had assets frozen needs to come forward and demonstrate his innocence)" (at 91). Instead, asset freezes should be temporary and *ad hoc* pending a full criminal-style procedure at the national level. In the absence of such a procedure, the asset freeze should be lifted.

Harpaz, Guy. "Judicial Review by the European Court of Justice of UN Smart Sanctions against Terror in the Kadi Dispute," (2009) 14(1) *European Foreign Affairs Review* 65.

This article focuses on the ECJ's decision in *Kadi*, commenting favourably on the outcome of that case and urging that so long as the UN sanctions regime is deficient in the legal protections it extends, it will be proper for the "EC judicature to strike that balance and to safeguard it" (at 88). The author describes the ECJ decision as establishing an appropriate equilibrium between multilateralism and regionalism and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

between the need to safeguard uniform obedience to international law and to maintain the coherence of EU law, and between the need to counter terrorism and observe human rights.

Johnston, Angus. "Thawing out? The European courts and the freezing of terrorist assets," (2007) 66(2) *Cambridge Law Journal* 273.

This brief case comment discusses several EU cases examining the unilateral listing system. First, it highlights Case T-228/02 *OMPI v. Council of the European Union* (18 December 2006), which the author describes as annulling "the Council's decision to add the Organisation des Modjahedines du peuple d'Iran ("OMPI") to that list because the Council had failed to communicate to the OMPI the reasons for adding it to the list contemporaneously with the decision to do so: this failed to provide OMPI with the means to ensure its right to a fair hearing and also breached the Article 253 EC requirement that reasons be given for the adoption of EC acts." The author describes the decision as a positive acknowledgment of the availability of judicial review, but also signals out problematic aspects of the decision: "First, since the Council had considerable discretion in deciding to place a name on the list, judicial review would be very limited (covering only procedure, the accuracy of material facts and misuse of power) … Second, even after the pleadings and the oral hearing, the CFI still found that it was 'not in a position to review the lawfulness of the contested decision' due to the Council's inability to provide coherent information as to which was the relevant decision of the 'competent authority' which led to the listing of the OMPI … This is a damning indictment of the way in which the listing system operates in practice."

Second, the comment discusses the ECJ's decision in Case C-229/05 PKK and KNK v. Council of the European Union (18 January 2007), a case that turned on what can be broadly described as procedural questions. The author concludes the terrorist listing processes have serious impacts on fundamental rights and predicts (correctly) that they will invite future scrutiny by the EU's judicial organs.

Johnston, Angus. "The European Union, the ongoing search for terrorists' assets and a satisfactory legal framework: getting warmer or colder?" (2007) 66(3) *Cambridge Law Journal* 523.

This brief case comment discusses Cases C-354/04 P Gestoras Pro Amnistı´a v. Council and C-355/04 P Segi v. Council (judgments of 27 February 2007), cases that concerned the jurisdictional competence of the EU judicial bodies to hear certain complaints stemming from the listing processes.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Johnston, Angus. "Freezing terrorist assets again: walking a tightrope over thin ice?" (2008) 67(1) *Cambridge Law Journal* 31.

This brief case comment discusses Case T-47/03 Sison v. Council and Case T-327/03 Stichting Al-Aqsa v. Council (both judgments handed down 11 July 2007), describing these cases (and Sison in particular) as "fleshing out the procedural protections in the process of deciding to freeze the assets of those suspected of terrorist connections" but arguing that "there is still some distance to travel before this system can be said to have achieved a proper balance between its laudable anti-terrorist goals and the need for effective judicial protection of the interests of those who may be affected by orders to freeze their assets."

Kunoy, Bjorn and Anthony Dawes. "Plate Tectonics in Luxembourg: The Ménage à Trois between EC Law, International Law and the European Conventions on Human Rights Following the UN Sanctions Cases," (2009) 46(1) *Common Market Law Review* 73.

This article provides an overview of the *Kadi* case, examining the concept of fundamental rights in EU law and the historic relationship between EU law and international law. It views the European Court of First Instance's decision in *Kadi* as a break with this history, and argues that the ECJ was correct to reject this departure.

Menz, Simon and Tobias B. Scholz. "The Kadi Case or the Legal Protection of Persons Included in the European Union Anti-Terror List," (2009) 17(1) *European Journal of Crime, Criminal Law and Criminal Justice* 61.

This brief case comment described the ECJ's *Kadi* decision. It concludes that the decision "closes the existing gap of legal protection with its decision for individuals concerned on the EU level. At the same time it would be desirable if the Security Council were to establish an independent organ for the supervision of its own actions as well" (at 68). The authors express hope that the *Kadi* decision will prompt such a move by the UN.

Michaelson, Christopher. "Kadi and Al Barakaat v Council of the European Union and Commission of the European Communities" (2009) 10 *Melbourne Journal of International Law* 330.

This 18 page case note examines the European Court of Justice's Kadi decision in light of the 1267 listing regime. It argues that the focal point in the committee does not

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

provide listed persons with the right to be heard and "does not operate as an independent review mechanism."

The author concludes that the UN listing process still violates rights to judicial review, procedural fairness and an effective remedy that form "the very basis of due process of law" as guaranteed by the Universal Declaration, the ICCPR, the African Charter and the American Convention on Human Rights. It also concludes that *Kadi* confirms the intergovernmental and diplomatic nature of the delisting process and that it does not provide a real opportunity to assert rights. The article predicts that *Kadi* will be influentially legally and politically and that it will support increased challenges to the 1267 process.

Payandeh, Mehrdad and Heiko Sauer, "European Union: UN sanctions and EU fundamental rights," (2009) 7(2) *International Journal of Constitutional Law* 306.

This article is essentially a case comment focusing on the ECJ's *Kadi* decision. It begins with an overview of the UN 1267 process, then describes the procedural background to the *Kadi* matter and follows with a summary of the ECJ's holding. The article favours the ECJ's outcome, and particularly its unwillingness to subordinate EU law to UN Charter obligations. It urges that "[e]ven if the ECJ judgment were to entail a breach of EU member states' responsibilities under the UN Charter, its long-term implications for the UN system are not necessarily negative, since it may encourage the development of legal protections for listed persons within the UN sanctions regime."

Porretto, Gabriele, *The European Union: Counter-Terrorism Sanctions Against Individuals and Human Rights Protection* (June 25, 2009). Transitional Justice Institute Research Paper No. 09-08.

This research paper, published also in Penelope Mathew and Miriam Gani (eds.) Fresh Perspectives on the 'War on Terror' (Canberra: ANU E Press, 2008) pp. 235-268, examines decisions of the EU judicial institutions in relation to the UN 1267 process. It begins by examining the counter-terrorism sanctions regime at the United Nations level, before discussing implementation of this regime by the EU. It then examines European Court of First Instance jurisprudence in this area, criticizing the court's deference to UN measures. The cases it examines, however, pre-date the ECJ's decision in *Kadi*. As a consequence, this article has been superseded by events.

Posh, Alberto, "The Kadi Case: Rethinking the Relationship between EU Law and International Law? (2009) 15 *Colum. J. Eur. L. Online* 1.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

This very brief article constitutes a case comment on the ECJ's *Kadi* decision. It concludes that the decision leaves open a number of questions, not least "whether the primacy of the UN Charter obligations is jeopardized." The article asserts that a potential clash between UN Charter obligations and EU notions of fundamental rights arises where it would be impossible to implement a UN resolution without disregarding these EU legal rights. It concludes that the decision makes "it harder for the UN Security Council to adhere to violations of fundamental rights. As such, *Kadi* stands for a new bottom-up process in which a regional court pressures the UN Security Council to change its policy towards fundamental rights."

Simoncini, Marti "Risk Regulation Approach to EU Policy against Terrorism in the light of the ECJ / CFI jurisprudence," (2009) 10(11) *German Law Journal* 1526.

This largely theoretical article examines the EU listing process (both unilateral, and under the UN 1267 process) from the optic of "risk regulation". It examines the jurisprudence of EU judicial bodies from this perspective, noting that the *Kadi* decision stands as recognition of counter-terrorism as a persistent risk minimization issue, and not as a response to a permanent emergency. The article advances a theory of "proportionality" to be used in determining whether a breach of a fundamental right is lawful.

Spaventa, Eleanor, "Case T-256/07, People's Mojahedin Organization of Iran v Council" (2009) 46(4) *Common Market Law Review* 1239.

This article focuses on key cases before the European Court of First Instance challenging listings under the EU unilateral listing process. It focuses, in particular, on Cases T-256/07 and T-284/08 involving People's Mojahedin Organization of Iran. The article argues that the cases reveal "in considerable detail the deep flaws in the EU terrorist listing system" (at 1240). The article provides a detailed overview of the background to the cases, focusing on the interplay between EU and national level listing by member states. This article constitutes the most comprehensive piece analyzing the unilateral listing process, albeit one that focuses on challenges to it.

Tridimas, Takis and Jose A. Gutierrez-Fons, "EU Law, International Law, and Economic Sanctions against Terrorism: The Judiciary In Distress?" (2009) 32 *Fordham Int'l L.J.* 660.

This comprehensive article focuses on the ECJ's *Kadi* decision as well as the European Court of First Instance's case law under the EU unilateral listing process. The article begins by examining the factual and legal context surrounding *Kadi* and the issue of whether the EU has jurisdictional competence over smart sanctions. The authors

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

question whether the EU should have competency to enact such measures at the Community level. The article then discusses the extent to which the EU is bound by UN Security Council resolutions and the jurisdiction of the ECJ in reviewing implementation of these resolutions. The authors juxtapose the ECJ's relatively non-deferential approach to UN Security Council primacy to the approach adopted by the European Court of Human Rights in relation to Security Council authorized peace-making missions. The article analyzes the consequences of the ECJ's decision. It notes, correctly as it turned out, that "[s]ince the regulation was vitiated by procedural rather than substantive defects, it could not be excluded that the imposition of sanctions on appellants might prove to be justified" (at 702). The article then focuses on European Court of First Instance decisions in relation to the EU's unilateral listing process, noting the obligations established by those cases by giving notice to the person and an opportunity to comment and that reasons for the listing be provided. The authors argue that "[o]n the one hand, the CFI is keen to assert the application of procedural rights and confirm that any concept of emergency constitution is internalized, i.e., remains subject to the prerequisites for human rights protection provided for by the Community legal order. On the other hand, it recognizes that exceptions may be required with regard to the disclosure of evidence to the parties in order to accommodate concerns pertaining to the nature and sources of evidence."

This article is among the best for an understanding of the EU system and cases.

Tzanou, Maria. "Case-note on Joined Cases C-402/05 P & C-415/05 P *Yassin Abdullah Kadi & Al Barakaat International Foundation* v. *Council of the European Union & Commission of the European Communities*," (2009) 10(2) *German Law Journal* 123.

This case comment examines the ECJ's *Kadi* decision, focusing on the EU jurisdictional competence to impose smart sanctions in the anti-terrorism context and the relationship between EU law and UN Security Council resolutions. In relation to the latter issue, the author argues that the decision demonstrates "respect towards international law, while at the same time safeguards the constitutional principles of the domestic legal order" (at 147). The article also discusses protection of human rights in the listing process and the question of compliance with the ECJ's decision. On the last issue, the author expresses doubt that the subsequent relisting of Kadi and Al Barakaat after the ECJ decision – following comments on "narrative summaries of reasons" – satisfied the due process requirements established in the judgment.

Weema, Christopher, "Kadi v. Council: Putting the United Nations in Its Place," (2009) 17 *Tul. J. Int'l & Comp. L.* 571.

000100

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

This brief case comment examines the ECJ's *Kadi* decision, summarizing the background and context of the case and its key holdings. In his analysis, the author describes the decision as "the *Marbury v Madison* of the European Union, and more. Not only does it effectively establish judicial review of every act of the European Union, it does so in the context of the intersection of international treaty obligations and positive EU law" (at 582). He also argues that the decision "created a precedent that, if followed by other nations, could eviscerate or erode the power of the U.N. Security Council. The Court has in essence made the determination that subsequent treaties can modify the obligations of Member States under the U.N. Charter. That begs the question, does the Charter allow for such modification without ratification by the remaining U.N. members?" (at 583).

Zgonec-Rozej, Misa. "Yassin Abdullah Kadi & (and) Al Barakaat International Foundation v. Council & (and) Commission" (2009) 103(2) *American Journal of International Law* 305.

This brief case comment described the ECJ's *Kadi* decision, and then highlights several implications of the case. The author concludes that "[t]he judgment illustrates the important role played by the EC courts in assuming their competence to review EC acts implementing Security Council sanctions given the absence of a judicial body or judicial proceedings at the international level where the targeted persons and entities would be able to contest inclusion of their names in the Consolidated List. While the judgment does not compromise the primacy of the relevant Security Council resolutions on the international plane, it affects their implementation at the EC and domestic levels" (at 311).

C. Discussion and Conclusions

1. General

Speaking generally, the EU literature can be divided into three categories: the public international law category; the EU constitutionalism category; and the due process category. The public international law category focuses on the *Kadi* case and its implications in reference to the UN Charter. Most authors addressing this issue seem to be at least partially persuaded by the ECJ's efforts to side-step a direct clash between its holding in *Kadi* and compliance with UN Security Council 1267 obligations; that is, that room remains for UN members to decide how to implement the list. Most also seem to acknowledge, however, that in reality, the *Kadi* case gives clear primacy to EU legal expectations (a manifestation of a legal dualism in which EU rules stand apart from international law), since those legal expectations include due process protections that the 1267 process simply does not honour. Some authors attempt to reconcile this

000101

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

conflict, urging for example that the UN members have separate UN Charter obligations to observe human rights. Others see the conflict as incompatible with the UN Charter, and Article 103 of it.

A related theme in the literature focuses on EU constitutionalism; that is, an examination of the workings of the EU system and the implications of *Kadi* for the EU apparatus and for the ECJ as an emerging proto-constitutional court. These articles are sometimes highly theoretical, and in any event obviously of regional rather than general interest.

A final area in the literature focuses on due process, both as reflected in *Kadi* and also in the many cases challenging unilateral listing. The articles focusing on this area are supportive of the now very strong tendency of EU courts to graft notice, comment, and provision of reason expectations on the listing process. On the other hand, some authors clearly doubt that procedural formalism will satisfy all complaints about the fairness and reviewability of listing decisions. For instance, there are obvious concerns about the degree of disclosure made to listed persons by the EU of information supporting the listing.

2. Categorization of Position on Listing

It is not possible to truly typecast the literature into categories based on whether authors support listing as is, support with amendments or oppose outright – many authors focus on issues that are peripheral to opinions on the merits of the listing system, such as the relationship between EU and international law. Even where authors do focus on listing, it is often difficult to infer whether they would support a different system – authors do not focus on counterfactuals, instead examining (and in practice, critiquing) what exists at present. A very large number of the EU articles are simply case comments on *Kadi*.

Among the broader papers, no author has written an article that is an unvarnished defence of the status quo (although several authors in the Cremona *et al* collection do take the view that international law obligations do and should prevail over EU law, and that the *Kadi* decision was incorrect).

Among other authors, Almqvist clearly does not believe that domestic legal systems can ever be adequate fixes to the due process concerns of an inadequate international listing mechanism, but do not indicate whether they would support listing if that international system incorporated full due process protections. Likewise, Cameron seems skeptical that any system – international or domestic – can accommodate fully due process and human rights concerns. However, Godinho does propose a modified EU approach that does not abandon listing per se.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

PART THREE: UNITED KINGDOM

A. Methodology

General searches of the following electronic databases were conducted under the words "listing of terrorists" and "terrorist listings", "terrorist proscriptions" and the United Kingdom. The databases searched included Social Science Research Network,[103] Hein Online,[104] the Legal Journals index (UK), and Legal Trac as well as searches using Google and Google scholar on the web.

B. Findings
1. Legislation

a) Implementing the UN 1267 Process

The United Kingdom currently implements its international obligations in relation to the UN 1267 listing process using regulations made pursuant to section 2(2) of the *European Communities Act 1972*, c.68. This Act authorizes the incorporation of EU obligations into UK law by, *inter alia*, regulation. In essence, the resulting regulation – the *Al-Qaida and Taliban (Asset-Freezing) Regulations 2010*, SI 2010/1197 – implements EU Council Regulation No 881/2002. As discussed above, the latter in turn incorporates the UN 1267 listing process into EU law. (The United Kingdom is, of course, a member of the European Union). The current UK regulations freeze the funds and economic resources of listed persons and bar making funds or economic resources available to these people. Violation of these strictures is a criminal offence, subject to certain enumerated exemptions. The 2010 regulations follow a 2010 decision of the UK Supreme Court (discussed below) quashing an earlier 2006 iteration of the instrument,[105] enacted under the *United Nations Act 1946*, c.45.

b) Implementing UN Security Council Resolution 1373

Meanwhile, the United Kingdom has implemented its international obligations in relation to Security Council Resolution 1373 via the *United Nations Act 1946*, c.45. Section 1 of that instrument allows the UK executive to issue Orders-in-Council implementing resolutions of the Security Council made under Article 41 of UN Charter. These may include, among other thing, "provision for the apprehension, trial and punishment of persons offending against the Order."

The UK government has issued a number of statutory instruments pursuant to

---

[103] Available at http://www.ssrn.com/lsn/index.html

[104] Available at http://heinonline.org.myaccess.library.utoronto.ca/HOL/Welcome?collection=journals

[105] *Al-Qaida and Taliban (United Nations Measures) Order 2006*, S.I. 2006 No. 2952.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

this provision, the most recent of which is the *Terrorism (United Nations Measures) Order 2009*, S.I. 2009/1747. However, a prior iteration of this instrument – *Terrorism (United Nations Measures) Order 2006*, S.I. 2006/2657 – was adjudged *ultra vires* by the UK Supreme Court in 2010, per the discussion below. The same deficiency at issue in the 2006 statutory instrument also likely afflicted the 2009 measure, prompting the introduction and rapid passage of the *Terrorist Asset-Freezing (Temporary Provisions) Act 2010*, c.2 in February 2010. The latter validates the *Terrorism (United Nations Measures) Order 2009* and its predecessors, giving them a statutory imprimatur and deeming these measures to be properly made under section 1 of the *United Nations Act*. Prior to the recent election and change in government, the Gordon Brown government was discussing a more permanent, separate statutory authority for its unilateral listing process.

As it stands at present, the 2009 Order permits unilateral listing of persons by the UK government, as well as incorporating into UK law the unilateral list established by the European Union as EU Council Regulation 2580/2001. The UK government listing may be made where the Treasury has reasonable grounds for suspecting that a person is "(a) a person who commits, attempts to commit, participates in or facilitates the commission of acts of terrorism; (b) a person identified as provided in Article 2(3) of the Council Regulation [that is, on the EU unilateral list]; (c) a person owned or controlled, directly or indirectly, by a designated person; or (d) a person acting on behalf of or at the direction of a designated person."[106]

c) Proscribed Organization Listing

The United Kingdom also has a separate "proscribed organization" process; that is, a mechanism for listing terrorist groups and entities. In United Kingdom law, membership in a proscribed organization is a crime.[107]

The *Terrorism Act, 2000*, c.11, permits the Secretary of State to add an organization to the list of proscribed organizations "if he believes that it is concerned in terrorism", defined as committing or participating, preparing, promoting or encouraging or otherwise concerned with terrorism.[108] The *Terrorism Act, 2006*, c.11 extended the grounds of proscription to include circumstances where an organization engages in the "unlawful glorification of the commission or preparation (whether in the part, in the future or generally) of acts of terrorism" or where the organization's

---

[106] *Terrorism (United Nations Measures) Order 2009*, s.4.

[107] *Terrorism Act, 2000*, c.11, s.11.

[108] *Ibid*, s. 3.

000104

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

activities are "carried out in a manner that ensures that the organization is associated with statements containing any such glorifcation".[109]

A proscribed organization may apply for de-listing, and where the Secretary refuses such an application, the applicant may appeal to the Proscribed Organisations Appeal Commission. The latter may allow the appeal "if it considers that the decision to refuse was flawed when considered in the light of the principles applicable on an application for judicial review".[110] Further appeal of this decision is available in the various UK Courts of Appeal.

2. Court Cases

The single most important decision relating to the UK listing system is the recent decision of the UK Supreme Court (formally the judicial committee of the House of Lords) in *Her Majesty's Treasury v Ahmed and al-Ghabra (FC)* [2010] UKSC 2. That decision declared *ultra vires* the *Terrorism (United Nations Measures) Order 2006*, S.I. 2006/2657 (implementing Security Council resolution 1373) and the *Al-Qaida and Taliban (United Nations Measures) Order 2006*, S.I. 2006 No. 2952, and sparked the renovation to UK law implementing Security Council resolutions 1267 and 1373, discussed above.

Put simply, the UK Supreme Court concluded that the comprehensive sanctioning mechanisms put in place by the Orders were *ultra vires* the very general authority delegated by Parliament in the *United Nations Act, 1946*. In the words of Lord Hope, "as fundamental rights may not be overridden by general words, section 1 of the 1946 Act does not give authority for overriding the fundamental rights of the individual".[111] However, as Lord Roger suggested, this deficiency might be corrected if the Order were actually authorized by appropriate legislation passed by Parliament.[112] In his words, "the essential point is that these matters [concerning implementation of the Security Council's counter-terrorism resolutions] should not pass unnoticed in the democratic process and that the democratically elected Parliament, rather than the executive, should make the final decision that this system, with its inherent problems, should indeed be introduced into our law."[113] This approach was, in fact, subsequently followed by the UK government for its unilateral listing system, resulting in the enactment *Terrorist Asset-Freezing (Temporary Provisions) Act 2010*, c.2. (In relation to the

---

[109] *Terrorism Act, 2006*, s.21.

[110] *Terrorism Act, 2000*, s. 5.

[111] *Ahmed and al-Ghabra*, at para. 76.

[112] *Ibid* at 176.

[113] *Ibid* at para. 186.

000105

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

1267 process, the UK introduced new regulations under the *European Communities Act 1972*, discussed above, incorporating the EU 1267 implementation process into UK law).

A second case concerns the proscribed terrorist organization list under the *Terrorism Act, 2000*, c.11. *Lord Alton of Liverpool v. Secretary of State for the Home Department*, [2008] EWCA Civ 443 concerned the listing of the People's Mojahadeen Organisation of Iran (PMOI) and a subsequent refusal by the Secretary of State to delist the organization. The latter decision was appealed to the Proscribed Organisations Appeals Commission, which allowed the appeal on the basis that the PMOI was not an organization "concerned in terrorism", as this expression is understood under the *Terrorism Act 2000*. The Commission denied leave to appeal to the Court of Appeal, and that application was renewed before the Court by the Secretary of State.

The Court of Appeal agreed with the Commission's interpretation of the listing rules, holding that:

> 37 … an organisation that has no capacity to carry on terrorist activities and is taking no steps to acquire such capacity or otherwise to promote or encourage terrorist activities cannot be said to be 'concerned in terrorism' simply because its leaders have the contingent intention to resort to terrorism in the future. The nexus between such an organisation and the commission of terrorist activities is too remote to fall within the description 'concerned in terrorism'.
>
> 38. An organisation that has temporarily ceased from terrorist activities for tactical reasons is to be contrasted with an organisation that has decided to attempt to achieve its aims by other than violent means. The latter cannot be said to be 'concerned in terrorism', even if the possibility exists that it might decide to revert to terrorism in the future.

3. Literature

Middleton, Ben. "Terrorism Act 2000: seeking deproscription." (2008) 72 *Journal of Criminal Law* 270.

This brief article is a case comment on *Lord Alton of Liverpool v. Secretary of State for the Home Department*, [2008] EWCA Civ 443. The article describes the factual backdrop to the case and the Court of Appeal's holding. In its commentary on the

000106

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

decision, the author notes the vagueness and breadth of the proscription rules. He argues, however, that this case runs counter to the propensity of courts to defer to the executive in matters of national security, perhaps because the Proscribed Organisaton Appeals Commission was specifically set up as an appeal body in relation to proscription decisions. The author notes that the conventional (and deferential) judicial review standard of review anticipated by the Act has been overtaken in this case by a more thorough scrutiny of the issues.

C. Discussion and Conclusions

As our findings suggest, the UK literature on UK-specific terrorism listing rules appears to be virtually non-existent, amounting to a single article.[114] In part, this probably stems from the fact that the UK is part of the EU, and UK academics have focused on the EU listing system. (The more plentiful UK articles dealing with the EU listing system are discussed in the EU section). It should be expected, however, that with the very recent release of the UK Supreme Court decision in *Her Majesty's Treasury v Mohammed Ahmed and al-Ghabra (FC)* [2010] UKSC 2, new articles will appear within the next year.

Reviewers may also be interested in the UK public consultation document on the draft terrorist asset-freezing bill proposed to respond to *Ahmed and al-Ghabra*. [115] Of particular note, that document anticipates that in judicial review of government decisions under the proposed draft bill, special advocates will be used in the closed proceedings in which intelligence material is introduced as evidence.

PART FOUR: UNITED STATES

A. Methodology

General searches of the following electronic data bases were conducted under the words "listing of terrorists" and "terrorist listings" ,"terrorist proscriptions", "terrorist designation", "Executive Order 13224", "Specially Designated Global Terrorist" and "Foreign Terrorist Organization" and the United States. The databases searched included Social Science Research Network,[116] Hein Online,[117] and Legal Trac as well as searches using Google and Google scholar on the web.

---

[114] There are a few articles on money laundering and terrorism finance, but these do not deal with listing *per se*.

[115] United Kingdom HM Treasury *Public Consultation Draft Terrorist Asset Freezing Bill* CM 7852 (March 2010)

[116] Available at http://www.ssrn.com/lsn/index.html

[117] Available at http://heinonline.org.myaccess.library.utoronto.ca/HOL/Welcome?collection=journals

000107

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

B. Findings

1. Legislation

a) Specially Designated Global Terrorist (SDGT)

The United States implements the UN 1267 listing process pursuant to Executive Order No. 13224, an instrument issued under the *International Emergency Economic Powers Act* (IEEPA), 50 U.S.C.S. §§ 1701-1706. The latter permits the President to "deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy or economy of the United States".[118] Subsequently, the President may, e.g., "investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States".[119] Other sources of legislative authority for EO 13224 include the *National Emergencies Act*, 50 U.S.C. 1601 et seq., section 5 of the *United Nations Participation Act of 1945*, 22 U.S.C. 287c (UNPA), and section 301 of title 3, United States Code (3 U.S.C. 301). Regulations implementing EO 13224 are found as 31 C.F.R. 594.

b) Foreign Terrorist Organization Listing

The United States has a separate terrorist organization listing process, situated in the *Immigration and Nationality Act* (INA), 8 U.S.C. 1189(a). This provision authorizes the designation of foreign terrorist organizations, where that organization engaged in terrorist activity or retains the capability and intent to do so and that terrorist activity threatens US security or nationals. Once designated, a terrorist organization's assets may be frozen. Pursuant to section 2339B of the U.S. *Criminal Code* (18 U.S.C 2339B), it is also a crime for anyone to provide material support or resources to a designated organization.

2. Court Cases

---

[118] 50 USC s. 1701.

[119] 50 USC s.1702.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Executive Order No. 13224 originally empowered the Secretary of Treasury, in consultation with the Secretary of State and Attorney General, to designate "persons" (broadly defined to include individuals or entities and sometimes described as "Specially Designated Global Terrorists" or SDGT) whose property should be blocked because they "act for or on behalf of" or are "owned or controlled by" designated terrorists, or because they "assist in, sponsor, or provide financial, material or technological support for, or financial or other services to or in support of" or are "otherwise associated" with them. The language of "otherwise associated" was declared unconstitutional for vagueness in *Humanitarian Law Project v. U.S. Department of Treasury*, 463 F. Supp. 2d 1049, 1070-71 (C.D. Cal. 2006). In the result, a regulation (31 C.F.R. § 594.316) was issued defining "otherwise associated" to refer to "(a) To own or control; or (b) To attempt, or conspire with one or more persons, to act for or on behalf of or to provide financial, material, or technological support, or financial or other services to." The U.S. Federal District Court for the Central District of California concluded that this clarification cured the provisions constitutional deficiency in *Humanitarian Law Project v. U.S. Department of Treasury*, 484 F.Supp.2d 1099 (C.D. Cal. 2007). Subsequently, the Court of Appeals for the 9th Circuit held in *Humanitarian Law Project v. U.S. Department of Treasury*, 578 F.3d 1133 (9th Cir. 2009), that Humanitarian Law Project lacked standing to challenge the presidential listing authority under Executive Order No. 13224, as it itself was not a designated organization, and at any rate, its further constitutional challenge for vagueness to the regulation's reference to "services" failed on the merits.

A second challenge to the EO 13224 process arose in the Kindhearts for Charitable Humanitarian Development, Inc. cases. In that protracted case, Kindhearts assets were blocked pending investigation by the Treasury. In August 2009, the Federal Court for the Northern District of Ohio ruled in *KindHearts for Charitable Humanitarian Dev., Inc. v. Geithner*, 647 F. Supp. 2d 857 (N.D. Ohio 2009) that the government action 1) violated Fourth Amendment rights (by failing to obtain a warrant based on probable cause), 2) violated Fifth Amendment rights (by depending on criteria for the blocking pending investigation that were unconstitutionally vague and by failing to provide Kindhearts with adequate notice and a meaningful opportunity to respond) and 3) was arbitrary and capricious in limiting Kindheart's access to its own funds to pay for defence counsel. On the question of remedy, the Federal District Court ordered in 2010 that the government must show probable cause and notice for its blocking investigation.

Not every US court has arrived at the same constitutional findings. For instance, the Federal District Court for the District of Oregon found no Fourth Amendment violation in a EO 13224 blocking order at issue in *Al Haramain Islamic Foundation, Inc. v. U.S. Department of the Treasury*, Civil Case No. 07-1155-KI (November 5, 2009).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Likewise, the U.S. Court of Appeals for the District of Columbia Circuit rejected a number of constitutional and administrative objections to listing pursuant to EO 13224 in *Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156 (D.C. Cir. 2003), a decision later followed in *Islamic American Relief Agency v. Gonzales*, 477 F. 3d 728 (D.C. Cir. 2007). For its part, the US Court of Appeals for the Seventh Circuit rejected constitutional due process claims in a challenge to the SDGT system in *Global Relief Found., Inc. v. O'Neill*, 315 F.3d 748 (7th Cir. 2002). Another due process challenge failed in *Al-Aqeel v. Paulson*, 568 F. Supp. 2d 64 (D.D.C. 2008).

The FTO designation rules have also sparked challenges. The most recent decision of note was the *Humanitarian Law Project* v. *Mukasey*, 552 F.3d 916 (9th Cir., 2009), until June of 2010. This decision was the latest in a series of cases, beginning in the late 1990s, that challenged the criminalization of the provision of material support or resources to designated organizations on vagueness grounds. Often successful, these challenges have sparked a number of amendments to section 2339B, designed to clarify its reach. One of these amendments included adding a prohibition on providing a "service" to a designated organization as a form of "material support or resources". Amendments also defined "training", already a form of material support or resources, as "instruction or teaching designed to impart a specific skill, as opposed to general knowledge."

In above-cited 2009 decision, the Court of Appeal for the Ninth Circuit held that the reference to "services" was unconstitutionally vague – not least because it could capture such things as advice or assistance on how, e.g., to lobby or petition the United Nations (at 930). The definition of "training" was also adjudged insufficient "[b]ecause we find it highly unlikely that a person of ordinary intelligence would know whether, when teaching someone to petition international bodies for tsunami related aid, one is imparting a 'specific skill' or 'general knowledge'" (at 929).

In June 2010, this series of cases culminated in *Holder v. Humanitarian Law Project*, 561 U.S. _(2010), a decision of the U.S. Supreme Court. By the time of that decision, the plaintiff claimed that four types of "material support" prohibited by section 2339B – "training", "expert advice of assistance", "service" and "personnel" were impermissibly vague (and therefore violated the Fifth Amendment's due process clause) and violated the First Amendment rights of free speech and association. The US Supreme Court disagreed, holding that the provisions were not unconstitutionally vague because they provided a person of ordinary intelligence with fair notice of what is prohibited. Further, the narrow prohibition on speech encompassed by the prohibition meets a compelling governmental objective and survived First Amendment scrutiny, at least insofar as it covers the types of support that the plaintiffs sought to provide. Nor was there a basis to conclude that free association rights were impinged by a provision that relates, not to membership, but to the provision of material support.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

It is worth noting that the UN Human Rights Committee, in "Consideration of Reports Submitted by States Parties under Article 40 of the Covenant: Concluding Observations of the Human Rights Committee – United States of America" CCPR/C/USA/CO/3/Rev.1, expressed "its concern about the potentially overbroad reach of the definitions of terrorism under domestic law, in particular under 8 U.S.C. § 1182 (a) (3) (B) and Executive Order 13224 which seem to extend to conduct, e.g., in the context of political dissent, which, although unlawful, should not be understood as constituting terrorism" (at para. 11).

An earlier challenge to the FTO designation process concerned due process questions – specifically, notice and a hearing prior to designation. In *National Council of Resistance of Iran v. Department of State*, 251 F.3d 192 (DC Cir. 2001), the US Court of Appeals for the District of Columbia held that "as soon as the Secretary has reached a tentative determination that the designation is impending, the Secretary must provide notice of those unclassified items upon which the proposes to rely to the entity to be designated. There must then be some compliance with the hearing requirement of due process jurisprudence—that is, the opportunity to be heard at a meaningful time and in a meaningful manner" (at 209). The matter was remanded to the Secretary of State, which re-designated the organization after giving the National Council of Resistance (and the organization was said to be affiliated with, the People's Mojahedin Organization of Iran ("PMOI")) with an opportunity to respond to non-classified information. PMOI challenged this decision in the US Court of Appeals for the District of Columbia on the basis that the reliance on classified information violated constitutional due process. The Court of Appeals rejected this argument in *People's Mojahedin Org. v. Department of State*, 327 F. 3d 1238 (D.C. Cir. 2003).

3. Literature

Chesney, Robert. "The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention," (2005) 42 *Harv. J. On Legis.* 1

This article focuses on 18 U.S.C. 2339B, the provision governing material support to a designated Foreign Terrorist Organization. It proposes changes to this law designed to alleviate certain civil liberty concerns. The article commences with a review of the origins and evolution of US terrorism-support laws. The article critiques these laws from both a civil liberties and national security perspective, focusing on constitutional issues that have been raised by courts. These include due process and freedom of expression concerns, and questions of vagueness and overbreadth. It then makes a number of reform recommendations, including new rules on active

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

membership in the Foreign Terrorist Organization with the specific intent of furthering its aim.

Chugani, Sumeet H. "Benevolent blood money: terrorist exploitation of Zakat and its complications in the war on terror." (2009) 34 *North Carolina Journal of International Law and Commercial Regulation* 601.

This article examines terrorist funding and includes an examination of charities designated as SDGT. The article begins with a brief overview of terrorism financing and its relevance to the 9/11 attacks and then examines surreptitious avenues of terrorist funding, including the Zakat system. The article then examines the US anti-terrorism financing provisions, including EO 13224, after which it examines cases of charities designated as terrorist organizations. The article questions whether the US measures reach too far and whether terrorism financing provisions are truly effective. The article questions whether the measures comply with the Fifth Amendment's due process clause and the First Amendment freedom of religion protections. It also examines the impact of the listing measures on Muslims and Muslim charitable giving.

Cole, David. "The New McCarthyism: Repeating History in the War on Terrorism," (2003) 38 *Harvard Civil Rights-Civil Liberties Law Review* 1.

This article critiques the response to the events of 9/11 from a civil liberties perspective. A portion of it examines the material support provisions found in 18 U.S.C. 2339B. The article urges that these laws are particularly attractive to prosecutors because of their overbreadth and their ability to criminalize otherwise innocuous behaviour. It describes these rules as a classic instance of guilt by association and rejects arguments that see contributions to designated organizations as freeing up resources that can be used to more malevolent purposes.

Donohue, Laura K. "Constitutional and legal challenges to the anti-terrorist finance regime," (2008) 43 *Wake Forest Law Review* 643

This article discusses the constitutionality of the SDGT and FTO designation processes. In relation to the SDGT system, operationalized by EO 13224, the author suggests that the process deviates from the governing statute – the International Economic Emergency Powers Act (IEEPA) – but concludes that courts are unlikely to declare the measure *ultra vires*.

The article traces the history of the IEEPA and its use since 1977. It then examines the much more extensive use of the instrument since 2001, especially as

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

directed at sanctioning individuals (as opposed to states). The article focuses particular attention in EO 13224. In relation to the Foreign Terrorist Organization listing, the article examines its origins in the mid-1990s as part of the 1996 Antiterrorism and Effective Death Penalty Act (amending the *Immigration and Nationality Act*). The article traces actual use of the listing process since that time.

In its discussion on constitutional matters, the article focuses on: procedural due process concerns with designation; the impact of listing on access to legal advice and resources to bring suit; substantive due process and equal protection; vagueness and overbreadth; privacy rights and search and seizure; and the question of whether EO 13224 is *ultra vires* its governing statute.

Folendorf , Carrie. "Breaking Terror's Bank Without Breaking the Law: A Comment on the USA Patriot Act and the United States Financial War on Terrorism" (2003) 23 J. NAALJ 481.

This article argues that EO 13224 violates several constitutional protections, including: the First Amendment freedom of association and the Fifth amendment due process clause. It begins with a history of asset freezing in relation to enemies and the origins and use of the *International Emergency Economic Powers Act* (IEEPA). It then focuses on the *Anti-terrorism and Effective Death Penalty Act* and the foreign terrorist organization designation process it introduced into US law, before examining EO 13224. It then examines the changes made to these laws by the US PATRIOT Act. The article argues that these laws infringe freedom of association rights in their overbroad criminalization of material support directed only to aid legal and political activities of designated organizations. The author's Fifth Amendments objections relate to the absence of meaningful notice and comment in the listing process.

Furst III, Joseph. "Guilt By Association and the AEDPA's Fund Raising Ban," (1999) 16 N.Y.L. Sch. J. Hum. Rts. 475.

This pre-9/11 article constitutes an early critique of the material support provisions introduced into US law in the 1996 *Anti-terrorism and Effective Death Penalty Act*. It urges that these rules amount to guilt by association and questions whether the provision complies with the First Amendment free speech. The article proposes an alternative model for barring terrorism fundraising, one that links material support to specific intent to fund an act of international terrorism.

Gurule, Jimmy. *Un-Funding Terror: The Legal Response to the Financing of Global Terrorism* (Edward Elgar Publ. 2008)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

This book provides an overview of the US designation instruments (including EO 13224 and the Foreign Terrorist Organization listing process) as well as other terrorism financing laws before focusing on whether this system has been effective is cutting off the flow of funds to international terrorists. It concludes that, in fact, the legal response to terrorism finance has been a failure in terms of starving Al Qaeda and the Taliban of funds. On the other hand, the regime has made it more difficult for jihadist sympathizers to fundraise and transfer funds. Among other things, the ability of corrupt Islamic charitable organizations to finance terrorist activities has been disrupted. The book argues, however, that criminal prosecutions in the US have been disappointing, the number of listings has fallen off, and the regime has not responded to new forms of terrorism financing (such as the drug trade).

Hardister, Angela D., "Can We Buy Peace On Earth?: The Price of Freezing Terrorist Assets in a Post-September 11 World," (2003) 28 *North Carolina Journal of International Law and Commercial Regulation* 605.

This article focuses on EO 13224, examining its origin and rationale. It describes the bureaucratic process whereby an organization is listed under the EO before examining the various legal basis for the measure, including the *International Emergency Economic Powers Act*. The article also discusses UN Security Council resolution 1373 and some of the international response to implementing it. Later, it examines whether asset freezing is consistent with US international trade law obligations, concluding that they are, and the implications of the US measures for its relations with other states. While the author describes the US measures as "aggressive", she urges that it is preferable to what she describes as the United Nation's "wait and see approach", allowing more terrorism financing.

Jonkait, Randolph. "A Double Due Process Denial: The Crime of Providing Material Support or Resources to Designated Foreign Terrorist Organizations," (2003-2004) 4a8 N.Y.L. Sch. L. Rev. 125.

This article focuses on section 2339B and the material support for foreign terrorist organization provision. It argues that this provision constitutes a double due process denial. It depends, for one thing, on the designation of a Foreign Terrorist Organization by the Secretary of States. That listing is done, however, without notice or a hearing in violation of due process. Second, the defendant in a section 2339B proceeding is barred from challenging the validity of the designations, again denying due process. In the result, the section 2339B process is unconstitutional. The article proposes amendments

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

to avoid these problems by permitting organizations notice of imminent designation and a hearing to contest the designation.

Nice-Petersen, Nicole. "Justice for the 'Designated': The Process that is Due to Alleged U.S. Financiers of Terrorism," (2005) 93 Geo. L.J. 1387.

This article focuses on the *International Emergency Economic Powers Act* and EO 13224, arguing that while the Act raised few constitutional issues when used to direct sanctions against foreign states, its use to authorize the freezing of assets of US entities raises constitutional due process questions. Specifically, the designation procedures fall short of basic due process standards – designated persons have no notice of the charges against them and lack a meaningful opportunity to be heard before a neutral arbiter. Further, the evidence against the person is classified, compounding the prospect of erroneous deprivations of their property. The article traces the history of the SDGT system and examines the court challenges to it existing at the time of the article. It then traces the constitutional requirement of due process and describes the risk of erroneous deprivation of property interests.

O'Leary, Robert E., "Improving the Terrorist Finance Sanctions Process," (2010) 42 N.Y.U. J. Int'l L. & Pol. 549.

This recent article proposes changes to the IEEPA and EO 13224 to enhance the effectiveness and legitimacy of the SDGT designation process. It begins with an overview of the IEEPA and EO 13224 and then a detailed overview of the actual designation process. It then examines judicial review of the designation process. Subsequently, the article highlights critiques of the system, including: the highly discretionary and prosecution-like power of the government, and the difficulty in successfully judicially reviewing its determinations; the potential ineffectiveness of asset freezes in dealing with informal money transfer systems (such as zakat); the tensions between the US and European states over asset freezes conducted through the UN 1267 system; and, the marginalization of Muslims who feel that legitimate charities are being targeted. The article then proposes a reformed system involving a National Security Sanctions Court empowered to impose a more nuanced designation.

Ortblad, Vanessa, "Criminal prosecution in sheep's clothing: the punitive effects of OFAC freezing sanctions," (2008) 98 *Journal of Criminal Law and Criminology* 1439.

This article focuses on the IEEPA and EO 13224. It criticizes the SDGT system as sometimes based on flimsy evidence, done without due process and subjected to

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

inadequate oversight. It examines in detail the evidentiary standard employed for designation, examining the implications of using minimal evidentiary standards, the punitive effects of the asset freezing process and the effectiveness of the SDGT process. The article concludes that judicial review is usually inadequate in curing deficiencies in the listing process because of the deferential standard of review applied by courts. The article argues that legislation should prescribe clear evidentiary standards and reporting requirements certifying compliance with this standard.

Piers, Matthew J. "Malevolent destruction of a Muslim charity: a commentary on the prosecution of Benevolence International Foundation," (2005) 25 *Pace Law Review* 339.

This commentary, authored by a lawyer for a Muslim charity designated a SDGT under EO 13224, offers a chronology of the listing of that organization and subsequent efforts to fight that designation, ultimately resulting in the collapse of the organization. The article condemns the listing process as lacking positive effect in counter-terrorism and as widely perceived in the Arab and Muslim community as unfair targeting of innocent Arab and Muslims.

Roth, John, Douglas Greenberg, Serena Willie, "National Commission on Terrorist Attacks Upon the Untied States: Monograph on Terrorist Financing," Staff Report to the Commission (2004).

This research study prepared for the 9/11 commission raised concerns about the SDFT process, focusing on several case studies. Two case studies focused on Islamic charities in which there was "little compelling evidence that…these charities actually provided financial support to al Qaeda – at least after…1999" (at 111). The two charities were shut down at "considerable cost of negative public opinion in the Muslim and Arab communities, who contend that the government's destruction of these charities reflects bias and injustice with no measurable gain to national security" (at 111).

Shapiro, Julie B. "The politicization of the designation of foreign terrorist organizations: the effect on the separation of powers," (2008) 6 *Cardozo Public Law, Policy & Ethics Journal* 547.

This article focuses on the Foreign Terrorist Organization designation process. It begins by summarizing the process for FTO designation under 8 U.S.C. 1189. It then examines how this statute affects the balance of powers among the branches of government, focusing in particular on the role of the courts. The article focuses on the limited basis for judicial review of FTO designations. It concludes that judicial review is

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

too constrained, and the role of the courts unduly diminished. As a result, the executive branch exercises too much control over the designation process. The article argues in favour of a rebalancing of powers, particularly given what the article views as the growing politicization of the FTO process (in relation to revolutionary dissident groups).

Stampley, Danielle. "Blocking Access to Assets: Compromising Civil Rights to Protect National Security Or Unconstitutional Infringement On Due Process And The Right To Hire An Attorney?" (2008) 57 Am. U.L. Rev. 683.

This article focuses on the IEEPA and EO 13224 and specifically the question of due process. It begins with an overview of these legal instruments, noting the broad powers they accord the executive. It then examines the constitutional due process jurisprudence to identify the standards that should apply to SDGT proceedings, with a specific emphasis on notice and hearing requirements. The article argues that the SDGT system is too constraining of due process, especially in relation to the release of funds to pay attorneys' fees. The article proposes that the system be overhauled to permit greater access to resources to pay for lawyers.

Wyatt, Micah, "Designating Terrorist Organizations: Due Process Overdue" (2008-2009) 39 Golden Gate U. L. Rev. 221.

This article focuses on the Foreign Terrorist Organization designation process under 8 USC 1189. It argues that FTO process is bereft of basic due process protections: it does not provide notice of designation or an opportunity to be heard before an unbiased decision maker. The article begins with an overview of the FTO process (and the criminalization of material support under section 2339B). It then examines the extent to which constitutional due process standards should extend to organizations being considered for listing, and juxtaposes these due process protections against what the statute provides. It examines the jurisprudence grafting some additional due process protections onto the FTO process and notes that even with this judicial gloss, the system is still inadequate. Specifically, the listing decision is never made by an unbiased adjudicator. The article proposes that the statute be amended to create such an unbiased decision-maker.

C. Discussion and Conclusions

As in other sections, it is not always possible to truly typecast the literature into categories based on whether authors support listing as is, support with amendments or

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

oppose outright. At least some of the literature is narrowly focused on the caselaw, without discussing the merits of listing more generally.

There is at least one author who supports listing – Garule – although even he doubts its efficacy. Hardister is also generally sympathetic to at least the U.S. domestic listing system. It is fair to say, however, that the US legal literature is overwhelmingly hostile to the SDGT and FTO designation processes, with almost all of the critique relating to due process deficiencies (notice, hearings, use of confidential intelligence, inability by designated organizations to use assets to pay for lawyers). Many authors are skeptical that judicial review can cure those deficiencies, although a certain proportion of this literature pre-dates some of the recent cases in which US courts have imposed constitutional standards (including in relation to due process) onto the system. Writers who seem most animated in their doubts concerning the listing concept *per se* include Cole and Piers.

While the preoccupation with due process is a recurring theme for almost all of the jurisdictions examined in this report, the US literature differs in three key respects. First, it is almost entirely silent on the United Nations context. The focus in the literature is almost exclusively on US law, and Security Council resolutions and listing obligations are rarely mentioned. There is, in other words, little or no concern with reconciling domestic due process concerns with the due process deficiencies of the 1267 process. (US authors do write on the 1267 process, as the section on that process in this report indicates. However, the US literature easily partitions into articles on public international law instruments such as the 1267 system and articles on domestic designation. Very few articles straddle that divide, and none seems to engage the question of reconciliation between the two processes in a manner analogous to many of the post-*Kadi* EU articles).

Second, a number of the US articles go beyond a critique to imagine reforms to the US listing system that would cure some of its shortcomings. Notable proposals include the creation of special national security or listing courts that would adjudicate designations, removing the matter from the hands of the executive and, in the views of authors supporting such a move, rebalancing a distortion in the separation of powers that exists at present and curing a core due process shortcoming; the absence of a hearing on the listing in front of an impartial adjudicator. The authors who propose modified listing regimes include Chesney, Furst, Jokait, O'Leary, Ortblad, Shapiro, Stampley and Wyatt.

Third, the US literature includes critiques on the effectiveness of listing and its role as a counter-terrorism tool and also addresses collateral consequences of listing, including perceptions in the Muslim community of harassment.

PART FIVE: AUSTRALIA

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

A. Methodology

General searches of the Australian Legal Information website were conducted using the phrases "listing" and "proscription" and terrorism and terrorist group and organisation both in terms of their comprehensive collection which includes both jurisprudence and law journal articles. In addition, these terms were also searched in the Social Science Research Network[120] Hein Online[121] the Legal Journals index (UK), Legal Trac, World Journals and Law Reviews (Westlaw), Informit, AustLii, Scaleplus, and BarNet Jade (www.jade.barnet.au) and google and google Scholar.

B. Findings

1. Legislation

There are two main means to list groups and individuals associated with terrorism in Australia. Division 102 of the Commonwealth Criminal Code (*Criminal Code Act 1995*, Act No. 12 of 1995, as amended) provides a means for terrorist groups to be listed. Section 101.2 provides that the Attorney General:

> must be satisfied on reasonable grounds that the organisation:
>
> (a) is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not a terrorist act has occurred or will occur); or
>
> (b) advocates the doing of a terrorist act (whether or not a terrorist act has occurred or will occur).

A terrorist organisation is defined as either a group listed by regulation or a group that otherwise satisfies the above definition. The listing of a terrorist group is subject to a renewable two year time period. The main review for listings are Parliamentary with requirements that the Leader of the Opposition be briefed before a regulation listing a group is made.[122] In addition, there are subsequent reviews at three year intervals by the Parliamentary Committee responsible for the review of Australia's security intelligence agencies.[123] The original 2002 legislation required that terrorist groups listed domestically also be listed by the UN but this was changed by 2004 amendments.

---

[120] Available at http://www.ssrn.com/lsn/index.html

[121] Available at http://heinonline.org.myaccess.library.utoronto.ca/HOL/Welcome?collection=journals

[122] *Commonwealth Criminal Code*, s.102.2(2.A)

[123] Ibid s.102.1 (A)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The second means of listing is provided by the *Suppression of the Financing of Terrorism Act, 2002*, No. 66 of 2002. This act amended the *Charter of the United Nations Act, 1945* to provide that the Minister or the Governor in Council by regulation may list a person or entity if doing so would 1) give effect to a Security Council decision under Chapter VII of the United Nations Charter, 2) Article 25 of the Charter requires Australia to carry out the obligation and 3) the matter relates to terrorism.[124] The Minister may revoke the listing if those grounds do not apply.[125] A listed person may apply to the Minister to revoke the listing.[126] It is a strict liability offence subject to five years imprisonment to give assets to a listed or proscribed person or entity with the Minister being able to make certain exemptions.[127]

2. Court Cases

No court cases were identified directly challenging the Australian listing procedures.

3. Australian Law Reform Proposals

A notable feature of the Australian listing process is a variety of proposals that have been made to change the listing process, particularly in relation to terrorist organizations under the Criminal Code.

Report of the Security Legislative Review Committee (June 2006).

This report, commonly known as the Sheller Review Committee, devoted two chapters to the listing of terrorist groups.[128] It recommended that in order to conform to administrative law principles that the organizations and affected individuals should be provided with advance notice of listing except where not practicable.[129] It also recommended that either an advisory committee of retired judges and experts in security and policing be created to advise the Attorney General of Australia about the listing of terrorist groups or that listing be decided in Federal Court on application by the Attorney General of Australia with notice to affected individuals and groups.

On the notice issue, the Sheller Committee noted that while it may be impracticable to notify overseas organizations before listing that there is "is every

---

[124] *Charter of the UN Act 1945*, s.15

[125] Ibid s.16

[126] Ibid s.17

[127] Ibid ss.21 and 22.

[128] *Report of the Security Legislative Review Committee* June 2006 Simon Sheller chair chapters 8 and 9

[129] Ibid at Recommendation 3

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

reason why an Australian organisation and its members should be given an opportunity to oppose the proscription of the organisation."[130] After examining a variety of legal and community submissions, the Committee concluded that "better transparency and additional measures" were needed "to foster community confidence" in the listing process.[131] The Committee then examined a number of reform options including listing by a court, an independent tribunal, or the Attorney General acting with an independent advisors. The Committee was divided in its views concluding that "Some members favour the view that the process for proscription of an organization as a terrorist organisation be a judicial process brought by application to the court, with service on affected parties and an open hearing so far as that is practicable. Other members … favour retaining the Attorney- General's role with some additional safeguards."[132]

Judicial involvement was thought to increase both the "procedural fairness" and "transparency" of the process and with that "help reduce the fear of discrimination and error".[133] Those on the Committee who supported retaining the role of the Attorney General stressed the need for continuing review of a listing and concerns that it would be "awkward and perhaps impractical"[134] to give the court a continuing review function.

The division of views within the Commission is reflected in its final recommendations. At the same time, all members agreed that some reform was necessary to increase the procedural fairness and transparency of the listing proposal by providing notice prior to listing "where practicable". The final recommendations of the Sheller Committee were as follows:

> 9.33 The SLRC recommends that the process of proscription be reformed to meet the requirements of administrative law. The process should be made more transparent and should provide organizations, and other persons affected, with notification, unless this is impracticable, that it is proposed to proscribe the organisation and with the right to be heard in opposition.
>
> 9.34 The SLRC recommends that either:

---

[130] Ibid at 8.15

[131] Ibid at 9.2

[132] Ibid at 9.3

[133] Ibid at 9.18

[134] Ibid At 9.24

000121

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

i. the process of proscription continue by way of regulation made by the Governor-General on the advice of the Attorney-General

In this case there should be built into that process a method for providing a person, or organisation affected, with notification, if it is practicable, that it is proposed to proscribe the organisation and with the right to be heard in opposition.

An advisory committee, established by statute, should be appointed to advise the Attorney-General on the case that has been submitted for proscription of an organisation. The committee would consist of people who are independent of the process, such as those with expertise or experience in security analysis, public affairs, public administration and legal practice. The role of the committee should be publicized, and it should be open to the committee to consult publicly and to receive submissions from members of the public.

Or

ii. the process of proscription become a judicial process on application by the Attorney-General to the Federal Court with media advertisement, service of the application on affected persons and a hearing in open court.

The Sheller Committee also noted that the grounds for proscribing a terrorist organization included not only direct or indirect involvement in terrorism but also advocacy of the doing of a terrorist act whether or not a terrorist act has or will occur. Advocacy of terrorism is defined as not only counseling or providing instruction for terrorist acts but also praising a terrorist act where "there is a risk that such praise might have the effect of leading a person (regardless of his or her age or any mental impairment…to engage in a terrorist act."[135] The Sheller Committee recommended that the praising of terrorism ground be removed as a ground for proscribing a

[135] Criminal Code 102.1(1A)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

terrorist organization. If this was not done, the Committee recommended that the provision be amended to require "a substantial risk" that the praise might lead someone to engage in a terrorist act.[136]

Parliamentary Joint Committee on Intelligence and Security *Inquiry into the proscription of 'terrorist organizations' under the Australian Criminal Code* (September 2007).

This report notes that 19 terrorist groups had been designated under the Australian Criminal Code process and concludes that "the current model of executive regulation and parliamentary oversight provides a transparent and accountable system that is consistent with international practice."[137] The report notes the existence of community concerns about the listing process and recommends clearer statutory criteria and better communication of the process used for listing. In another report, this Committee recommended advocacy not be removed as a ground for listing a terrorist group but that a terrorist group should only be listed on the basis that its praise of a terrorist act created "a substantial risk" that a person would engage in a terrorist act.[138] The report notes that to date no judicial review application had been made, but that one could be made on general administrative review grounds.[139] It also recommended that consideration be given to restoring the regime that existed prior to amendments made after the Bali bombings that would have the regulation listing an entity not take place until after a 15 day period that allows for Parliamentary disallowance of the listing. This report also details the procedure used by the committee to review listing decisions which includes private briefings on the basis of secret material provided by ASIO.[140] It concluded that Parliamentary review provides a valuable testing of decisions made by the executive and allows those opposed to the listing to make public presentations. It rejected claims that listing either discriminated against Muslims, infringed freedom of expression or precluded legitimate refugee claims by individuals. It also approved of the ability to depart from UN lists particularly where Australian interests are at stake.[141] It also rejected the Sheller Committee's proposals that either listing be done either judicially or that there be an independent advisory committee or a separate commission

---

[136] *Report of the Security Legislative Review Committee* June 2006 Simon Sheller chair at 8.10, 8.11

[137] Parliamentary Joint Committee on Intelligence and Security *Inquiry into the proscription of 'terrorist organizations' under the Australian Criminal Code* September 2007 at iii

[138] Parliamentary Joint Committee on Intelligence and *Security Review of Security and Counter Terrorism Legislation* at 71 Recommendation 14

[139] Ibid at 2.26

[140] Ibid at 2.36

[141] Ibid at 4.29

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

that could conduct a merits-based review. This Joint Committee expressed a preference for the Attorney General and the security intelligence agencies maintaining direct responsibility for listing subject to Parliamentary review and the possibility of non merits-based judicial review on administrative law principles and reconsideration by the Attorney General.[142]

National Security Legislation Discussion Paper on Proposed Amendments (July 2009).

This discussion papers make proposals for reforms to both the listing of terrorist groups under the Commonwealth Criminal Code and under the *Charter of the United Nations Act*. With regards to the former, it followed the 2007 recommendations of the Parliamentary Committee on Intelligence and Security and proposed that the listing of an organization should expire after three rather than two years. The purpose of the expiry is to require the AG to consider afresh the information that led to the listing.[143] It also followed the Parliamentary committee in recommending that listing of a terrorist organization on the basis of its praise of a terrorist should require that there be "a substantial risk" that a person would engage in a terrorist act. [144]It also proposed the addition of the following provision that would allow for aid organizations to be declared legitimate organizations in cases whether the Attorney General concludes that the provision of humanitarian aid "outweigh, or will outweigh, any benefits that could be received, directly or indirectly, by a terrorist organization as a result of the organization providing aid."[145] This provision would only provide an exemption from an offence of providing aid to a terrorist organization. The list would be subject to the same expiry and judicial review provisions as the list of proscribed organizations.[146] The proposed provision provided as follows:

> 102.8A Declared aid organisations and declared regional aid organisations
>
> (1) The Minister may declare, in writing, that:
>
> (a) an organisation is a *declared aid organisation;* or

---

[142] Ibid at 5.26

[143] National Security Legislation Discussion Paper on Proposed Amendments July 2009 at 59

[144] Ibid at 57

[145] Ibid at 66

[146] Ibid at 69

000124

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(b) an organisation is a *declared regional aid organisation* in respect of one or more particular geographical areas.

(2) The Minister must not make a declaration under subsection (1) in relation to an organisation unless the Minister is satisfied on reasonable grounds that:

(a) the organisation is, or will be, providing humanitarian aid to a community; and

(b) the benefits to that community of providing the humanitarian aid outweigh, or will outweigh, any benefits that could be received, directly or indirectly, by a terrorist organisation as a result of the organisation providing the aid.

(3) A declaration under subsection (1) in relation to an organisation may be made:

(a) on written application by the organisation; or

(b) on the Minister's own initiative.

(4) If an application for a declaration is made and the Minister does not make the declaration, the Minister must refuse to make the declaration.

(5) A declaration made under subsection (1) remains in force for the shorter of the following periods, unless earlier revoked:

(a) the period specified in the declaration;

(b) 3 years.

(6) The Minister must cause a notice of a declaration made under subsection (1) to be published in the *Gazette*.

(7) A declaration made under subsection (1) is not a legislative instrument.

102.8B Revocation of declaration

(1) The Minister may, in writing, revoke a declaration in relation to an organisation if the Minister is no longer satisfied of the matters in paragraphs 102.8A(2)(a) and (b) in relation to the organisation.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> (2) If the Minister revokes under subsection (1) a declaration under subsection 102.8A(1), the Minister must cause a notice of the revocation to be published in the *Gazette*.

Although this provision was included in a subsequent exposure draft bill[147], it was not included in the *National Security Legislation Amendment Bill*, 2010 because of concerns raised in the public consultation about how practical and workable such a list would be.[148] That Bill, however, followed the proposals made by both the Sheller Committee and the Parliamentary Committee on Intelligence that a terrorist group can only be listed on the basis of its praise for a terrorist act if such praises produces a "substantial risk" as opposed to a "risk" that a person would engage in a terrorist act. That Bill also proposes that the listing of an organization in the Criminal Code should expire after three years instead of the current two.[149]

With respect to listing under the *Charter of the United Nations, 1945 Act*, the Discussion Paper proposed that amendments made to require that listing of persons or entities or assets be made on "reasonable grounds" It also recommended that listings expire after three years to ensure consistency with the Criminal Code listing provisions.[150] Both of these recommendations are now contained in *National Security Legislation Amendment Bill*, 2010.[151]

An *Anti-Terrorism Law Reform Bill, 2009* introduced by Senator Ludlam also contained a variety of proposals to reform the listing of terrorist groups. They included advance notice where practicable to a group before it was listed and the creation of an independent advisory group with intelligence, political and legal expertise to advise the

---

[147] Exposure Draft available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(966BB47E522E848021A38A20280E2386)~SLB+-+National+Security+Legislation+Amendment+Bill+2009+Exposure+Draft.PDF/$file/SLB+-+National+Security+Legislation+Amendment+Bill+2009+Exposure+Draft.PDF

[148] See the 2nd reading speech by the Attorney General of Australia at: http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/2010-03-18/0039/hansard_frag.pdf;fileType=application%2Fpdf

[149] National Security Legislation Amendment Bill at p 15 Schedule 2 Terrorism available at http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r4320_first/toc_pdf/10072b01.pdf;fileType%3Dapplication%2Fpdf

[150] National Security Legislation Discussion Paper on Proposed Amendments July 2009 at 166-167

[151] National Security Legislation Amendment Bill at p 45 Schedule 7 Terrorsim available at http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r4320_first/toc_pdf/10072b01.pdf;fileType%3Dapplication%2Fpdf

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Attorney General on listing decisions and to hear representations from concerned citizens. Both the advisory group and the organization to be listed would have to be advised if the listing decision was at the request of a foreign country.[152]

4. Literature

Hocking, Jenny. "Counter-terrorism and the Criminalization of Politics: Australia's New Security Powers of Detention, Proscription and Control" (2003) 49 *Australian J of Politics and History* 355.

This article relates executive proscription of terrorist groups in Australia with the unsuccessful attempt in the 1950's in Australia to outlaw the Communist Party. Flaws in the process are related to overbroad definitions of terrorist activities and groups, the absence of any prior notice before a group is listed and limited administrative law procedural review after listing. Proscription is criticized as inherently undemocratic especially when viewed in conjunction with the many derivative terrorism offences that flow from proscription.

Joseph, Sarah. "Australian Counter-Terrorism Legislation and the International Human Rights Framework" [2004] 27 *University of New South Wales* 428.

This article argues that the exclusion of substantive judicial involvement from the proscription process may violate article 22 of the International Covenant on Civil and Political Rights which provides that "no restrictions may be placed on the exercise of this right other than those which are prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others" The author argues that a more proportionate approach to restricting freedom of association would require a judicial decision on proscription and that judicial oversight on the merits of proscription would help to protect against politically motivated or arbitrary proscriptions.[153] She noted that the legislative proscription of a fascist Party in Italy had been found by the Human Rights Committee

---

[152] Anti Terrorism Laws Reform Bill 2009 available at http://www.austlii.edu.au/cgi-bin/sinodisp/au/legis/cth/bill_em/alrb2009317/memo_0.html?stem=0&synonyms=0&query=listing%20and%20terrorism

[153] Sarah Joseph "Australian Counter-Terrorism Legislation and the International Human Rights Framework" [2004] 27 University of New South Wales 428 available at http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/UNSWLawJl/2004/29.html?stem=0&synonyms=0&query=listing%20and%20terrorism At fns 52-53

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

of the UN to be consistent with the ICCPR. The author stressed, however, that the Australian provisions involved executive as opposed to legislative proscription and that executive action had even less transparency than a legislative act. The author warns that the broad definition of terrorist activities increases the danger of abuse of the proscription process.

Ruddock, Phillip. "Australia's Legislative Response to the Ongoing Threat of Terrorism" (2004) 27 U.N.S.W.L.Rev. 254.

This article outlines how the original 2002 legislation to allow the proscription of terrorist organizations was amended in March 2004 to allow proscription that was not tied to the UN listing process and to enable Australia to respond to its own security needs. The failure of the UN to list Jemaah Islamiyah before the Bali bombing is cited in support of this change. The Australian listing process is defended as transparent in part because of requirements that the Attorney General be satisfied of the basis of the listing and Parliamentary review including briefing of the Leader of the Opposition. It is also noted that listings expire in two years and that delisting requests can be made to the Attorney General earlier who can apply for delisting.

Tham, Joo-Cheong. "Possible Constitutional Objections to the Powers to Ban 'Terrorist' Organisations" [2004] UNSWLawJl 31; (2004) 27(2) University of New South Wales Law Journal 482.

This lengthy and thoughtful article assesses both Australia's Criminal Code power to list terrorist organizations and the powers to list groups and individuals under its Charter of the United Nations Act as amended in 2002 from an Australian constitutional perspective. It finds that the listing powers in the Criminal Code disproportionately burdens political communication and association because of the breadth of the definition of terrorist groups, the possibility of discrimination in the listing process and the severe consequence of listing. At the same time, the author concludes that the regulations listing specific groups are probably constitutional because they are foreign groups not engaging in political communication and association in Australia. The author also concludes that the same provisions infringe constitutional protections of the judicial power by amounting to bills of attainder at least to the extent that membership in a listed or proscribed organization is an offence in itself under Australian law.

With respect to the UN listing powers, the article concludes that while they are supported by the Commonwealth's powers over external affairs, they also burden political expression and association in Australia. He also suggests that they may

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

infringe the judicial power by constituting a bill of attainder that effectively makes a person guilty of a criminal offence on the basis of legislative and executive as opposed to judicial acts.

Gani, Miriam and Gregor Urbas "Alert or Alarmed? Recent Legislative Developments Aimed at Terrorist Organizations and Persons Supporting or Assisting in Terrorist Acts" (2004) 8 Newcastle L.Rev. 23.

This article compares the power to list terrorist organization by regulation under the Criminal Code with powers enacted in Australian criminal law in 1926 that allowed the Attorney General to obtain a judicial order declaring organizations dedicated to rebellion and subversion to be illegal organizations. This latter power was never used, but is contrasted with both the ability of Ministers to list groups and individuals under the *Charter of the United Nations Act* and under amendments to the Criminal Code. It is also noted that before the 2004 amendments to the Criminal Code listing powers, legislation proscribing organizations that had not been listed by the UN was used, but that this legislative power was not necessary after the 2004 Criminal Code amendments allowing the Attorney General to list groups not necessarily listed by the UN. This article, like Tham's, also concludes that listing provisions may violate implied freedom of political communication and association as well as judicial power.

Hogg, Russell. 'Executive Proscription of Terrorist Organisations in Australia: Exploring the Shifting Border between Crime and Politics' in Miriam Gani and Penlope Mathew (eds) *Fresh Perspectives on the 'War on Terror'* (ANU Press, 2008).

This article examines the listing process under the Criminal Code. It examines the reviews of listing conducted by the Joint Parliamentary Committee noting that while the committee has never disallowed a listing, it has expressed reservations about the process. One reservation is the breadth of the legislative definition of terrorist organizations which makes the choice of listing selective and that it may involve organizations that participate in war crimes in conflict zones but not necessarily terrorism or terrorism that threatens Australian interests. It is suggested that proscription decisions of some groups could interfere with legitimate refugee claims and that some proscription decisions such as that of the PKK were made for political and diplomatic reasons. It also notes that the Parliamentary committee has complained that the Attorney General and ASIO has not provided full reasons for the listing of terrorist groups as well as a lack of participation by the Department of Foreign Affairs and lack of effective consultation about listing. The article notes that no prosecutions have taken place in Australian in relation to the 19 proscribed terrorist organizations.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

McGarrity, Nicola. "Review of the Proscription of Terrorist Organizations: What Role for Procedural Fairness? (2008) 16 *Australian J. of Admin Law* 45.

This paper examines the listing of terrorist groups under the Criminal Code and finds that existing mechanisms of review are inadequate and have not yet resulted in the delisting of a terrorist group. The Attorney General's self review of listing is deficient in part because of the high standard of being persuaded that there is no basis for the listing and the broad definition of a terrorist group. Review by Parliament is inadequate in part because of time restraints and a reluctance of the executive to share with Parliament all the reasons for the listing. Possible review in courts is inadequate in part because it is not merits-based and because the government would be able to maintain the secrecy of much of the information. The author suggests that prior notice wherever feasible as recommended by the Sheller committee should be implemented and giving groups an opportunity to respond before being listed is not inconsistent with either the protection of secret information or claims that listing must be done on an urgent basis.

Lynch, McGarrity and Williams "The Proscription of Terrorist Organizations in Australia" (2009) 37 *Federal Law Review* 1.

This recent and comprehensive 40 page article accepts that Australia will continue to proscribe terrorist groups both for denunciatory reasons and to facilitate enforcement of various anti- terrorism laws including those prohibiting terrorism financing. It focuses on means to improve the process of proscription under Division 102 of the Criminal Code as opposed to the *Charter of the United Nations Act* as amended by *Suppression of Terrorism Financing Act*. It explains how the listing of terrorist groups was originally limited to those listed by the UN Security Council but how this was changed in 2004 amendments. Listing is done by regulation issued by the Attorney General subject to Parliamentary disallowance and with advance consultation with states and territories and the Commonwealth Leader of the Opposition. It concludes that a listing of a terrorist organization will be conclusive in criminal proceedings and notes that a 2006 review committee concluded this might assist the accused by avoiding a trial on whether the organization was in fact listed. Listing decisions will only be subject to general judicial review for reasonableness or bad faith. It also notes that listing under the Criminal Code are also subject to review in the Joint Parliamentary Committee on Intelligence and Security. The article expresses concern about the political and arbitrary nature of listing, the possibility of discrimination against Muslims (18 of 19 groups listed are Muslim), the lack of transparency of the decision-

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

making process, and the serious penal consequences of a listing decision. The article considers the alternative of having the judiciary make listing decisions, but concludes that this would not be appropriate because of concerns about the limit of judicial capacity, most notably access to secret intelligence that may justify the listing. For similar reasons, the authors oppose merits-based judicial review of listing decisions. They propose the formation of an independent advisory body of retired judges and security and policing experts to engage in community consultation and challenge functions prior to listing. They propose the enactment of more specific legislative criteria for listing especially with regards to the threats that particular organizations pose to Australia and the adverse effects of listing on Australians. They also propose procedural fairness in the listing process including prior notification where possible. Finally, they propose the creation of a Proscribed Organization Appeal Commission as exists in Britain and allows special advocates to challenge the intelligence supporting a listing.

C. Discussion/Conclusions

The literature on the Australian listing process reflects many of the same themes as found with respect to other listing processes. In other words, most commentators have expressed concerns about the fairness of the listing process given that affected individuals and entities do not have prior notice of the listing or a full merits based before the judiciary. Indeed, the Australian literature and in particular the work of Tham and Gani and Urbas often features arguments that listing violates exclusive judicial powers and constitutes a bill of attainder by making by executive regulation what are in reality judicial determinations that a person or an organization is involved with terrorism.[154] Australian commentators take different positions on the optimal mechanism for reviewing listing decisions with Joseph arguing that there should be judicial review and Lynch, McGarrity and Williams arguing for Parliamentary review. They, however, join Hogg in arguing for a more robust and searching form of Parliamentary review.

We were not able to discover any court cases challenging terrorist listings under either the Australian Criminal Code or the Charter of the United Nations Act. The reasons for the absence of cases compared to some other jurisdictions studied are speculative. One possible reason is that listed persons may have a greater incentive to challenge listing decisions in large jurisdictions such as the EU and the US given that

---

[154] Tham, Joo-Cheong "Possible Constitutional Objections to the Powers to Ban 'Terrorist' Organisations" [2004] UNSWLawJl 31; (2004) 27(2) University of New South Wales Law Journal 482 available at http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/UNSWLawJl/2004/31.html?stem=0&synonyms=0&query=terrorism

000131

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

listing, especially when it is supported by 1267 listing, will likely occur in many nations and the remedy of being delisted in one jurisdiction may be quite limited. Another possible reason is that Australia's especially broad offences relating to membership and association with terrorist organizations may deter people from bringing such challenges. Another possible reason is the limited non-merits grounds for judicial review of listing decisions including the possibility that judicial review would be frustrated by state claims of secrecy.[155] Finally, the absence of a national bill of rights in Australia may also be a factor.

There are some shortcomings in the Australian literature. The vast majority of the literature focuses on the listing of terrorist groups under the Criminal Code as opposed to the listing of individuals under the UN Act. There is an absence of case studies either of cases of wrongful listings or of the effectiveness of listing as a counter-terrorism device. One article notes that the listing of 19 terrorist groups has not been used in any terrorism prosecution in Australia[156], but larger questions of the effectiveness (or lack thereof) of listing remain largely unexplored.

The Australian experience is perhaps most noteworthy for the attention that has been devoted to possible reforms of the listing process. The 2006 Sheller Committee was divided on whether having the judiciary determine listings or allowing an expert advisory panel conduct listing and delisting hearings was the best reform. [157] Since that time, some commentators have expressed a preference for the latter advisory panel reform in part on the basis that the judiciary may not have the expertise to deal with intelligence that may form the basis for the listing request.[158]

An advisory panel approach has also been discussed with regards to the UN 1267 process. An advisory panel could combine expertise with the ability to give affected individuals a hearing in a manner that may be difficult for Ministers at the domestic level or States at the regional/international level to do. At the same time, one possible objection is that a listed person who appears before an advisory panel would not be making representations to the actual decision-maker. In addition, allowance would have to be made for reconciling the competing goals of protecting sensitive intelligence from disclosure and allowing fair and full challenges to intelligence that

---

[155] Nicola McGarrity "Review of the Proscription of Terrorist Organizations: What Role for Procedural Fairness? (2008) 16 Australian J. of Admin Law 45.

[156] Russell Hogg 'Executive Proscription of Terrorist Organisations in Australia: Exploring the Shifting Border between Crime and Politics' in Miriam Gani and Penlope Mathew (eds) *Fresh Perspectives on the 'War on Terror'* (ANU Press, 2008.) available at http://epress.anu.edu.au/war_terror/pdf/whole_book.pdf

[157] *Report of the Security Legislative Review Committee* June 2006 Simon Sheller chair chapters 8 and 9.

[158] Lynch, McGarrity and Williams "The Proscription of Terrorist Organizations in Australia" (2009) 37 Federal Law Review 1.

000132

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

forms the basis for listing in an advisory committee. One possible response would be to rely on the expertise of the advisory committee and another would be to introduce some form of security cleared counsel who could see and challenge information not disclosed to the person challenging the listing. We note, however, that the adequacy of both responses is controversial and contested. As with the 1267 literature, the Australian literature does not really engage with these difficult and practical issues.

Another reform option that has emerged from the Australian experience is the idea of constructing a list of organizations that might fear being listed or prosecuted as terrorist organizations but that have established their bona fides as humanitarian organizations. Such proposals acknowledge concerns that listings can have overinclusive effects on humanitarian efforts and they provide a broader alternative to the ability of domestic Ministers or the 1267 Committee to make case specific humanitarian exemptions from travel bans and asset freezes. At the same time, such proposals place significant burdens on the applicant and have a "prove your innocence" type of quality. Although humanitarian exemptions have been available under most listing regimes since the start, they have not emerged in the literature as a main concern or a mitigation of more fundamental concerns about the fairness and effects of the listing process. Although more thought needs to be devoted in the literature to devising remedies for those who may have been wrongly listed as terrorist groups and the possibility of obtaining humanitarian exemptions, the burden and possible risk placed on an organization or individual that applies for a humanitarian exemption or for an advance ruling of whether they should be on a terrorist list should not be discounted. The same incentives that may explain why listing decisions in Australia have not to our knowledge been the subject of a court challenge may also make it difficult to rely on such individuals and organizations seeking clarification that they are not on a terrorist list. In general the literature on listing could be improved by examining the practical difficulties that are faced by those who wish to challenge listing. One advantage of using independent expert advisors is that they have the potential to exercise a challenge function both before and after listing. Nevertheless, such review does not respond to concerns about the absence of an effective judicial remedy in the listing process.

The Australian listing process is also notable for its use of Parliamentary safeguards both before and after listing. The leader of the Opposition and the state leaders are briefed before organizations are listed under the Criminal Code but not before individuals are listed under the *Charter of the United Nations Act*. A Joint Parliamentary committee on Intelligence and Security also reviews the Criminal Code listing. It has not invalidated a listing decision but has expressed reservations about the breadth of the definition of terrorist groups, lack of community consultation and lack of full information from the government about the listing. The consensus of

000133

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

commentators in Australia seems to be that Parliamentary review of listing has not been particularly effective.[159]

Recommendations for an advisory committee of experts or a proscribed organization appeal tribunal suggest that listing processes might be improved by including intelligence experts who can question the analysis, reliability and conclusions drawn by intelligence analysts. Such review has a potential to improve the accuracy of the listing process especially to the extent that it involves experts in intelligence who are in a good position to judge the reliability of the intelligence behind the listing. Nevertheless, review by an advisory committee of expert or a specialized tribunal likely will not respond to concerns that listed individuals or groups should have an opportunity to know and challenge the basis for their listing.

PART SIX: NEW ZEALAND

A. Methodology

General searches of the New Zealand database of World Legal Information website[160] were conducted using the phrases "listing" and "proscription" and terrorism and terrorist group and organization both in terms of their comprehensive collection which includes both jurisprudence and law journal articles. In addition, these terms were also searched in the Social Science Research Network[161] Hein Online[162] the Legal Journals index (UK), Legal Trac, World Journals and Law Reviews (Westlaw), Informit, AustLii, Scaleplus, and BarNet Jade (www.jade.barnet.au) and google and google Scholar.

B. Findings

1. The New Zealand Listing Process

---

[159] Russell Hogg 'Executive Proscription of Terrorist Organisations in Australia: Exploring the Shifting Border between Crime and Politics' in Miriam Gani and Penlope Mathew (eds) *Fresh Perspectives on the 'War on Terror'* (ANU Press, 2008.) available at http://epress.anu.edu.au/war_terror/pdf/whole_book.pdf ; Nicola McGarrity "Review of the Proscription of Terrorist Organizations: What Role for Procedural Fairness? (2008) 16 Australian J. of Admin Law 45.

[160] http://www.worldlii.org/catalog/242.html

[161] Available at http://www.ssrn.com/lsn/index.html

[162] Available at Available at http://heinonline.org.myaccess.library.utoronto.ca/HOL/Welcome?collection=journals

000134

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Before the 2002 New Zealand *Terrorism Suppression Act*, 2002 No. 34, New Zealand listed terrorist entities by regulations enacted under its *United Nations Act*, 1946 No. 7. It adopted *UN Sanctions (Afghanistan) Regulations* in both 1999 and 2001 to implement listing under the 1267 process.[163] Legislation enacted in 2002, the *Terrorism Suppression Act*, 2002 provided a statutory basis for listing both under the 1267 process and the broader freeze of assets of all terrorists contemplated under Resolution 1373. The Prime Minister under that Act has power to make both 30 day interim designations of terrorist entities on the basis of "good cause to suspect" and final designations of terrorist on the basis of a "reasonable grounds to believe" that the entity is involved with terrorist activities or that it has been listed as associated with terrorists by the UN including the 1267 Committee.[164] The 2002 Act provides that the Prime Minister may take into account any information including classified security intelligence when deciding whether to list or revoke a listing.[165]

The listing by the Prime Minister expired after three years and in the original version of the Act could only be renewed for another three year period if the Attorney General established in the High Court on a balance of probabilities that the entity was the subject of a terrorism prosecution in or outside of New Zealand or had been convicted of a terrorism offence or controlled by another entity that had been so convicted. There were also provisions that enable the High Court to approve either non-classified summaries of information prepared by the Attorney General or conduct *ex parte* proceedings without the affected person or the public being present if the court was satisfied that such procedures were desirable for protecting classified information.[166]

---

[163] New Zealand report to the 1267 Committee 2003 available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/350/95/IMG/N0335095.pdf?OpenElement

[164] Ibid

[165] *Terrorism Suppression Act, 2002* s.30

[166] Section 37 of the Terrorism Suppression Act, 2002 now repealed provided that the High Court must not renew a terrorist listing:

unless the Attorney-General satisfies the Court on the balance of probabilities that the entity who is the subject of the designation concerned –

- (a) is the subject of criminal proceedings in a national or international court or tribunal (within or outside New Zealand), for an offence relating –
  - (i) to carrying out, or to participating in the carrying out of, 1 or more terrorist acts; or
  - (ii) to facilitating the carrying out of 1 or more terrorist acts by, or with the participation of, another entity; or

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

In 2007, the *Terrorism Suppression Act* was amended to remove the requirement for judicial approval to relist an individual or group after three years. Under the 2007 amendments however the Prime Minister is allowed to extend the listing on the same basis and including with reference to classified information as is available for the original designation. The current Act also provides that nothing precludes judicial review of a listing[167] but this appears limited to procedural and not merits-based judicial review.

2. Court Cases

No court cases were discovered that challenged the New Zealand listing process. Possible explanations for this finding including the above noted restrictions on judicial review, as well as the concerns noted above with respect to Australia, about the limited effect of even a successful challenge to a listing in one jurisdiction, as well as possible concerns by individuals about being associated with a listed terrorist group or individual.

3. The Literature

- (iii) to acting on behalf of, or at the direction of, another entity that has done, or is doing, what is referred to in subparagraph (i) or subparagraph (ii); or

- (b) has been convicted in criminal proceedings in a national or international court or tribunal (whether within or outside New Zealand), being proceedings not subject to any appeal and that are finally determined, of an offence relating—
  - (i) to carrying out, or to participating in the carrying out of, 1 or more terrorist acts; or
  - (ii) to facilitating the carrying out of 1 or more terrorist acts by, or with the participation of, another entity; or
  - (iii) to acting on behalf of, or at the direction of, another entity that has done, or is doing, what is referred to in subparagraph (i) or subparagraph (ii); or
- (c) either—
  - (i) has knowingly carried out, or knowingly participated in the carrying out of, 1 or more terrorist acts; or
  - (ii) is knowingly facilitating the carrying out of 1 or more terrorist acts by, or with the participation of, another entity; or
  - (iii) is acting on behalf of, or at the direction of, another entity, knowing that the other entity has done, or is doing, what is referred to in subparagraph (i) or subparagraph (ii); or
- (d) is an entity (other than an individual) that is wholly owned, or effectively controlled, directly or indirectly, by an entity that has done, or is doing, what is referred to in paragraph (c)(i) or (ii) or (iii)

[167] *Terrorism Suppression Act, 2007 as amended s.*33

000136

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Reflecting its small size, the literature on terrorist listing in New Zealand was more sparse than that found in the other jurisdictions (other than the United Kingdom) examined in this paper. Fortunately, however, we were able to discover a monograph that deals extensively with listing and makes creative reform proposals.

Conte, Alex. *Counterterrorism and Human Rights in New Zealand* (New Zealand Law Foundation, 2007).

This comprehensive monograph examines anti-terrorism law in New Zealand and has several chapters devoted to listing. It examines how regulations enacted under the *United Nations Act* were used to list Al Qaeda and the Taliban before the enactment of the *Terrorism Suppression Act*, 2002. It concludes in chapter 11 that the regulations including the listing powers were lawful under the United Nations Act and required to comply with Resolution 1373.

It examines the power of the Prime Minister to make interim and final designation of terrorist entities under the Terrorism Suppression Act on the basis of information received from the UN Security Council and any other information including classified information. The designation originally lasted for three years with the High Court having to authorize extensions. The Attorney General would have to satisfy the court on a balance of probabilities that the entity is a terrorist or associated entity or is being prosecuted for or has been convicted of terrorism either in New Zealand or elsewhere.[168] The author notes that this raised the potential of New Zealand courts requiring the removal of an entity that is listed by the UN when New Zealand would be required to list such individuals and groups under its obligations under Chapter VII of the UN Charter. This reflects a theme also seen in the 1267 literature.

In the 2007 amendments to the Act, however, the Prime Minister was given the power to extend the listing of groups not listed by the UN and the listing of entities listed by the UN 1267 Committee was made automatic without Prime Ministerial intervention or judicial review when the domestic listing was extended beyond three years. The author praises the 2007 amendments that require that listings by the 1267 Committee be made domestically on the basis that it is "an appropriate response"[169] that fulfills New Zealand's international obligations.[170] At the same time, however, he notes wide spread concerns about the fairness of the delisting process used by the 1267 Committee and expresses the view that a person should be able to seek delisting at least

---

[168] Alex Conte *Counterterrorism and Human Rights in New Zealand* (New Zealand Law Foundation, 2007) at p.307

[169] Ibid at 315, see also at 420

[170] Ibid at 312-313

000137

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

from the domestic New Zealand listing in New Zealand courts.[171] He also does not provide a rationale for the 2007 repeal of the mandatory judicial review of renewals, but this may be related to concerns about the confidentiality of the intelligence that supports the listing and the difficulties of maintaining that confidentiality while conducting judicial review. He notes that the Prime Minister now need only have a belief on reasonable grounds to renew a listing whereas before 2007 the High Court had to be convinced on a "balance of probabilities" that grounds for renewal of the listing existed. He concludes, however, that the 2007 changes are "not of substantial concern" [172] because the extension of the listing could still be subject to judicial review. That said, the 2007 change requires a listed group to take the initiative to commence the judicial review and removes mandatory judicial review for renewals of listings. A separate chapter in the Conte monograph is devoted to the natural justice implications of the listing process with the author noting the absence of any prior notice to the listed entity, the lack of a right to be heard by the Prime Minister when listing or extending the listing and provisions which allow courts that review listing to consider national security information that is not disclosed to the entity or other person contesting the listing. Natural justice considerations are informed by both the ICCPR and the New Zealand Bill of Rights. He concludes that the process violates art 14 of the ICCPR and the New Zealand Bill of Rights by denying the person challenging the listing an opportunity to meet the case. He also notes that New Zealand has not attempted to derogate from this right.[173] He suggests that the Prime Minister is not capable of providing a fair hearing and that such reviews be conducted by the Inspector General of Intelligence.[174]

The author concludes that the provisions in s.38 of the Terrorism Suppression Act, 2007[175] for preserving national security information are not in accord with natural

---

[171] Ibid at 315

[172] Ibid at 309

[173] Ibid at 335

[174] Ibid at 337

175 These provisions provide: **Procedure in proceedings involving classified security information**

- (1) This section applies to any proceedings in a court arising out of, or relating to, the making of a designation under this Act.

(2) The court must determine the proceedings on the basis of information available to it (whether or not that information has been disclosed to or responded to by all parties to the proceedings).

(3) If information presented, or proposed to be presented, by the Crown includes classified security information,—

- (a) except where proceedings are before the Court of Appeal, the proceedings must be heard and determined by the Chief High Court Judge, or by 1 or more Judges nominated by the Chief High Court Judge, or both; and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

justice or the ICCPR. Although the protection of such information is an important objection, the potential of denying an entity of any of the reasons behind the listing is a disproportionate restriction on the right. He proposes that the Inspector General be given powers to review terrorist listings and also whether more information about the reasons for the listing can be disclosed to the entity.[176] In addition, the Inspector General could also provide a right for the petitioner to be heard when challenging the designation.[177] He also proposes that security cleared counsel be able to have access to confidential material used to support the listing on judicial reviews and appeals.[178] He suggests that any criminal prosecution that relies on a listing should be stayed to allow the accused to seek independent judicial review of the listing.[179] He concludes by both affirming the importance of the listing process as a critical part of counter-terrorism efforts, but one that needs reforms to be compliant with natural justice and article 14 of the ICCPR and the New Zealand Bill of Rights.

- (b) the court must, on a request for the purpose by the Attorney-General and if satisfied that it is desirable to do so for the protection of (either all or part of) the classified security information, receive or hear (the relevant part or all of) the classified security information in the absence of—
  - (i) the designated entity concerned; and
  - (ii) all barristers or solicitors (if any) representing that entity; and
  - (iii) members of the public.

(4) Without limiting subsection (3), if the designated entity concerned participates in proceedings,—

- (a) the court must approve a summary of the information of the kind referred to in section 32(2) that is presented by the Attorney-General except to the extent that a summary of any particular part of the information would itself involve disclosure that would be likely to prejudice the interests referred to in section 32(3); and
- (b) on being approved by the court a copy of the statement must be given to the entity concerned.

(5) Nothing in this section limits section 27 of the Crown Proceedings Act 1950 or any rule of law that authorises or requires the withholding of a document or the refusal to answer a question on the ground that the disclosure of the document or the answering of the question would be injurious to the public interest.

(6) Subsections (2) to (5) apply despite any enactment or rule of law to the contrary.

Section 38: substituted, on 20 November 2007, by section 21 of the Terrorism Suppression Amendment

[176] Ibid at 349

[177] Ibid at 351

[178] Ibid at 353

[179] Ibid at 327

000139

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

C. Discussion/Conclusions

The New Zealand experience is noteworthy in large part because of the central role that the Prime Minister plays in the listing process and the now repealed provisions that provided for mandatory judicial review of renewals of terrorist listings. Professor Conte's detailed examination and critique of the failure of the listing process to satisfy natural justice requirements and his proposed reforms are also of interest.

The New Zealand process in common with other listing processes examined in this paper recognized that the basis for listing could be secret intelligence that could cause harms to national security if disclosed publicly or to a person challenging the listing. For this reason, the 2002 Terrorism Suppression Act made clear that the Prime Minister could receive information from the Security Council including the 1267 Committee in confidence and base his or her decision on such confidential information. Similarly, the New Zealand act provided means to protect confidential information in judicial reviews of a terrorist listing including in its innovative provision that required judicial review and approval of listings that expired after three years.

The New Zealand legislation also has an interim 30 day listing process that allows the Prime Minister to list a terrorist group on the basis of "good grounds to suspect" a lower standard than the "reasonable grounds to believe" that is required to list a terrorist group for a renewable three year period. The lower standard for interim listing is partially compensated by the fact that the Leader of the Opposition can request a briefing on an interim listing but not a final listing.[180]

Professor Conte has concluded that the provisions for the protection of confidential information in the present Act violate principles of natural justice and fair trial protected by the common law, the ICCPR and the New Zealand Bill of Rights. He proposes a new regime that will allow the Inspector General with expertise in intelligence to conduct reviews of terrorist listings and provide affected individuals with the right to be heard. Implicit in this proposal seems to be the idea that the Inspector General would have the power to revoke a listing even if the Prime Minister and/or the 1267 Committee maintained that the individual or group should continue to be listed as a terrorist entity. This raises a recurring issue found in the literature and possible reforms of the terrorist listing. It is possible to imagine and perhaps create a body with expertise in intelligence and other relevant matters to review listing decisions. This body could be assisted by security cleared counsel and other relevant experts. Nevertheless whether it is in New Zealand or the 1267 process, the fundamental question of who makes the listing decision remains a problem and it is not clear if the 1267 Committee or the domestic executive would wish to cede their listing

---

[180] *Terrorism Suppression Act, 2002* ss.20(5), 22 (4)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

powers to an advisory committee or other body. The newly created Ombudsperson under Security Council Resolution 1904 can make representations to the 1267 Committee with respect to delisting, but that committee composed of governments that have already agreed to list the petitioner, maintains the ultimate decision-making power with respect to the listing. A similar advisory role for the New Zealand Inspector General might not respond to the concerns about the lack of natural justice because the person challenging the listing would still not have a hearing before the actual decision-maker, in this case the Prime Minister.

Another common dilemma that is revealed through the New Zealand experience and in particular Professor Conte's reform proposals is that effective domestic delisting remedies run the risk of placing the domestic nation at least temporarily in breach of its international obligations under the 1267 process. Professor Conte's proposals do not provide a solution to this difficult dilemma because he both praises the automatic listing in New Zealand of the 1267 list as one that it necessary to fulfill New Zealand's international obligations but also proposes a more effective domestic review process that if used could conceivably provide a listed person with a domestic remedy of delisting that would put New Zealand in breach of its international obligation. This underlines the need for the 1267 Committee to respond quickly to successful domestic reviews or to make its own listing process temporary or contingent on domestic processes. The fact that extensive reform relating to secret information and the role of the Prime Minister is proposed by Professor Conte, however, underlines that it may be dangerous to assume that nation states have the capacity to review terrorist listings and provide an indirect check on the 1267 process. Our inability to identify court cases challenging listing in either Australia or New Zealand is also consistent with this concern.

The original 2002 New Zealand Terrorism Suppression legislation is also of interest to reforms of the 1267 and other listing process because it provided an innovative and creative combination of time limited executive listing and mandatory judicial review. It will be recalled that some proposals for reform of the 1267 process contemplates that listing could be temporary and provisional and subject to domestic procedures that would allow the affected individual to challenge the basis of the listing.[181] This was essentially the approach taken in the 2002 New Zealand legislation but it has been replaced in 2007 with a process that simply allows the Prime Minister to renew a listing once it has expired. The New Zealand experience suggests that similar

---

[181] Iain Cameron "UN Targeted Sanctions, Legal Safeguards and the European Convention on Human Rights" (2003) 72 Nordic Journal of International Law 159 ;Peter Gutherie "Security Council Sanctions and the Protection of Individual Rights" (2004) 60 NYY Annual Survey of American Law 491; Johannes Reich "Due Process and Sanctions Targeted Against Individuals Pursuant to UN Resolution 1267 (1999)" (2008) 33 Yale J of Int Law 505.

000141

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

reforms in the 1267 process might encounter obstacles by decision-makers who wish to retain the power to make listing decisions.

The repealed New Zealand provisions for judicial review of listing contained provisions for the protection of confidential and sensitive intelligence. These provisions also remain with respect to any remaining natural justice and administrative law review of listing. Nevertheless, these provisions have themselves been criticized as infringing the ICCPR and the New Zealand Bill of Rights.[182] This underlines the need in the literature to pay more attention to exactly how the competing interests in disclosure and secrecy will be reconciled in any mechanism that allows listing decisions to be challenged. In the end, the New Zealand experience cast doubt on some of the most creative proposals for reform of the 1267 process which are based on making listing provisional and subject to judicial review and challenge.

PART SEVEN: OVERALL CONCLUSION

The New Zealand experience brings us full circle to the same themes discussed in relation to the 1267 process as well as those of the EU and a variety of domestic jurisdictions.

The first theme is the difficulties of reconciling the reality, as reflected in the New Zealand legislation and the practice of the 1267 Committee, that listing decisions will be made on the basis of intelligence that governments will desire to keep secret with the fact that those who are listed will often be unable to have a meaningful opportunity to challenge the listing without access to the intelligence. More specifically, governments will have legitimate interests in keeping the sources and methods used to obtain intelligence secret but those challenging listing decisions will also have legitimate interests and arguably rights to demand access to some of that information in order to challenge the reliability and sufficiency of the intelligence that is said to support a terrorist listing. There are no simple solutions to the dilemmas of secret evidence that are seen not only in the listing process but other anti-terrorism activities.

The second common theme is that while it is possible to imagine and propose creative reforms that will improve the various listing processes by allowing review of listing decisions by outside experts both before and after listing, such reforms may flounder if those who presently have the power to make listing decisions, the governments on the 1267 Committee and the domestic executive, are unwilling to give up decision-making power over the listing process.

---

[182] Alex Conte *Counterterrorism and Human Rights in New Zealand* (New Zealand Law Foundation, 2007) at 335.

000142

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

As has been seen, the listing of terrorists is a procedure that is woven deeply into counter-terrorism regimes at the international, supranational and national levels. The UN Security Council and many governments claim that terrorist listing is an essential instrument to prevent terrorism, but the extensive literature on listing does not seriously examine these claims in light of the evolving nature of international terrorism. It is, however, difficult to deny that being listed as a terrorist has profound effects on affected individuals and organizations who find themselves subject to asset freezes and travel bans and on public lists that place those who associate with them or provide them support in risk of criminal sanctions. The consensus that emerges from the growing number of court cases challenging listing decisions and the mostly critical literature on the 1267 and other listing processes is that listing is difficult and that the 1267 process is perhaps impossible to reconcile with values of transparency and effective challenge and remedies for errors made in the listing process. Especially in the wake of the EU *Kadi* case, there is doubt in the literature as to whether the 1267 process will survive.

000143

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

A Summary of De-Radicalization and Counter-Terrorism Programs

Melissa Northcott
Research and Statistics Division
Department of Justice Canada
November 2010

This report provides a snapshot of de-radicalization and counter-terrorism programs at the time that this report was created. Major developments in the United Kingdom have already occurred since the completion of this report.

This report is a work product, and the findings presented herein are not to be construed as an official Department of Justice Canada position, unless they are designated as such by other authorized documents and the report is posted on the official Department of Justice Canada Web site.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Contents

1. Introduction 4
2. Methodology 4
3. De-Radicalization Programs Focusing on Neo-Jihadist Terrorism 5
3.1 Canada 5
3.1.1 The Specialized De-radicalization Intervention Program (Mohammed Shaikh-Masjid el Noor Mosque) 5
3.2 Germany 5
3.2.1 Exit Program for Militant Islamists 5
3.3 The Netherlands 5
3.3.1 Action Plan Polarization and Radicalization 2007-2011 5
3.3.2 Wij Amsterdammers Action Plan 6
3.3.3 Actieplan Slotervaart Het tegengaan van radicalisering 7
3.4 United Kingdom 8
3.4.1 Birmingham 8
3.4.2 Preventing Violent Extremism Together Program 8
3.4.3 SEED/PROSEED 13
3.5 Prison-Based De-radicalization Programs 14
3.5.1 Prison-Based De-radicalization Programs Focused on Neo-Jihadist Terrorism 14
3.5.2 Other Prison-Based De-radicalization Program 21
4. De-Radicalization Programs Focusing on Right-Wing Terrorism 22
4.1 Denmark 22
4.1.1 De-radicalization-Targeted Intervention 22
4.2 Germany 23
4.2.1 Aussteigerprogramm fur Rechtsextremisten vom Bundesverfassungsshutz 23
4.2.2 Exit Deutschland 23
4.2.3 Help for Right-Wing Extremist Drop-Outs 24
4.2.4 Taking Responsibility-Breaking Away from Hate and Violence 24
4.2.5 The Hessian Programme for Disengagement from Radicalization 25
4.2.6 The North-Rhine Westphalian Programme for Disengagement from Radicalization 25
4.3 Norway 25
4.3.1 Exit Programme 25
4.4 Sweden 27
4.4.1 Exit Stockholm 27
4.4.2 Exit Motala 28
5. Counter-Radicalization Programs 30
5.1 Australia 30
5.1.1 National Action Plan for Commonwealth 30
5.2 Canada 31
5.2.1 Cross-Cultural Roundtable on Security 31
5.2.2 RCMP's National Security Community Outreach Program 31
5.2.3 The Canadian Association of Chiefs of Police (CACP) Counter-Radicalization Study Group 33
5.2.4 Counter-Terrorism Information Officers (CTIO) 34
5.2.5 RCMP Research Initiatives 35

000145

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5.3 Indonesia 35
5.3.1 The Lib for All Foundation 35
5.4 United Kingdom 36
5.4.1 The CHANNEL Project. 36
5.4.2 The DELPHINUS Program 36
5.4.3 Gold Groups 36
5.4.4 Islam and Citizenship Education 37
5.4.5 Operation NICOLE 37
5.5 United States 37
5.5.1 The White House Office of Faith-based and Neighbourhood Partnerships 37
5.5.2 Federal Bureau of Investigation 38
5.5.3 United States Department of Justice 39
5.5.4 The Department of Homeland Security 39
References 42

000146

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

1. Introduction

This compendium explores de-radicalization and counter-terrorism programs that are currently established, or that have been established, in various countries around the world. In this compendium, de-radicalization[1] programs refer to programs that are focused on changing the mindset and behaviours of radicalized individuals to one that is less extreme and more tolerant. Counter-terrorism programs refer to programs that are focused on preventing and combating radicalization and extremism. The compendium begins with an exploration of de-radicalization programs that focus on Neo-Jihadist terrorism in several countries, including the United Kingdom, Canada and the Netherlands. Prison-based de-radicalization programs focusing on Neo-Jihadist terrorism are then discussed, along with a brief description of these programs in different countries. An examination of de-radicalization programs focusing on right-wing terrorism is then conducted, followed by a discussion of various counter-radicalization programs that have been established in various countries. In each section, a discussion of evaluations that have been conducted on the specific programs is provided, where this information is available. Within each section of this compendium, the programs are presented and discussed by country.

2. Methodology

This compendium was created by doing a literature search of relevant resources relating to de-radicalization and counter-terrorism programs in several countries. Initially, the project began with a focus on de-radicalization programs in democratic countries specifically. Throughout the search process, however, other non-democratic countries were added to the compendium, as were several counter-radicalization programs, as this information was useful to the review. An internet search was conducted using the Google search engine. Keywords included in this search included: 'counter-radicalization'; 'de-radicalization'; 'outreach to minority groups'; 'collaboration with religious groups/minority groups/youth programs'; 'evaluation of de-radicalization programs'; and 'evaluation of counter-radicalization programs'. Relevant websites of government departments in various countries concerned with justice issues and national security were also searched (e.g., RCMP; United States Department of Justice; The Home Office). In addition, websites of various think tanks and Non-Governmental Organizations were also searched (e.g., The International Centre for the Study of Radicalisation and Political Violence; The Change Institute). A search of the Scholars Portal and EBSCOhost search engines was also conducted using the names of the projects that were found in the initial Google search. Research for this compendium was conducted between February 2010 and January 2011.

[1] Demant et al. (2008) define de-radicalization as "the process of becoming less radical. This process of 'becoming less radical' applies both to behaviour and beliefs. With regard to behaviour, this primarily involves the cessation of violent actions. With regard to beliefs, this involves an increase in confidence in the system, a desire to once more be a part of society, and the rejection of non-democratic means" (13).

000147

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

3. De-Radicalization Programs Focusing on Neo-Jihadist Terrorism

s.19(1)

3.1 Canada

3.1.1 The Specialized De-radicalization Intervention Program (-Masjid el Noor Mosque)

The 'Specialized De-radicalization Intervention Program', established by the Masjid el Noor Mosque in Toronto in February 2009, is Canada's first de-radicalization program. The program was established by (Bell 2009). The program involves a 12-step program, which includes teachings on "Allah, the Koran and Mohammed; the connections between Islam, Christianity and other faiths; Canadian society; and countering extremism through education, public speaking and writing" (Bell 2009, 2). The goals of the program are:

- to teach peace;
- to teach the positive aspects of Canadian society; and
- to teach the concept of an open society (Bell 2009).

Because it is newly established, the program has not been formally evaluated (Pressman 2009).

3.2 Germany

3.2.1 Exit Program for Militant Islamists

Germany's Federal Office for the Protection of the Constitution launched an exit program for neo-jihadists at the end of June 2010 (Spiegel Online 2010). The program includes a telephone hotline that individuals wishing to leave the neo-jihadist movement can call. The individuals who call the helpline are offered services in a variety of languages, including Turkish, Arabic and German (Spiegel Online 2010). Because this program has only recently been established, additional information could not be located.

3.3 The Netherlands

3.3.1 Action Plan Polarization and Radicalization 2007-2011

The Netherlands' de-radicalization program is entitled, 'Action Plan Polarization and Radicalization 2007-2011'. The program is aimed at both Neo-Jihadist extremism and right-wing extremism. The program has a budget of €28 million and covers the programs of eight ministries: the Ministry of Interior and Kingdom Relations; Justice; Housing, Communities and Integration; Social Affairs and Employment; Health, Welfare and Sport; Youth and the Family; Education,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Culture and Science; and Foreign Affairs (The Change Institute 2008). The program is led by the Ministry of Internal and Kingdom Affairs and has three distinct goals:

- The prevention of isolation, polarisation and radicalization by including individuals who are at risk of becoming radicalized through education, training and work (prevention).
- The early detection of radicalization by administrators and professionals (pro-action).
- The exclusion of those who have violated the boundaries of radicalization and limiting their influence on others (repression) (The Change Institute 2008; Ministry of the Interior and Kingdom Relations 2007).

The program takes place at three levels. The first is at the level of local government and municipalities. The activities performed at this level are aimed at prevention and intervention (Ministry of the Interior and Kingdom Relations 2007). The local approach is aimed at neighbourhoods that have experienced polarization and radicalization and includes both 'soft' and 'hard' approaches. The 'soft' approach includes meetings and debates, discussion about ideologies and the supervision of individuals who have dropped out of high school (Ministry of the Interior and Kingdom Relations 2007). The 'hard' approach consists of compulsory school attendance and increased street supervision. Professionals, such as police, youth workers, and teachers, work together at this level (Ministry of the Interior and Kingdom Relations 2007).

The second is the national level, which is meant to support the local approach. Activities at this level include implementing a "housing policy for young people, promoting long-term participation of youth in the labour market, and promoting economic, social and political participation of young people" (Ministry of the Interior and Kingdom Relations 2007, 17).

The third is the international level, which is focused on reducing polarization and radicalization both inside and outside of the European Union, as well as working with the Ministry of Foreign Affairs on radicalization policies (Ministry of the Interior and Kingdom Relations 2007).

According to the Ministry of the Interior and Kingdom Relations (2007), the program is to be measured periodically, with baseline measurements taken in October 2000. Although the Minister of Foreign Affairs is to prepare annual progress reports (Ministry of the Interior and Kingdom Relations 2007), these reports could not be located.

3.3.2 Wij Amsterdammers Action Plan

Amsterdam has established its own de-radicalization plan, the 'Wij Amsterdammers Action Plan', with the goal of stopping Neo-Jihadist radicalization (European Commission 2008). The program involves a multi-level approach. The first involves a hard approach against 'doers', those who are suspected of being extremist and willing to use violence (European Commission 2008). The mayor works closely with the police force, judiciary, AIVD (Dutch Intelligence Service) and NCTb (National Coordinator for Counterterrorism). In order to facilitate this approach, the powers of the police and security forces have been extended in an effort to disrupt activities. The second involves a softer approach against the 'thinkers', those who do not use violence but follow radical ideologies. These individuals receive person-specific interventions aimed at halting further radicalization (European Commission 2008). There is alsc a preventive

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

approach, which is focused on increasing resistance against radicalization (European Commission 2008). The soft and preventive approaches mainly focus on the risks of radicalization that cannot be dealt with by the law, and is strengthened by working closely with key partners, including important individuals from the Muslim community (European Commission 2008).

Several local authorities are involved in this Action Plan and have received a total of €1.33 million for organizing activities aimed at addressing radicalization (European Commission 2008). The activities are divided into 16 topics that are sub-divided into three overarching goals:

- De-radicalization, and includes activities such as developing intervention, training professionals, and increasing knowledge and knowledge exchange.
- "Increase of defensibility", and includes increasing the defensibility of Muslims and women.
- "Eliminating breeding grounds", which includes "eliminating discrimination and intolerance, increasing insight in diversity of Islam and enhancing intercultural relations" (European Commission 2008, 30).

Although a formal evaluation could not be located, critics have stated that extending the powers of the police may lead to police profiling, which in turn may create more problems (European Commission 2008). The European Commission (2008) has stated that although the Amsterdam approach addresses both the external and social levels, the possible causes of radicalization that occur at the individual level are not addressed, including psychological characteristics and personal experiences.

3.3.3 Actieplan Slotervaart Het tegengaan van radicalisering

The 'Slotervaart Action Plan' involves a joint effort between city and sub-municipal authorities and various civil society groups, including mosques. The goals of the action plan are to "improve awareness of issues of radicalization and their consequences amongst the local youth population" and "strengthen the resilience of local youth against all religious forms of radicalization" (The Change Institute 2008, 83). The main measures of the program include:

- raising consciousness amongst youth;
- developing the ability of youth to be resilient against radicalization;
- supporting parents;
- supporting mosques and imams;
- building a radicalization response network;
- increasing collaboration between public schools and youth; and
- promoting interaction between different groups (The Change Institute 2008).

An important element of the action plan is "Academia Islamica", which is a youth intervention program that involves empowering key figures in the community; organising debates; and "personal coaching and counselling of radicalised youth" (The Change Institute 2008, 84).

000150

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

According to the Change Institute (2008), a formal evaluation of the program is currently being conducted; however, data are not yet available.

3.4 United Kingdom

A major shift has occurred in the United Kingdom's approach to de-radicalization programs since this report was completed. As such, it is important to note that the information below reflects only a snapshot in time.

3.4.1 Birmingham

Birmingham's de-radicalization program was established in 2007. The program is focused both on prevention and defensibility against radical ideas, as well as de-radicalization (see Demant et al. 2008 for a full description of this program). The program consists of several projects, including Study Circles, Success Clubs, the Journey of the Souls program and the Women's Development Project:

- The Study Circles provides information on Islam to youth in non-religious settings, including youth centers.
- Success Clubs are community service programs in which both Muslim and non-Muslim youth work on a community-oriented project based on a topic important to the youth.
- The Journey of the Souls Program is one in which youth from radical groups are invited to join the program and are taken on trips, with the goal that the youth will become more tolerant once out of their current surroundings.
- The Women's Development Project is aimed at training Muslim women to recognize the signs of radicalization and helping family members to defend themselves against radical influences.

Because the projects are recent, there has been no formal evaluation. The program has received some criticism as the obligation to report individuals who are radical places pressure on family members, as well as members of the project, and can cause tension with the police. Furthermore, the overall program has not yet designed a project focusing on the (de)radicalization of females. Despite these drawbacks, the team consists of Muslims representing all orientations and some of the members were once radical themselves, which enhances the credibility of the program (Demant et al. 2008).

3.4.2 Preventing Violent Extremism Together Program

Under the UK government's counter-terrorism strategy, "CONTEST' there are four pillars: *Prevent, Pursue, Protect* and *Prepare*. The program focusing on preventing extremism is the Preventing Violent Extremism Together (Prevent) program (The Change Institute 2008). The Government revised the "CONTEST" strategy in March 2009, rendering the *Prevent* pillar as the most important element in the counter-terrorism initiative (House of Commons Communities and Local Government Committee 2010). The revised strategy is known as "CONTEST II" and its

000151

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

goal is "to reduce the risk to the UK and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence" (HM Government, as cited in House of Commons Communities and Local Government Committee 2010, 6).

The Prevent strategy has seven key objectives aimed at addressing factors associated with extremism:

- challenge the ideology behind violent extremism and support mainstream voices;
- to disrupt those who promote violent extremism and support people living in the communities where they may operate;
- to support individuals who are vulnerable to recruitment, or have already been recruited by violent extremists;
- to increase the resilience of communities to violent extremism;
- to address grievances which ideologues are exploiting;
- to develop supporting intelligence, analysis and information; and
- to improve strategic communications (House of Commons Communities and Local Government Committee 2010, 6).

The program works with Muslim communities to prevent radicalization in four areas:

- promoting shared values;
- supporting local solutions;
- building civic capacity and leadership; and
- strengthening the role of faith institutions and leaders (The Change Institute 2008, 108).

The Prevent Program involves individuals at many levels, including the local police. There is a strong focus on neighbourhood policing, which involves engagement with the community and the gathering of "community intelligence", which is information about individuals or places of concern (Bettison 2009, 133). The program is supported by the Preventing Violent Extremism Community Leadership Fund and the Preventing Violent Extremism Pathfinder Fund (Department for Communities and Local Government 2007a).

Preventing Violent Extremism Community Leadership Fund. The Preventing Violent Extremism Community Leadership Fund was launched in 2007 and is aimed at national level projects on preventing violent extremism. The initial fund was £650,000 and an additional £25 million was later added. The program's goal is to help Muslim communities find the means to fight extremism and feel welcome in British society (Department for Communities and Local Government 2007a). The program focuses on three key areas:

- Increasing the leadership capacity of Muslim leaders through support;
- Increasing organizational capacity, which is aimed at "building the capacity of organizations in the Muslim community to actively resist the influence of violent extremists" (Department for Communities and Local Government 2007a, 3); and

000152

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Developing the capacity of Muslim women so they are able to help young Muslims who are at risk of radicalization (The Change Institute 2008; Department for Communities and Local Government 2007a).

Preventing Violent Extremism Pathfinder Fund. The Preventing Violent Extremism Pathfinder Fund was established in 2006. The fund provides funding to support local authorities to fight violent extremism. The aim of the fund is to increase the resilience of Muslim communities in fighting violent extremism (Department for Communities and Local Government 2007b). The budget for the project is £75 million, distributed over a three-year period. An additional £12.5 million was announced in June 2008 (The Change Institute 2008).

There have been many different projects funded through the Pathfinder Fund. For example, "The Reading Forum against Extremism" consisted of 13 discussion events held from February to April 2007, where discussions were held on causes of and solutions to extremism. This project received £10,000 in funding (The Change Institute 2008). The "Oxford Muslim Pupils' Empowerment Programme" is another example of a project funded through the Pathfinder Fund. This project involved lunchtime forums in which Muslim youth could openly talk about issues of concern (The Change Institute 2008).

Evaluation of the Prevent Program. The Prevent Program, and the Pathfinder Fund in particular, was the focus of a learning and development exercise by a UK government audit commission. The Audit Commission visited 15 sites to evaluate how the program is working. The Commission found that four themes emerged, including a need for a more clearly-defined strategic approach; a need for greater information sharing; a need for visible and effective leadership; and a need for more assessments of the project (Audit Commission 2008, 4-6).

Kundnani (2009), for the Institute of Race Relations, also conducted an assessment of the Prevent program. The assessment involved 32 interviews with individuals who work for the Prevent programs, individuals belonging to Prevent boards, as well as volunteer and community workers. The assessment also involved a roundtable discussion. The assessment conducted by the Institute of Race Relations revealed many criticisms, including:

- Local authorities have been pressured to accept Prevent funding in direct proportion to the number of Muslims in their area [which] construct[s] the Muslim population as a 'suspect community';
- Prevent decision-making lacks transparency and accountability, [as] decisions are taken behind closed doors rather than in consultation with the voluntary and community sector;
- Prevent-funded voluntary sector organisations and workers in local authorities are becoming increasingly wary of the expectations on them to act as providers of information to the police; and
- The current emphasis of Prevent on depoliticising young people and restricting radical dissent is [...] counter-productive because it strengthens the hands of those who say democracy is pointless (Kundnani 2009, 6-7).

Several recommendations were provided by Kundnani (2009) as a result of the assessment's findings:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Central government funding should be available to any local area which, through a genuine process of local decision-making, independently identifies a need to win individuals away from support for illegitimate political violence;
- The minutes of all decision-making meetings [...] should be published along with exact details of what has been funded;
- Public services (such as teachers and youth workers) should not be used as 'instruments of surveillance'; and
- Young people should be provided with the opportunities to engage in open discussions about difficult political issues without feeling as though their opinions need to be met with official approval (Kundnani 2007, 7).

Other criticisms of the program have been noted by other organizations and individuals, many centering around the program's exclusive focus on Muslim communities. According to Thomas (2009, 2010), the program's focus on Muslim communities is in conflict with the program's goal of community cohesion. In addition, the exclusive focus on Muslim communities draws attention away from 'violent extremism' that is growing among other groups, which is seen in the growing support for groups such as the British National Party (Thomas 2009). Moreover, the focus on Muslim communities is seen as biased and as a result, many choose not to apply for funding from the program (The Change Institute 2008).

Other criticisms of the program include:

- Some of the members of the Muslim community believe that the program is part of a political agenda aimed at changing Muslim communities;
- Many Muslim communities have found the criteria too rigid and some think that funding decisions are biased in favour of Muslim groups that are well-known in the community;
- Many believe that receiving funding from Prevent might damage their credibility, as it is tied with local government, and as such there has been difficulty finding groups who are willing to apply for funding;
- Government-funded programs focused on moderation may lead individuals to extremism due to their ties with government;
- Prevent's focus on ideology as the central reason for extremism is misguided and funding would be better spent on targeting disadvantage;
- Prevent has increased surveillance of Muslim communities; and
- The organisation and implementation of the policies have been problematic in a number of ways, including disagreements between different areas of local government regarding the central focus of Prevent and the use of misleading titles (Stevens, 2009; The Change Institute 2008; Thomas 2009, 2010).

Evaluation of the Prevent Program by the UK House of Commons' Communities and Local Government Committee

Similar concerns were voiced in the UK House of Commons' Communities and Local Government Committee's inquiry into the Prevent program. The Committee found that the program, as it is currently organized, is "contentious" and the individuals toward whom the

000154

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

program is aimed will likely never fully be accepting of it (House of Commons Communities and Local Government Committee 2010).

The Committee questioned the lead role taken by the Department of Communities and Local Government in the program. The Department of Communities and Local Government is mandated with promoting cohesiveness, however many of the witnesses believed that Prevent undermines cohesiveness in the communities (House of Commons Communities and Local Government Committee 2010). As such, the Committee suggested the Department for Communities and Local Government focus more on building stronger communities.

The inquiry also revealed allegations of spying and surveillance in Muslim communities. The Committee suggested that the Government should conduct an independent investigation into these allegations and provide clear direction on the type of information needed for the program and how this information is not 'information gathering' of the type undertaken by the police or security services" (House of Commons Communities and Local Government Committee 2010, 63).

The overlap between the Prevent and Pursue pillars was also discussed as an issue of concern. Many of the witnesses who testified in front of the Committee felt that this overlap has given the impression that community work with Muslim groups is associated with counter-terrorism efforts (House of Commons Communities and Local Government Committee 2010). Much of this concern has to do with the "under-developed information sharing practices between the police and local authorities [that] have exacerbated perceptions of Prevent being police-controlled" (House of Commons Communities and Local Government Committee 2010, 53). The Committee also found that the program's focus on al-Qaeda inspired terrorism has led to stigmatization and a sense of alienation among Muslim communities, and has led to resentment in non-Muslim communities that funding is not being applied in other areas of need (House of Commons Communities and Local Government Committee 2010). The Committee also found that there is a lack of risk-based assessment and an understanding of actual risk, which has led to the program's unfocused approach. This unfocused approach has in turn led to a lack of agreement among partners regarding the goals of Prevent, including between central government departments. Similarly, the Committee stated that because the aims and objectives of the program are unclear, monitoring and evaluation of the program has suffered (House of Commons Communities and Local Government Committee 2010).

Recommendations Made by the UK House of Commons' Communities and Local Government Committee

In addition to some of the recommendations discussed above, the Committee made additional recommendations focusing on how the Prevent program could be strengthened. The report states that "the development of a proportionate risk-based approach to delivering Prevent, along with greater clarity as to what the programme aims to achieve, are needed before any useful performance measures can be agreed at national and local level" (House of Commons Communities and Local Government Committee 2010, 52). Other recommendations made by the Committee include:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- allocating some of Prevent's funding towards "encouraging participation in democratic means of debate" (29);
- ensuring that the Government continues to prioritize investment into alleviating socio-economic deprivation;
- that universities and prisons be included in risk assessments and that work with these institutions be better co-ordinated with the Prevent program;
- that the Government provide more opportunities for empowerment and civic engagement to strengthen the engagement of all excluded groups;
- that the Government seek the advice of independent academics in determining how programs should be developed, rather than relying solely on local authorities to determine which organizations are the best fit in challenging the al-Qaeda narrative.
- sharing between local partners be improved and that more training and support be provided to front-line workers, including police and teachers (House of Commons Communities and Local Government Committee 2010).

The Committee also felt there may be too much emphasis on the theological basis of extremism and more attention may need to be placed on other factors, such as politics, policy and socio-economics, which may play an even greater role in the process of radicalization (House of Commons Communities and Local Government Committee 2010). The Committee suggested that the Government should take into account current research on the risk factors for radicalization and update the government's anti-terrorism strategy (CONTEST) to reflect the fact that there are other factors, beyond theological causes, that are associated with radicalization. In addition, the Committee stated that the Muslim community should be involved in developing a counter-narrative to extremist views (House of Commons Communities and Local Government Committee 2010).

3.4.3 SEED/PROSEED

The 'SEED' (Support for Employability, Enhancement and Development) project was established in Lambeth in 2004 (Simpson 2007). The project was implemented by the Stockwell Green Community Services (SGCS), which is a Muslim-led volunteer organization. The 'SEED' project focused on the employability of Muslim youth through the use of unaccredited training and personal development sessions and ran from 2004 to 2005 (Marsden 2008; Simpson 2007). The 'SEED' project was replaced by 'PROSEED' in 2006, which was in place for three years (Providing Real Employability Enhancement and Development) (Marsden 2008). 'PROSEED' offered accredited training, as well as work experience. The goals of these programs were to "divert those at risk of social and economic marginalisation, crime and radicalization through the provision of educational, training and personal development" (Marsden 2008, 7). The project brought together members of the Metropolitan Police, Lambeth Borough Council and the community, including the local mosque (Marsden 2008).

Family and community members who were concerned about certain youth introduced the youth to mosque elders or other project leaders, who in turn introduced the youth to the program. Youth were also recruited through personal development seminars, after which they would participate in mentoring with the aim of changing their extremist beliefs (Marsden 2008).

000156

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Evaluation of SEED/PROSEED. This project was evaluated in 2007. Stockwell Green Community Services' records were analyzed in order to determine if the projects were meeting their objectives. This analysis revealed that the project was meeting its initial objectives on the majority of the measures, including the goals of referral to employment advice and employment gains, as well as providing individuals with personal development support (Marsden 2008). The evaluation also found that the projects were able to "reach, attract and engage with those most at risk of progressing towards extremist views and economic inactivity" (Marsden 2008, 9).

The evaluation also involved semi-structured interviews with nine individuals who were familiar with the project, including police and other local authorities. These interviews found that the project met their goals of meeting needs of the youth, helping youth establish a sense of belonging, building capacity among individuals at many levels, and providing empowerment to participants (Marsden 2008).

3.5 Prison-Based De-radicalization Programs

3.5.1 Prison-Based De-radicalization Programs Focused on Neo-Jihadist Terrorism

According to a recent report published by the International Centre for the Study of Radicalisation and Political Violence (ICSR), there are approximately 12 countries around the world that have established prison-based de-radicalization programs (Neumann 2010). These prison-based de-radicalization and disengagement programs are focused on "helping individual terrorists abandon terrorism and eas[e] their re-integration into mainstream society" (Neumann 2010, 3). Below is a brief description of some of these programs, followed by a general evaluation of prison-based programs provided in Neumann's (2010) report.

Afghanistan

Afghanistan's prison-based de-radicalization program has recently been established. The program assumes that Taliban foot soldiers should be separated from religious ideologues and provided with skills, such as reading and writing, which will be beneficial when they are released from prison (Neumann 2010). This program does not provide material incentives, but does provide early release, practical skills and education to the participants (Neumann 2010). This program has yet to identify a principal interlocutor, which, according to Neumann (2010), may be a shortcoming due to the importance of an interlocutor in establishing credibility among prisoners. Additionally, the program has made attempts at involving "village elders and organis[ing] symbolic welcome ceremonies, [however], the programme struggles to overcome hostility and the difficulties between tribes which can result from travelling around the country" (Neumann 2010, 54). The country's current environment has also impeded the program developers from offering an after-care program. Information regarding a formal evaluation of this program could not be located.

000157

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Egypt

The de-radicalization program in Egypt involved dialogue between Islamic scholars and prisoners from the Gamaa Islamia[2] (GI) in an attempt to have the prisoners denounce violence (Goerzig and Al-Hashimi 2007). Leaders of the GI were permitted to go to other prisons to talk to their followers about how they had changed their ideas. The prisoners were not released from prison, nor did they receive recognition for their participation in the program. The detainees were also not allowed to converse with individuals outside of prison (Demant et al. 2008). Despite these constraints, members of the GI eventually chose to reject violence. The leaders of the GI began several initiatives to encourage others to denounce violence and have made various statements about their new standpoints, including through published books on the topic (Demant et al. 2008; Goerzig and Al-Hashimi 2007; Gunaratna and Bin Ali 2009).

Indonesia

Indonesia's police-based deradicalization program is aimed at members of the Jamaah Islamiyah (JI) (Demant et al. 2008). The police choose people who are in prison and are members of the JI. They must be high-ranking and willing to cooperate with the police. In exchange for their cooperation, the prisoners' personal needs are met and upon release, there is an attempt to reduce the effect of individuals in the prisoners' social circles that still maintain extremist views (Demant et al. 2008; International Crisis Group 2007). The prisoners engage in informal discussions with scholars regarding jihad and are then sent to discuss the drawbacks of jihad with other prisoners. The program involves an after-care component, including livelihood programs, which involves the participation of the former prisoner and their spouse in "co-operative enterprises" (Neumann 2010, 55). Twenty members of the JI, as well as individuals from other organizations, have participated in the program (Demant et al. 2008).

This program has not been formally evaluated, but it has been reviewed. The International Crisis Group (2007) states that because the police treat the prisoners with kindness, the prisoners may no longer assume that the police are un-Islamic. In addition, the ICSR report states that the program's use of former terrorists enhances their credibility among prisoners (Neumann 2010). The program, however, has a number of flaws. There are too few staff and they are undertrained and underpaid (International Crisis Group 2007). Furthermore, attention is not paid to the background and situation of the prisoners. There is corruption and prison administrators are not trained sufficiently in counter-terrorism techniques (Demant et al. 2008; International Crisis Group 2007). Also, many prisoners are held in police cells for a long period of time before they are sent to prison, because once in prison, they are at greater risk of becoming re-involved in extremism (Demant et al. 2008; International Crisis Group 2007). Moreover, Horgan and Braddock (2010) state that there is a lack of transparency regarding recidivism statistics. While officials claim that very few released prisoners have recidivated, Horgan and Braddock (2010)(citing Abuza 2009), state that "there is actually no evidence to suggest that those who have been released due to sentence remissions or amnesties were in reality exposed to any kind of de-radicalization efforts of the Indonesian government" (274).

---

[2] The Gamaa Islamia is an extremist group that emerged in the southern regions of Egypt in the 1970s (Goerzig and Al-Hashimi 2007).

000158

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Singapore

Singapore's de-radicalization program was established in 2001. Prisoners must participate in the program in order to be released. The Religious Rehabilitation Group (RRG) was established in 2003 and is made up of 30 clerics who engage in weekly one-on-one counselling sessions with prisoners in an attempt to correct their views of Islam (Bin Ali 2008; Demant et al. 2008; Montlake 2007). The RRG also provides counselling to the families of the detainees, as well as public education on the issue of Islam. Since its inception, the RRG has carried out over 800 counselling sessions (Religious Rehabilitation Group 2010). This program has recently implemented artistic classes into their existing program and provides support for the prisoners' families, as well as help with resettlement after release (Neumann 2010).

The Philippines

The prison-based de-radicalization program in the Philippines will be launched in the near future and according to the ICSR report (Neumann 2010), it will be similar to the program used in Singapore.

Malaysia

The de-radicalization program in Malaysia is similar to that of Indonesia and Singapore. As with Singapore's program, the prisoners are forced to participate and the detainees cannot be released unless they participate (Demant et al. 2008). No further information regarding a formal evaluation of this program was found.

Saudi Arabia

The Saudi Arabia de-radicalization program was established in 2004. The program involves religious re-education and psychological counselling, with the goals for the prisoners to change their thinking from an extremist takfir[3] ideology to a secular view of Islam, as well as to change their behaviour. The detainees receive a reduced sentence in exchange for taking part in the program (Demant et al. 2008; Porges 2010b).

The program is headed by the Ministry of Foreign Affairs and is implemented by an advisory commission in Riyadh (Demant et al. 2008). The advisory commission is formed by four subcommittees:

- a religious committee that includes clerics, scholars and professors who participate in discussions with prisoners;
- a psychological and social committee that assess the participants' status and determines the support the prisoner and his family require;
- a security committee that determines the release of the prisoner and counsels the participants; and

[3] Note that takfir ideology refers to the belief that other Muslims and followers of other faiths are considered infidels (Demant et al. 2008).

000159

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- a media committee that provides educational and informational material (Demant et al. 2008).

Participation is mandatory; however, the prisoners are not always released (Demant et al. 2008). The program has several components, including:

- conversations between the prisoners and members of a religious committee (Demant et al. 2008);
- a six-week course consisting of group lessons that includes an exam that must be passed (Demant et al. 2008);
- counselling and an after care program which aids in the prisoner's reintegration into society (Porges 2010b);
- visitation rights of family members, who also provide support and input on the program the prisoner receives (Porges 2010b);
- an oath that must be signed by the prisoner, as well as the head of the family, stating that extremists views will be renounced (Mohammed 2009); and
- screening of clerics and an assurance that the clerics are seen as "brotherly", in order to assure credibility (Neumann 2010).

As of 2008, approximately 3000 prisoners had participated and 1400 have been released (Boucek 2008); however, 11 known former detainees of Guantanamo Bay who took part in the program returned to terrorist activities after release and the Interior Ministry has recently admitted that 10 to 20% of the prisoners may return to terrorism (Porges 2010b).

The program has been reviewed. With regard to its strengths, it has been argued that the program is successful because the detainees are treated with respect (Boucek 2008; Demant et al. 2008). Also, there is no torture and former militants participate in discussions with prisoners, increasing the credibility of the program (Demant et al. 2008). Furthermore, the prisoner's economic needs are addressed, which ensures that the prisoner does not have to return to illicit activities in order to support his family (Boucek 2008; Demant et al. 2008).

Some have argued that the program is 'too soft' and is not a strong deterrent to extremism (Demant et al. 2008). Also, not all participants are honest and as such, those who are released may still be very dangerous. Of further concern is that the prisoners must partake in the program but are not always released in return for their participation and the deep-rooted causes of radicalization are not addressed (Demant et al. 2008).

United States

The United States implemented their prison-based de-radicalization program in Iraq in 2006 at the detention facilities of Camps Cropper and Bucca (Azarva 2009). To date, 26,000 detainees have participated and 18,000 have been released (Kruglanski et al. 2010). Between January 2008 and September 2008, one-hundred of 15,000 released detainees returned to prison (Azarva 2009). The program is based on that of Saudi Arabia and includes:

- religious de-radicalization;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- vocational training;
- civic education;
- art programs;
- family, tribe and community engagement;
- counselling and medical treatment; and
- job placement (Kruglanski et al. 2010, 2).

The program also includes an accredited education centre (Dar al-Hikma or the House of Wisdom), which was implemented in August 2007. The education center offers lessons on several topics, including languages, math and science, and is now in high demand among detained and non-detained individuals. The education program also includes discussions between Iraqi clerics and detainees, which are aimed at changing extremist beliefs (Azarva 2009). The education program "is designed to enable the detainees to read and interpret religious text on their own" (Azarva 2009, 5). In addition, there are vocational and pay-for-work programs, which aid in the reintegration process (Azarva 2009).

Although the program has not yet been formally evaluated, it has received some criticism. Some have argued that this program acts as a 'band-aid', as it focuses on the symptoms of extremism, but does not address the causes (Azarva 2009). In order to maintain the program and attend to the detainees, many more corrections officers will be needed. Also, the transfer of detainees from Camps Cropper and Bucca to the government-run Iraqi prison system will also cause concerns, as the Iraqi prison system is known for overcrowding and abuse (Azarva 2009).

Yemen

The Yemen deradicalization project was launched in 2002 under the name "The Yemeni Committee for Dialogue". The project was founded by [redacted], but was never fully established (Porges 2010a). The project consisted of dialogues with imprisoned Islamists with the goal of changing their views from neo-Jihadist views to one that is more tolerant and ultimately helping the detainees reintegrate into society (Birk 2009). The content of the dialogue focused on a number of goals, including the "rejection of violence, respect for the rights of non-Muslims, protection of foreign interests and respect for the constitution and laws of the country" (Birk 2009, 10). The dialogues consisted of several sessions in which five to seven detainees would meet with the dialogue committee. Prisoners who were suspected of having engaged in serious offences were not allowed to participate in the religious dialogues (Neumann 2010). In addition, in order to be released, the detainees had to sign an oath stating that they would abide by the program goals (Birk 2009). s.19(1)

More than 300 prisoners were released between 2002 and 2005; however, the program was terminated in 2005 after "two former detainees were caught fighting American forces in Iraq" (Birk 2009, 3). Some of the detainees have stated that "they did not actually change their ideas and that no genuine exchange of opinions amounting to dialogue actually took place" (Birk 2009, 4). Moreover, several former program participants have recently been caught leading violent attacks in Yemen. Also, the detainees were held for as long as two years, without having been officially charged or seeing a lawyer (Birk 2009). Many of the detainees stated that they were not extremists, but they had become anti-government as a result of having been forced to

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

take the program and being held on weak evidence. Furthermore, Birk (2009) argues that the committee and the detainees were unequal, as the committee was assembled by the president personally and the detainees were at the state's mercy. As such, "the possibility of a true dialogue with a genuine mutual exchange of ideas was undermine from the beginning" (Birk 2009, 17). In addition, the prisoners were promised financial aid after release, which they were not provided (Neumann 2010).

As a result of the potential transfer of Yemeni prisoners currently held in Guantanamo Bay prison back to Yemen, there have recently been discussions around the reinvention of the Yemeni Committee for Dialogue (Porges 2010a). The plans for the possible reinvention of the de-radicalization program have only recently begun and according to Porges (2010a), a rehabilitation program has not yet been established, nor has any funding been committed to the program.

Evaluation of Prison-Based De-radicalization Programs Targeting Neo-Jihadist Terrorism.
The International Centre for the Study of Radicalisation and Political Violence (ICSR) recently published a report exploring prison-based de-radicalization and disengagement programs in several countries, including Afghanistan, Indonesia, the Philippines, Saudi Arabia, Singapore and Yemen.

Factors Unique to Prisons

The report discusses elements related to the use of prisons generally. According to the report, the vulnerability that inmates feel while in prison can facilitate radicalization, and overcrowded and understaffed prisons can also amplify the risk for radicalization as radicalization becomes more difficult to detect (Neumann 2010). As such, the report suggests that the most important step that prisons can take in reducing radicalization is to "improve general conditions, avoid overcrowding, train staff, and provide meaningful programming that allows prisoners to develop stable inmate identities" (Neumann 2010, 60).

Other Factors for Consideration Regarding Prison Programs

Another important element discussed in the report is the importance of involving the prisoners' families and providing them with financial support or employment opportunities (Neumann 2010). According to the ICSR report, programs need to be adjusted to reflect the specific circumstances and locations of the prison, as elements that work in one program may not necessarily work in another program (Neumann 2010). Additionally, the report argues that "for programmes to be effective, their scope, structure and instruments must reflect local contexts and conditions" (Neumann 2010, 57), such as the needs and motivations of the prisoners, the ideology of the prisoners and the prisoners' societies, other external conflict that may influence the program's effectiveness, and what the external society deems to be acceptable (Neumann 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Considerations of Inmate Management

Another aspect that is discussed in the report is the dispersion of terrorist prisoners in prisons. While some prisons hold terrorists in the same location (concentration), others separate them from other prisoners (separation), while others isolate terrorists from one another (isolation) (Neumann 2010). Many prisons disperse the terrorist prisoners among a small number of prisoners, which is a dispersal and (partial) concentration approach. It is argued, however, that "even with such mixed regimes, it rarely seems to be a good idea to bring together leaders with followers and mix ideologues with hangers-on" (Neumann 2010, 1). The ICSR report also states that prisons should focus on both security and reform, rather than only on security alone, as this will aid prisoners in their re-entry into society once they are released (Neumann 2010). In regard to the use of prison imams[4], the report argues that while they are important, they are not a cure all and their "independence and credibility needs to be protected…it is neither reasonable nor realistic to expect them to be spiritual advisers, welfare officers and terrorism experts all at the same time" (Neumann 2010, 2).

Best Practices and Recommendations

The ICSR report states that evaluating the programs is difficult, as is comparing the different programs, due to differences in location, the length of time the programs have been in effect, as well as differences in eligibility rules (Neumann 2010). The report is careful to note that while prison-based de-radicalization programs can be effective, it is important that they be used in conjunction with other anti-terrorism policies. Nevertheless, the report discusses elements that are common in the most effective programs. These include:

- A mix of different kinds of programming, typically combining ideological and/or religious re-education with vocational training;
- Credible interlocutors, who can relate to prisoners' personal and psychological needs;
- Emphasis on prisoners' transition back into mainstream society, typically by providing them with the means for a new beginning and by establishing social networks away from extremism;
- Sophisticated methods for locking prisoners into multiple commitments and obligations towards family, community and the state; and
- Although material incentives (e.g., early release from prison, financial assistance upon release) can be useful, they are not adequate on their own as an effective way of changing an individual's extremist views (Neumann 2010, 3).

A recent Canadian publication by Wilner (2010) also provides recommendations regarding steps that can be taken in combating radicalization in the prison setting. Wilner (2010)'s recommendations are similar to those provided in the ICSR report, such as the need to help prisoners re-integrate into society once released and providing education to prisoners on more moderate ideas of Islam. In addition, Wilner (2010) states that it is important to understand how radicalization occurs in Canada specifically and suggests that a prison guide be produced on the

---

[4] The primary role of a prison imam "is to look after prisoners' spiritual needs and ensure the provision of adequate religious services" (Neumann 2010, 36).

000163

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

processes of and indicators of radicalization in the prison setting. Wilner (2010) also suggests that extremists should not have access to other prisoners, that radical religious leaders should not be granted access to prisons, that prison libraries be screened for radical literature and that legitimate grievances be dealt with in a sensitive manner, so as to not violate the rights of prisoners and allow radicals to "seize on these incidents to start promoting their message of alienation and hate" (Wilner 2010, 5).

3.5.2 Other Prison-Based De-radicalization Program

Northern Ireland's Early Release Scheme

Northern Ireland's Early Release Scheme was initiated in 1998 as part of the Good Friday Agreement (Horgan and Braddock 2010). The Early Release Scheme ensured release to political prisoners on the promise that they would not violate the conditions of their release. If the released prisoner did violate these conditions, or if the individual's affiliated group broke the ceasefire, the individual would have to return to prison and serve the remainder of their sentence, along with any new sentences (Horgan and Braddock 2010). Only groups that respected the Good Friday Agreement were eligible to take part in the Early Release Scheme.

Upon release from prison, the individuals were provided with financial aid, skills training and with help in finding employment by the government (Horgan and Braddock 2010). Many criticized the government aid that the ex-prisoners received, as many believed that the aid received was unsatisfactory in helping the individuals reintegrate. As a result, other organizations, such as the European Union, launched programs to aid the ex-prisoners in their rehabilitation and reintegration process (Horgan and Braddock 2010).

According to Horgan and Braddock (2010), the Early Release Scheme has "played a pivotal and successful role in bringing peace to Northern Ireland" (271). Although a formal evaluation of the Early Release Scheme could not be located, publications discussed by Horgan and Braddock (2010) indicate that recidivism among individuals who have been released under the Early Release Scheme has been quite low. A 2008 report by the Independent Monitoring Commission[5] (IMC) found that, between "March 2003 through August 2008, [...] of all the groups whose violent activity was documented by the IMC, none were signatories of the Good Friday Agreement" (Horgan and Braddock 2010, 270).

[5] The International Monitoring Commission was established in 2003 by the British and Irish governments to "supervise and report on the actions of paramilitary groups in Northern Ireland" (Horgan and Braddock 2010, 270).

000164

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

4. De-Radicalization Programs Focusing on Right-Wing Terrorism

4.1 Denmark

4.1.1 De-radicalization-Targeted Intervention

Denmark's national radicalization and extremism prevention strategy was established in 2009 and is entitled "A common and safe future: An action plan to prevent extremist views and radicalization among young people" (Ministry of Refugee, Immigration and Integration Affairs 2010). The strategy is coordinated by the Ministry of Integration's Division for Cohesion and Prevention of Radicalisation. This strategy includes seven different areas:

1. Direct contact with the young people
2. Inclusion based on rights and obligations
3. Dialogue and information
4. Democratic cohesion
5. Efforts in vulnerable residential areas
6. Special initiatives in prisons
7. Knowledge, co-operation and partnerships (Ministry of Refugee, Immigration and Integration Affairs 2010, 24).

Programs focused on intervention are included under the first area of the strategy (direct contact with young people) (Ministry of Refugee, Immigration and Integration Affairs 2010). One program that has been developed in this area is the "De-radicalization–Targeted Intervention" program. This program has been established for a three-year period, from 2009 to 2012, and is supported by the EU Commission (Ministry of Refugee, Immigration and Integration Affairs 2010).

The De-Radicalization-Targeted Intervention program, in which participation is voluntary, "aims at supporting young persons in leaving extremism and discriminatory violent behaviour behind" (Ministry of Refugee, Immigration and Integration Affairs 2010, 25). The program consists of two components. The first component of the program, which is being developed by the Danish Security and Intelligence Service, consists of the development of 'exit talks' with youth who are part of extremist groups. The second part of the program, which is being developed by the Danish Ministry of Refugee, Immigration and Integration Affairs, in cooperation with the municipalities of Copenhagen and Aarhus and the East Jutland Police, is the development of mentoring schemes, which involve contact between a mentor and an individual who holds extremist views (Ministry of Refugee, Immigration and Integration Affairs 2010).

Young people who are eligible for the program are to be identified by youth workers, teachers and other groups familiar with extremist groups. The program involves on-going contact and dialogue between the mentors and the participants, in which the participant is provided with support and in which their extremist views are challenged (Ministry of Refugee, Immigration and

000165

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Integration Affairs 2010). The program is tailored to the participant's needs and may involve social support, aid in obtaining education or employment, counselling and family member involvement. The program does not provide financial support to the participant (Ministry of Refugee, Immigration and Integration Affairs 2010).

According to the Ministry of Refugee, Immigration and Integration Affairs (2010), mentors were to be selected in 2010 and were to be selected based on their skills and knowledge regarding the local area of the participant. It was expected that the mentors would likely be social workers, teachers, or former police officers. The mentors were to also be supervised and supported by a group of municipal employees who were also to receive training (Ministry of Refugee, Immigration and Integration Affairs 2010). As this program has only recently been implemented, an evaluation of this program could not be located.

4.2 Germany

4.2.1 Aussteigerprogramm fur Rechtsextremisten vom Bundesverfassungsshutz

This program focuses on two different groups. The first group consists of individuals who are leaders of extreme right-wing groups who wish to disengage and require help to leave their group (Demant et al. 2008). The second group of individuals are group members who are not group leaders. The program begins when a member of the project team called the Bundesverfassungsshutz (BfV) contacts these individuals and provides them with information about how they can disengage. Once the individual had agreed to disengage, a profile is constructed of these individuals and a detailed contract is created that establishes a timeline in order to meet their goals (Demant et al. 2008). The individual is provided with help in finding a different source of income and with rehabilitation. The state security services are also involved through contact with the BfV (Demant et al. 2008). The program takes approximately four years to complete, as the individual generally takes two years to meet the goals of the project and must maintain these goals for two years in order to be considered to have completed the program successfully. Approximately 100 people have disengaged from extreme right-wing groups, or are receiving counselling, with the help of this organization (Demant et al. 2008). Information on evaluations of this project could be not found.

4.2.2 Exit Deutschland

Founded in 2000, 'Exit Deutschland' was the first de-radicalization project in Germany. Individuals who wish to disengage are responsible for contacting the program (Demant et al. 2008). Once in the program, a profile of the individual is formed and from this profile, potential problems are identified. The project involves in-depth discussions between the disengager and a project team member, intended to compel the individual to re-consider their extremist views. The individual is also provided with support for psychological issues, where applicable, and measures to ensure the safety of participants are taken and job support is provided (Demant et al. 2008). The length of the program varies from six months to three years and the program has helped 230 individuals disengage from the extreme right-wing movement. Information on formal evaluations of this program could not be located. Demant et al. (2008) do note, however, that because the program does not have stable funding, it experiences financial difficulties.

000166

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

4.2.3 Help for Right-Wing Extremist Drop-Outs

This program is targeted at individuals who have committed a crime that is related to right-wing extremism and who also wish to leave the right-wing extremist movement. The individual must voluntarily contact the program and be able to provide personal information (Ministry of Refugee, Immigration and Integration Affairs 2010). The program provides the participants with a safe environment in which they can discuss their problems and fears. In addition, ideological alternatives to the participants' right-wing extremist views are provided. The participant is provided with support in planning for their future, finding accommodation, obtaining an education and finding employment (Ministry of Refugee, Immigration and Integration Affairs 2010). The participant is also provided with emergency accommodation and, in some circumstances, is provided with financial support to help meet their needs. According to the Ministry of Refugee, Immigration and Integration Affairs (2010), "[a] number of different partners have been involved in developing this program, [including] sub-national and local authorities, judicial sub-national agencies, police officers and non-governmental organisations" (16). Information regarding an evaluation of this program could not be located.

4.2.4 Taking Responsibility-Breaking Away from Hate and Violence

This program was established in 2005 and is focused on youth who are in prison for serious violent crimes and who also hold xenophobic and right-wing extremist viewpoints (Korn 2009; Ministry of Refugee, Immigration and Integration Affairs 2010). The program is in place in 11 prisons across Germany (Koschmieder and Heitmann 2009). "The programme takes measures to address issues on how to stay out of violence after release, and develop resources regarding communication, relationships and conflict-resolution in order to plan for an independent, non-violent and positive future" (Ministry of Refugee, Immigration and Integration Affairs 2010, 11). Youth are recommended for the program by prison staff and must have an upcoming release date. In order to participate in the program, the youth must be willing to discuss their past behaviours and must follow the rules of the program. It is a five-month program that involves weekly training sessions in which the youth discuss the consequences of violence, ideology and social issues such as unemployment (Hartnub, n.d.; Ministry of Refugee, Immigration and Integration Affairs 2010). At the beginning of the program, the youth partakes in a one-on-one interview. After this initial interview, training sessions are provided in a group setting with 6 to 9 participants (Ministry of Refugee, Immigration and Integration Affairs 2010). In addition to the group training sessions, discussions challenging right-wing extremism are also held in the detention centres. The youths' family and friends are also encouraged to be involved in the program. Once released, the participants are provided with one year of counselling and support in obtaining education, employment and housing (Ministry of Refugee, Immigration and Integration Affairs 2010). More than three-hundred youth participated in the program between 2001 and 2007 (Korn 2009). According to Korn (2009), "of these [youth], 80% have been released already, less than 5% have been imprisoned again and only 1% [of these have been re-imprisoned] due to criminal acts of violence (35).

The program engages in ongoing evaluation and regular re-assessments by program management (Hartnub n.d.). According to the Ministry of Refugee, Immigration and Integration Affairs (2010), the program has been evaluated "through interviews with participants, prison staff,

000167

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

trainers and inmates, who are not participating in the programme" (14).[6] In addition, results of the evaluation have been used to improve and update the program and its curriculum (Ministry of Refugee, Immigration and Integration Affairs 2010).

4.2.5 The Hessian Programme for Disengagement from Radicalization

This program began in 2003 and targets youth from extreme right-wing groups (Demant et al. 2008). In this program, a personality profile is prepared, extreme right-wing paraphernalia is removed from the individual's residence and a detailed contract is created (Demant et al. 2008). The project officer ensures the individual's safety, as well as a source of income and personal support. The program generally lasts from three to six months; however, for some, the program can last up to two years. To date, the program has helped 50 individuals disengage from the extreme right-wing movement since it began (Demant et al. 2008). A formal evaluation of this program could not be located.

4.2.6 The North-Rhine Westphalian Programme for Disengagement from Radicalization

This program targets members from the Kameradschaften[7] and other right-wing groups (Demant et al. 2008). The program begins with "a clean up of the individual's residence, in which all extreme right-wing paraphernalia is confiscated" (Demant et al. 2008, 168). Individuals in this program must sign a contract agreeing to disengage from right-wing surroundings and not to commit any offences (Demant et al. 2008). The program helps disengagers through the process of changing their lives and with obtaining drug and alcohol rehabilitation. The program, which lasts three years on average, is initially very intensive, but the intensity declines over time (Demant et al. 2008). Formal evaluations of this project could not be located.

4.3 Norway

4.3.1 Exit Programme

The 'Exit Programme' exists in Norway, Sweden and Denmark[8] (Kimmel 2007). Norway's 'Exit Programme', which is focused on helping youth, was developed between 1995 and 1997. The program has three main goals:

- to provide help and support to youth who want to leave the extreme right-wing movement, or other violent groups;
- to provide support to parents whose children are involved in the extreme right-wing movement or other violent group through the development of local parental networks; and
- to develop and provide knowledge for professionals who work with youth from violent groups (Demant et al. 2008).

---

[6] Please note that this evaluation is not available in English.
[7] The Kameradschaften is an extreme right-wing group in Germany.
[8] Note that information regarding the Exit Program in Denmark could not be located.

000168

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Local government agencies manage the Project, with support from community members (Counter-Terrorism Implementation Task Force n.d.). The government withdrew much of its funding for this program, as they felt that the situation has been addressed (Demant et al. 2008). The program employs former members of extremist groups and provides a contact not only for the youth who wishes to leave the movement, but also to parents and professionals. The program includes a telephone number that youth can use when they would like to disengage and individuals in prison can also contact the program when they are also ready to disengage. The program helped more than 70 youths leave the right-wing movement or other violent groups over a two-year period (Demant et al. 2008).

The program includes several different organizations. For example, the Police Security Service is involved by ensuring that youth who are at risk of being involved in right-wing extremism do not become more deeply involved. In order to achieve this goal, the police contact the youth and the youth's parents to attend a meeting at the police station for a preventive talk in which the youth is informed of future consequences if the youth continues on their current path (Demant et al. 2008). The Police Security Service is also involved by removing the more entrenched members out of the groups by arresting the individual for small violations and discussing the consequences of their actions (Demant et al. 2008).

The Coordination Group for Crime Prevention in Kristiansand, which is a coordination group consisting of various authorities in Kristiansand, is charged with the development of intervention methods for youth and is another organization involved with the 'Exit Program'. The Coordination Group includes several sub-projects. For example, the Church Youth Project consists of three social workers and helps youth find jobs, housing or education (Demant et al. 2008).

Demant et al. (2008) noted that the Project is aimed at individuals who do not yet have strongly established social positions. Because the majority of the right-wing extremists in Norway are youth who have not yet developed their own social position, the program appeals to these youth. The program does not, however, appeal to those who are more entrenched in the right-wing movement. Demant et al. (2008) also state that the programs would be more successful if ideology was addressed. In addition, Demant et al. (2008) argue that "there is little overview of groups or movements that extend beyond local level" (170), and the role of the internet has not been taken into consideration. In addition, Kimmel (2007) conducted interviews with several clients and staff of the Exit programs in Norway, Sweden and Denmark. According to Kimmel (2007), a reason why the Exit program is successful is because it balances its focus on both ideology and on the need for the young men to prove their manhood. This approach helps the client think about his ideology and how it is separate from his identity (Kimmel 2007).

000169

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

4.4 Sweden

4.4.1 Exit Stockholm

The 'Exit Program' was established in Sweden in 1998 under the name 'Exit Stockholm'[9]. The Exit Program "aims to facilitate disengagement of young persons from groups consisting of destructive young people such as Neo-Nazi groups or other right-wing extremist groups" (Ministry of Refugee, Immigration and Integration Affairs 2010, 28). In addition to providing help to individuals wishing to leave the extreme right-wing movement, parents whose children are involved in the right-wing movement and authorities who would benefit from knowledge of right-wing extremism, such as the police, are also provided with support (Ministry of Refugee, Immigration and Integration Affairs 2010).

Although 'Exit Stockholm' has the same goals as the 'Exit Norway' program, it is organized differently (Demant et al. 2008). For example, many of the staff have formerly been involved in the extreme right-wing movement, which increases the credibility of the staff among the youth who they are targeting (Demant et al. 2008).

The program is composed of five different stages:

- The first is a motivation phase, in which the youth is involved in a right-wing group, but is questioning this involvement and contacts the program.
- The second phase is disengagement, in which the youth has decided to leave the group and begins to receive help from the program.
- The third is the settling phase, wherein the person has left the group completely and the members of the program help the individual to establish ties to a more mainstream life.
- The fourth phase is the reflection phase, in which the individual lets go of their extremist ideas and is often in need of mental health support.
- The final phase is the stabilisation phase, in which the individual is now removed from the group and is living a more mainstream lifestyle. In the stabilisation phase, the Exit Program is no longer involved, although the individual often remains in contact with the program (Demant et al. 2008).

The discussions that take place throughout the phases are aimed on "building upon the personal desire to distance oneself from the extreme right-wing movement and establish a normal life" (Demant et al. 2008, 164). The program takes six to 12 months to complete (Demant et al. 2008). In addition to a focus on disengagement, the program also includes education and information for teachers, individuals who work in youth-focused clubs and other individuals that focuses on the awareness of signs of right-wing extremism (Ministry of Refugee, Immigration and Integration Affairs 2010).

The individual wishing to participate in the Exit program must contact the program to seek help. Upon contacting the program, the participant engages in meetings with the program's coaches

[9] This program is now known as 'Exit Fryshuset' and is known internationally as 'Exit Sweden' (Orëll 2010, Personal Communication).

000170

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Ministry of Refugee, Immigration and Integration Affairs 2010). The participants are not provided with financial aid; however, they are provided with practical support with help in finding temporary shelter. The program also provides a 24-hour help-line for the participants and family members are often encouraged to participate (Ministry of Refugee, Immigration and Integration Affairs 2010).

Sweden's National Council for Crime Prevention conducted an evaluation[10] of the program in 2001. The evaluation involved interviews with youth who had received help from Exit, as well as their parents, and representatives from schools and other institutions in which Exit had provided lectures and training sessions. These interviews indicated that the youth and the parents had found the assistance they received from Exit very helpful and school representatives were very satisfied (National Council for Crime Prevention 2001). The evaluation notes that the strengths of the program include familiarity of the staff with the issues of the extreme right-wing movement, as well as flexibility of the staff to be available to work at all times. Moreover, the evaluation found that by 2001, 133 individuals had received help by the Exit program and 125 of these individuals had left the extreme right-wing movement (National Council for Crime Prevention 2001), indicating a very high success rate.

The program, however, does have some flaws. The program was accused of fraud after the release of their 2001 revision report (Englund 2002), and has suffered from a high staff turnover, as well organizational problems (Demant et al. 2008). The weaknesses of the operation that were discussed in the evaluation conducted by Sweden's National Council for Crime Prevention were that its "organizational structure, decision-making procedures and professional leadership are often inadequate" (National Council for Crime Prevention 2001, 48). The report states that in order to address their high turnover rates and for the program to continue, both administration and personnel management capabilities must be improved. Finally, the report states that the program must improve its collaboration with other local agencies (National Council for Crime Prevention 2001).

4.4.2 Exit Motala

The 'Exit Motala' program was established in 1999 and exists in three cities: Motala, Karlskrona and Helsingborg (Englund 2002). The program is focused on offering help to youth from violent extreme right-wing environments, marginalized young immigrants and asylum seekers (Demant et al. 2008). The objectives of the project include disengagement from extreme right-wing environments, fighting racism and marginalization and promoting democratic principles (Demant et al. 2008).

The project has three components. The first is 'Exit', which targets extreme right-wing youth and is similar to the 'Exit Stockholm' program. The second is 'Amir', which is aimed at helping young immigrants from criminal gangs and asylum seekers. The third is 'Dellen', which is oriented towards girls from extremist groups. The general objective of Exit Motala is to integrate

[10] Note that according to the Ministry of Refugee, Immigration and Integration Affairs (2010), the program is continuously evaluated by the government; however, these evaluations could not be located.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the members from these three components through activities that bring members from the three groups together, in an attempt to help eliminate racist views (Demant 2008; Englund 2002).

The organization involves three key individuals when working with a youth: a social worker that offers mental health support, a member of the team who was previously engaged in the right-wing movement, and administration staff that ensure the day-to-day operations of the program (Englund 2002). Some of the methods used include the same five-step plan for disengagement that is applied in Exit Stockholm, as well as individual therapy, and the 'Choice of Path' programme, which targets youth involved in crime (Demant et al., 2008). The 'Choice of Path' program includes a brochure highlighting ethical and moral questions and exercises aimed at improving their value judgements in making choices (Demant et al., 2008).

Although the program has not been formally evaluated, Englund (2002) does note that in order for the project to expand, more staff is needed. Englund (2002) also states that the program has received support from the local community and media, and has been successful in facilitating the integration of quite a few marginalized youth into Swedish society.

000172

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5. Counter-Radicalization Programs

5.1 Australia

5.1.1 National Action Plan for Commonwealth

On August 23, 2005, the Prime Minister of Australia met with leaders of Muslim communities throughout Australia (Council of Australian Governments 2008). At the conclusion of this meeting, a 'Statement of Principles'[11] was formed, which denounced terrorism, and provided a framework for the development of a National Strategy to combat intolerance and extremism (Council of Australian Governments 2008; Department of Immigration and Citizenship 2005).

As a result of the 'Statement of Principles', the 'National Action Plan for Commonwealth' was formed. The 'National Action Plan' outlines government initiatives to "deliver an effective means to promote the common goals of harmony and understanding and challenge extremism" (Department of Immigration and Citizenship 2005, 13). Initiatives of the plan focus on:

- public education, employment and community activities;
- engaging with communities through consultations and ongoing dialogue;
- building leadership capacity and communication skills in Australian communities;
- supporting leaders and teachers; and
- improving understanding of the causes of extremism (Department of Immigration and Citizenship 2009).

The National Action Plan will be evaluated in 2009/2010.

Another initiative that was formed as a result of this meeting was the 'Muslim Community Reference Group' (MCRG), which was formed in 2005 (Muslim Community Reference Group 2006). The group was established for one year to provide advice to the government (Department of Immigration and Citizenship 2009). The MCRG consisted of 14 Muslim community members who were chosen by the Prime Minister (Spalek and Imtoual 2007) and was made up of seven subgroups which focused on "issues relating to youth, education and training of imams and other religious teachers and leaders, women, schooling, employment, crisis management and family and community" (Muslim Community Reference Group 2006, 9). In 2006, the MCRG published a report for the Commonwealth providing recommendations on issues of radicalization and extremism. [12]

The Muslim Community Reference Group (MCRG) has received criticism. Spalek and Imtoual (2007) argue that the MCRG does not reflect the concerns of ordinary Muslim Australians and that the "main task of the MCRG is to assist the Commonwealth government to identify, isolate

---

[11] A full listing of the Statement of Principles can be found at http://www.coag.gov.au/coag_meeting_outcomes/2005-09-27/docs/attachment.cfm (Date last accessed: December 20, 2010).

[12] A copy of this report can be found at http://www.immi.gov.au/living-in-australia/a-diverse-australia/mcrg_report.pdf (Date last accessed: December 20, 2010).

000173

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

and detain Muslim community members who are also seen to be 'extremists', 'terrorists' or potential terrorists" (193). In addition, the MCRG is tasked with providing advice to the government on several issues of importance to Muslim communities, such as the role, training and accreditation of imams in Australia. Spalek and Imtoual (2007) state, however, that discussions held around this issue were largely controlled by the government and that members of the Muslim community were not adequately involved. In line with the discussions surrounding the training and accreditation of imams, Spalek and Imtoual (2007) further argue that there was also oversight with regard to religious differences within Muslim beliefs, as there were no distinctions made between the religious differences held by Muslim communities (at the time the report was published).

5.2 Canada

5.2.1 *Cross-Cultural Roundtable on Security*

The Cross-Cultural Roundtable on Security consists of a maximum of 15 members who are "leaders in their respective communities and who have extensive experience in social and cultural matters" (Public Safety Canada 2010). The members provide information and advice to the Ministers of Public Safety and Justice regarding issues related to national security which are considered in decisions relating to policy, including topics such as terrorism and radicalization (Public Safety Canada 2010). The first members were appointed in February 2005, with new members announced in March 2008. Members are appointed for a term of two years. The mandate of this group is "to engage Canadians and the Government of Canada in an ongoing dialogue on national security in a diverse and pluralistic society" (Public Safety Canada 2010). Members of the Roundtable also organize outreach events in their respective communities designed to better facilitate dialogue between members of the community and the Government.

5.2.2 RCMP's National Security Community Outreach Program[13]

The RCMP's experience with outreach and community policing in the provinces has allowed it to develop significant expertise when it comes to reaching out to diverse communities.

Starting in 2005, [the RCMP's] efforts provided a more coordinated and effective delivery of outreach, and to address concerns raised by a number of communities. These concerns centred around marginalization, racial and ethnic profiling and prejudice, as well as the fear of police. These efforts aim to establish trust with minority communities and gain their assistance and co-operation in protecting Canada's national security.

The RCMP's community policing problem solving model called CAPRA is the foundation used to develop national security outreach efforts. CAPRA's goal is to establish a community-led, police-supported response to mutually identified issues. Each letter in the acronym corresponds to actions taken by the stakeholders.

---

[13] Note that Section 5.2.2 to Section 5.2.5 come from an internal memo from the Royal Canadian Mounted Police that was prepared by Andrew Archibald on February 18, 2011. The memo was sent to Nicole Crutcher by Angus Smith on February 18, 2011.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

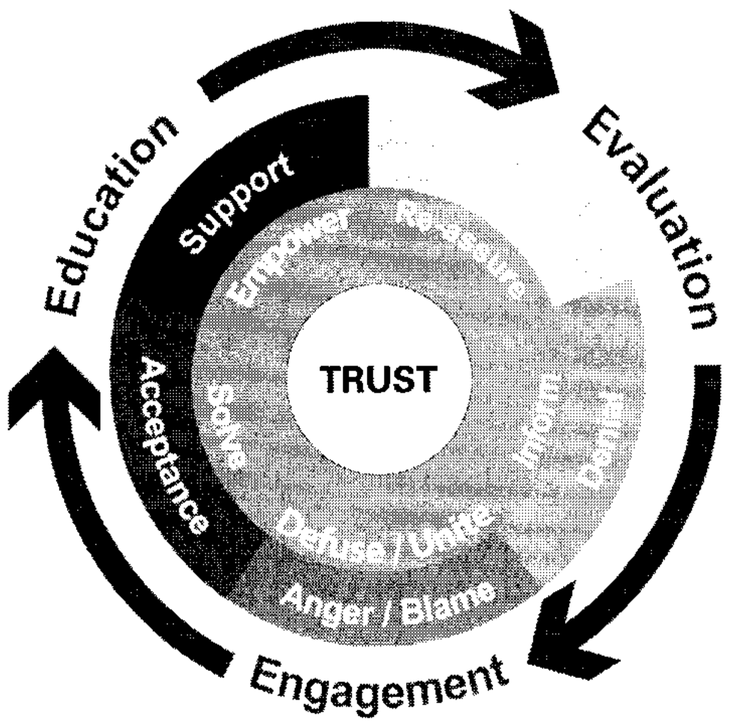
- *Clients*: Individuals and groups affected–both directly and indirectly–by the issue need to be identified. The views of these stakeholders should be understood and considered.
- *Acquiring and Analyzing*: The issue must be described in detail and a number of probing questions considered. How has this issue been dealt with in the past? What are the needs and expectations of a community? What barriers exist and how can we overcome them?
- *Partnerships*: Resources available to solve the issue need to be listed. Where gaps exist, new partnerships should be established. The right mix of knowledge, skills, and resources is the objective.
- *Response*: Solutions must be sustainable, measurable, realistic and timely. Partners must also be coordinated and work collaboratively toward the goal.
- *Assessment*: The decided upon solution needs to be measured for effectiveness so that continuous learning and improvement can occur.

Specifically, one of the goals of this outreach work is to educate Canadians of diverse backgrounds about the national security role of the RCMP and the need for the assistance and co-operation of all Canadians to prevent terrorism. As such, the RCMP meets regularly with community members through the National Security Community Advisory Committee in the National Capital Region, attends community events and makes presentations to students at post-secondary institutions. Since the New Year, RCMP National Security Outreach has spent time with more than 14 different community groups in the Ottawa area. Future events in the province of British Columbia include a multi-day event entitled the "Citizen's Academy." This event will introduce attendees to Canada's security partners, the criminal justice system, and will participate in a table top exercise based on a terrorism investigation.

In to these initiatives, the RCMP encourages communities to engage in the Cross-Cultural Roundtable on Security. As well, all National Security Criminal Investigations (NCSI) personnel and others, including investigators and analysts, are provided with cultural awareness training specifically developed and delivered in partnership with the community.

If a terrorist incident is to occur, affected communities will experience a range of emotions. During this time, the RCMP–through National Security Community Outreach–will work to provide the right support.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



In order to do so, the relationship between law enforcement and communities must be centred on trust. This trust is fostered through open dialogue and effective outreach. The inner light blue circle is the role of police during incidents such as arrests, criminal activity or other events that strain our communities. The next larger circle represents some of the phases communities can experience when exposed to a stressful event. During times of uncertainty, Police can re-assure communities. When communities are angry and laying blame, Police can defuse by sharing information and working to unite communities through open dialogue. The outer ring demonstrates that this is a continual, ongoing process that requires assessment to improve, engagement between the partners, and education of both the community and law enforcement agencies. Again, this is accomplished through existing community outreach efforts such as attending significant community events, sharing information about the RCMP's role, and work on crime prevention.

An additional component of National Security Community Outreach is National Security Youth Outreach, which aims to address increasing concerns about youth radicalization leading to violence. The two strategic goals are:

- To engage youth on national security issues (through education, awareness, dialogue, partnerships, and the formation of a National Security Youth Advisory Committee); and
- To prevent youth violent extremism in Canada (through consultations with stakeholders, examining existing research and programs, identifying lessons learned, best practices, and effective strategies in intervention and prevention, at the domestic and international levels)

Specific youth outreach events include day-long "Junior Police Academies" where youth from multiple faiths take part in realistic police training and build positive relationships among their peers and with members of the RCMP (Royal Canadian Mounted Police 2011).

5.2.3 The Canadian Association of Chiefs of Police (CACP) Counter-Radicalization Study Group

The [National Security Criminal Investigations (NSCI)] has worked closely with the [Canadian Association of Chiefs of Police (CACP)] Counter-Radicalization Study Group, consisting of

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.16(1)(b)

s.16(1)(c)

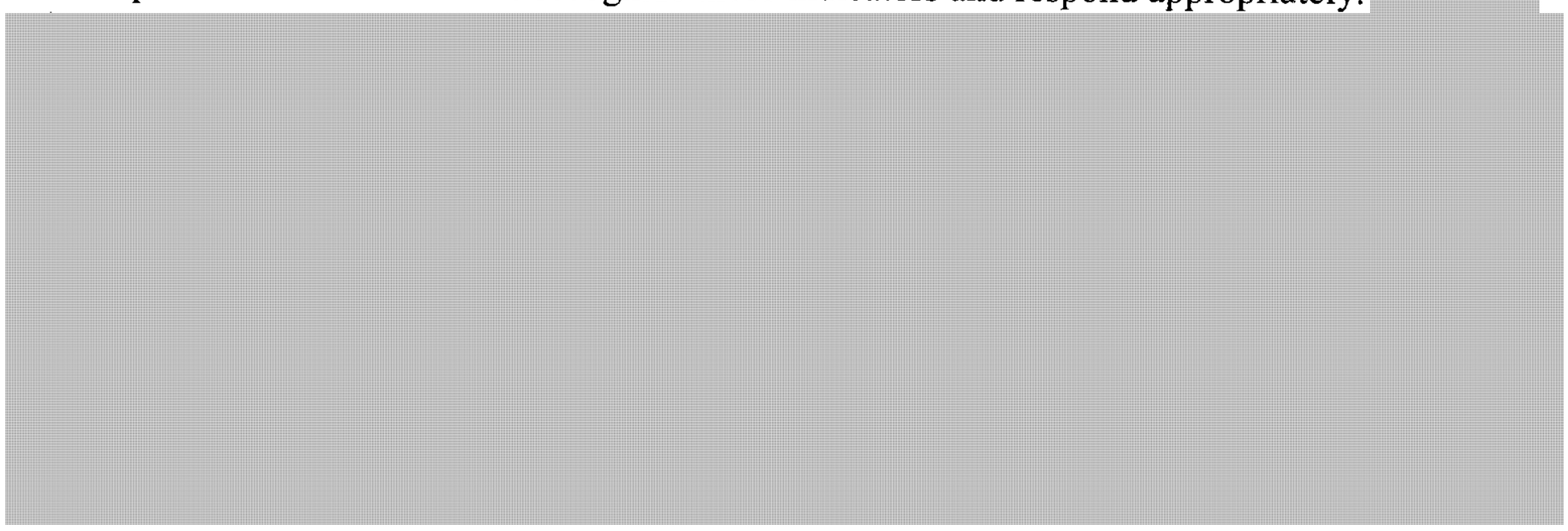
members of a number of other Canadian police agencies, the Canadian Security Intelligence Service (CSIS), the Department of Foreign Affairs and International Trade (DFAIT), and Public Safety Canada's National Security Policy Directorate. This working group, which was established in 2008, is developing a radicalization prevention strategy for the entire Canadian law enforcement community, under the auspices of the CACP Counterterrorism and National Security (CTNS) Committee. An initial position paper was submitted to the CTNS Committee in August 2008.

The paper is based on the Study Group's mission to the United Kingdom (UK) in May 2008, where it met with key British agencies engaged in counter-radicalization activities. The paper outlines lessons learned, identifies key challenges, and makes recommendations with respect to Canadian activity in this area. In brief, it notes that any comprehensive Canadian counter-radicalization strategy must reflect Canada's unique reality, and cannot blindly import methodologies that have had success in other countries. For example, it notes that the UK's focus on a specific ethno-cultural community would be at odds with Canada's approach to multiculturalism, and that any long-term strategy for countering radicalization leading to violence should be applicable to Canadian society as a whole. That said, the paper also points to the success of the UK's whole-of-government approach, and recommends a Canadian strategy that is similarly highly centralized at the policy level, and highly flexible at the implementation level.

The working group will continue to identify best practices related to radicalization and prevention, both within the RCMP and other agencies, and will then provide advice as to how to standardize them across the law enforcement community. In addition, the group will continue to work on developing appropriate indicators and messaging pertaining to radicalization. To follow up on a video conference that took place in May 2009, the group will meet again in September to continue developing the framework (Royal Canadian Mounted Police 2011).

5.2.4 Counter-Terrorism Information Officers (CTIO)

The objective of the [Counter-Terrorism Information Officers (CTIOs)] is to increase national security awareness across the provinces so that first responders have the necessary knowledge to identify national security threats as early as possible. CTIOs play a key role in keeping first responders abreast of current terrorist tactics, techniques and practices. With this information, first responders are better able to recognize these indicators and respond appropriately.



000177

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5.2.5 RCMP Research Initiatives

The RCMP is actively working with a number of academics on issues such as radicalization risk profiling and social cohesion measurement. A scale, known as the Pressman Social Cohesion Scale (PSCS) was developed to help assess in quantitative terms attitudes of individuals on topics relevant to identity, social cohesion, integration levels, values, and attitudes on current events. Some of the items included in the PSCS are related to information and attitudes which have been assessed as being linked to radicalization and pre-radicalization.

Through its National Security Program, the RCMP has also studied the efforts of international partners in preventing youth radicalization, (i.e. London Metropolitan Police Muslim Contact Unit). This includes identifying lessons learned and best practices in dealing with radicalization. In addition, the RCMP has published a number of papers that analyze various aspects of the radicalization issue, and are aimed at both informing policy development and fostering public understanding of the issue (Royal Canadian Mounted Police 2011).

5.3 Indonesia

5.3.1 The Lib for All Foundation

The 'Lib for All Foundation' was established in 2003 by former Indonesian President Kyai Abdurrahman Wahid. The Foundation is composed of a network of individuals and organizations and is aimed at countering extremism and fundamentalism and promoting a pluralistic view of Islam (The Change Institute 2008). The Foundation is beginning to develop in other countries and continents, including South Asia, North Africa, the Middle East and Europe (The Change Institute 2008; Lib for All Foundation 2009). The Foundation includes a range of projects, "including conferences and research activities challenging the spread of - in particular - Salafi and Wahabbi Islam" (The Change Institute 2008, 131). The Foundation partakes in many activities, including:

- blocking of radical scholars in Indonesia;
- developing a counter strategy to infiltration of a Muslim organization by radical and Islamist groups through support and coordination of key individuals; and
- developing school curricula promoting tolerance (The Change Institute 2008, 131).

Although it is not known if the program has been formally evaluated, it has been noted that the high profile of the members of the foundation increase its credibility and has a great breadth of engagement (The Change Institute 2008; Lib for All Foundation 2009).

000178

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5.4 United Kingdom

A major shift has occurred in the United Kingdom's approach to counter-radicalization programs since this report was completed. As such, it is important to note that the information below reflects only a snapshot in time.

5.4.1 The CHANNEL Project.

The 'CHANNEL Project' is a diversion program run by the Home Office and is included in the UK Government's overarching CONTEST program (House of Commons Communities and Local Government Committee 2010). It is aimed at youth and other individuals who are at risk of involvement in extremism, but that do not yet require police involvement (Canadian Association of Chiefs of Police n.d.). These individuals are often identified by opinions or views they may hold (House of Commons Communities and Local Government Committee 2010). Individuals of concern are referred to the program through police, MI5, the community, and education and child welfare representatives. The cases are screened and if intervention is needed, an intervention program is created through consultations with a case planning panel and appropriate services. The program focuses on all forms of extremism (House of Commons Communities and Local Government Committee 2010). The program is being tested in 10 communities in the UK (Canadian Association of Chiefs of Police n.d.).

The House of Commons Communities and Local Government Committee (2010) report discussed above states that the project is high risk as it has the potential for creating suspicion and mistrust, because those who hold opinions that are different, but not illegal, are being reported to the police. In addition, the 'CHANNEL Project' has exacerbated much of the concern regarding spying by authorities, which was described earlier. The House of Commons Communities and Local Government Committee (2010) report states that it should be made clear that the 'CHANNEL Project' focuses on all types of extremism, rather than solely on al-Qaeda inspired extremism, and that the CHANNEL project "be removed from the CONTEST strategy and placed within the context of other crime prevention initiatives" (House of Commons Communities and Local Government Committee 2010, 55).

5.4.2 The DELPHINUS Program

The 'DELPHINUS Program' outlines the role of the police in the Prevent initiative and has been adopted throughout the UK (Canadian Association of Chiefs of Police n.d.). The program requires that the police engage with communities and authorities through relationships and programming, in an effort to counter violent extremism. The program also requires that the police have a greater understanding of counter-terrorism matters. The program impacts all levels of the UK police, including Borough Commanders and Staff Commanders (Canadian Association of Chiefs of Police n.d.).

5.4.3 Gold Groups

'Gold Groups' are networks composed of faith and community leaders, as well as other trusted individuals in the community, that are chosen by Borough Commanders in the UK (Canadian

000179

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Association of Chiefs of Police n.d.). These networks provide expert advice on issues of crisis management and are kept informed of terrorism-related incidences. By keeping these networks informed, suspicions and anxieties within the community are alleviated. It is noted that these networks are formed before a crisis occurs (Canadian Association of Chiefs of Police n.d.).

5.4.4 Islam and Citizenship Education

The 'Islam and Citizenship Education' (ICE) project was developed by the School Development Support Agency, with funding from the Department for Children, Schools and Families and the Department for Communities and Local Government (Islam and Citizenship Education 2009). The project is closely involved with several Muslim communities, which provide guidance and material to the Project. The Project is aimed at teaching citizenship values through Islamic guidance in mosque schools (madrasahs) (Islam and Citizenship Education 2009). The project involves 44 lessons which are taught in two stages: the first stage is for children who are 9 to 11 years old and the second group is targeted for youth who are 11 to 14 years old. The lessons are aimed at teaching children and youth "about Islamic tradition, values and their roles and responsibilities in society as good Muslims" (Islam and Citizenship Education 2009)[14].

5.4.5 Operation NICOLE

'Operation NICOLE' is headed by the Association of Chief Police Officers (ACPO) National Community Tensions Team (Canadian Association of Chiefs of Police n.d.). The program involves a tabletop exercise in which influential members of the Muslim community are invited to act as senior police officers who are investigating a terrorist-related activity. The program provides the police a perspective "into the impacts of counter terrorist policing, and give(s) community members an insight into the decisions that the police have to make during investigations" (Canadian Association of Chiefs of Police n.d., 12). The program provides an opportunity for debate around "core issues of law, civil rights and the nature of the response to violent extremism and has met with a great deal of initial success" (Canadian Association of Chiefs of Police n.d., 12). 'Operation NICOLE' is currently being implemented throughout the UK as a key initiative in building relationships with Muslim communities (Canadian Association of Chiefs of Police n.d.).

5.5 United States

5.5.1 The White House Office of Faith-based and Neighbourhood Partnerships

Formed in February 2009, "The White House Office of Faith-based and Neighbourhood Partnerships" works with 11 Federal centers and one strategic advisor, including the Centers of the Departments of Homeland Security, Agriculture, Commerce, etc. on faith-based and community initiatives (Dubois 2009b; The White House 2010). Each Center creates partnerships with faith-based and community organizations, while the Office acts as a coordinator between

---

[14] This program has recently been evaluated by the Institute of Community cohesion. A copy of this evaluation was requested, but was not received.

000180

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

each Center (Dubois 2009a). The Office of Faith-based and Neighbourhood Partnerships has four main goals:

- Strengthening the role of community organizations in the economic recovery;
- Reducing unintended pregnancies, supporting maternal and child health, and reducing the need for abortion;
- Promoting responsible fatherhood and strong communities; and
- Promoting interfaith dialogue and cooperation (The White House 2010).

Within the White House Office of Faith-based and Neighbourhood Partnerships is the "President's Advisory Council on Faith-based and Neighbourhood Partnerships". The President's Advisory Council includes 25 "religious and secular leaders and scholars from different backgrounds" (The White House 2009). Each member sits on the Council for a one-year term and provides recommendations on effective partnerships with faith-based and neighbourhood organizations. The President's Advisory Council has three main tasks:

- Identify best practices and successful modes of delivering social services;
- Evaluate the need for improvements in the implementation and coordination of public policies relating to faith-based organizations; and
- Making recommendations to the President and the Administration on changes in policies, programs and practices (The White House 2010).

In the 2009/2010 year, the President's Advisory Council formed six task forces, which include "reforming the Faith-Based and Community Partnerships Office, economic recovery and domestic poverty, fatherhood and healthy families, interreligious cooperation, environment and climate change and global poverty and development" (The White House 2010). The President's Advisory Council's 2010 report highlights important recommendations to the President focusing on each of the six task forces. [15]

5.5.2 Federal Bureau of Investigation

The Community Relations Unit of the FBI's Office of Public Affairs has implemented engagement efforts with American Arab, Muslim, Sikh, Somali and South Asian Communities through constructive dialogues (US Department of Justice 2010; FBI website 2010[16]). The primary goal of these engagement efforts is "to enhance public trust and confidence in the FBI by fostering the FBI's relationship with various communities by educating members of the public on how they can help protect themselves and their communities" (US Department of Justice 2010). These efforts are used in hopes of building trust between the FBI and minority groups.

---

[15] The full report can be found at http://www.whitehouse.gov/sites/default/files/microsites/ofbnp-council-final-report.pdf (Date last accessed: December 20, 2010).

[16] More information on the FBI outreach program can be found at : http://www.fbi.gov/news/testimony/strengthening-relationships-in-the-community-to-prevent-radicalization/?searchterm=community relations unit (Date last accessed: December 20, 2010); http://www.justice.gov/open/collaboration.html (Date last accessed: December 20, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5.5.3 United States Department of Justice

Similarly, the Civil Rights Division of the United States Department of Justice invites leaders from the Muslim, Arab, Sikh and South Asian communities, as well as officials from the US Department of Justice and the Equal Employment Opportunity Commission to bi-monthly meetings in which civil rights issues that have arisen since September 11, 2001 are discussed (US Department of Justice 2010). There are several different issues that have been discussed, including hate crime prosecution and profiling by law enforcement. The goal of these bi-monthly meetings is "is to bring together a wide range of federal agencies whose policies impact these communities and allow the communities to raise a range of cross-cutting issues in a single forum" (US Department of Justice 2010).

5.5.4 The Department of Homeland Security

The Department of Homeland Security Office for Civil Rights and Civil Liberties (CRCL) has implemented many outreach initiatives with members of the American Arab, Muslim, Sikh and South Asian communities in an effort to ensure that these communities are included in homeland security efforts (Department of Homeland Security 2010). The initiatives implemented by CRCL include a number of programs and events.

Roundtables

The Office for Civil Rights and Civil Liberties has implemented regular roundtables with community leaders and government officials, such as the U.S. Citizenship and Immigration Services and U.S. Immigration and Customs Enforcement. These roundtables take place in eight regions across the U.S., including Washington, D.C., Detroit, Houston, Chicago, Boston, Los Angeles, Minneapolis and Columbus, Ohio (Department of Homeland Security 2010). "The meetings provide opportunities for community leaders to learn about significant government policies, as well as to raise specific issues of concern in a format that emphasizes accountability for answers" (Department of Homeland Security 2010). There are several topics that are discussed at these roundtables, including:

- immigration and naturalization policies;
- roles and responsibilities of law enforcement;
- detention of national security suspects; and
- border searches, etc. (Department of Homeland Security 2010).

The Office for Civil Rights and Civil Liberties has also organized four youth roundtables focusing on security and liberty. These roundtables have included "150 young leaders ages 18 to 25 from the American Arab, Muslim, Sikh and South Asian communities" (Department of Homeland Security 2010). The roundtables allow government officials to engage with youth to learn about issues facing young people, and also provide the youth an opportunity to discuss these issues (Department of Homeland Security 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Incident Community Coordination Team

The Office for Civil Rights and Civil Liberties has also established the Incident Community Coordination Team (ICCT), which connects federal officials and key community leaders after a critical incident has occurred (Department of Homeland Security 2010). There are many federal agencies that are part of the ICCT team, including officials from the Office of Public Affairs, the White House Office of Public Engagement and the FBI. Community individuals that are involved include "representatives of national organizations, community leaders from key cities, and religious and cultural scholars" (Department of Homeland Security 2010).

According to the Office for Civil Rights and Civil Liberties, the Incident Community Coordination Team is effective because:

- it allows participating agencies to get community leaders the information they need in the aftermath of an incident;
- it gives community leaders a channel to speak to federal officials in a timely and effective way; and
- it facilitates development of a common understanding about the messages that the government and community leaders will send to these communities, the country, and the world (Department of Homeland Security 2010).

National Security Internship Program

In 2007, the Office for Civil Rights and Civil Liberties and the FBI established the 'National Security Internship Program', in which college students with knowledge of the Arabic language intern for the summer at the Department of Homeland Security or the FBI (Department of Homeland Security 2010). In addition, the students attend George Washington University in order to improve their Arabic language skills. If the interns are successful in their placements, they are encouraged to apply for jobs with the Department of Homeland Security or the FBI (Department of Homeland Security 2010).

Other Initiatives

The Office for Civil Rights and Civil Liberties also trains "law enforcement personnel on cultural competency relating to American Arab, Muslim, Sikh and South Asian communities, Islam and some Sikh religious practices" (Department of Homeland Security 2010). This training is used as a form of facilitating local engagement with the communities in which the law enforcement officials serve. The training is often offered on site and there is also a training DVD. The topics that are covered in this training include:

- misconceptions and stereotypes of Arab and Muslim cultures;
- diversity within Arab and Muslim communities;
- effective policing without the use of ethnic or racial profiling: and
- a best practices approach to community interaction and outreach (Department of Homeland Security 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

In addition to the above noted programs and initiatives, the Office for Civil Rights and Civil Liberties is also working towards more initiatives and engagement efforts. For example, the CRCL plans to include additional cities to the roundtable discussions over the next year. Other initiative efforts will include:

- Frequent issue-specific engagement efforts, which "bring community leaders to the table who have particular contributions to make on specific topics";
- Promoting local engagement efforts by "modeling constructive engagement; providing in-person and scalable training and training materials; coordinating community-oriented activities; and promulgating best practices"; and
- Youth engagement efforts that will empower youth to be connected (Department of Homeland Security 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

References

Audit Commission. 2008. *Preventing Violent Extremism: Learning and development exercise. Report to the Home Office and Communities and Local Government*. London, UK: Her Majesty's Inspectors of Constabulary. Last accessed February 3, 2010 from http://www.auditcommission.gov.uk/SiteCollectionDocuments/AuditCommissionReports/NationalStudies/20081110preventingviolentextremism.pdf

Azarva, J. 2009. Is U.S. detention policy in Iraq working? *Middle East Quarterly, Winter 2009*: 5-15. Last accessed March 12, 2010 from http://www.meforum.org/2040/is-us-detention-policy-in-iraq-working

Bell, S. 2009. *Toronto mosque offers 'detox' for extremists: 12-step program targets al-Qaeda sympathizers*. National Post, February 11, 2009, Page A1. Last accessed February 2, 2010 from http://www.nationalpost.com/news/story.html?id=1275285

Bettison, N. 2009. Preventing Violent Extremism: A police response. *Policing, 3*: 129.

Bin Ali, M. 2008. De-radicalisation programmes: Changing minds? S. *RSIS Commentaries*. Singapore : S. Rajaratnam School of International Studies. Last accessed December 21, 2010 from http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=92092

Birk, A.S. 2009. *Incredible dialogues: Religious dialogue as a means of counter-terrorism in Yemen. London:* The International Centre for the Study and Radicalisation and Political Violence. Last accessed February 2, 2010 from http://www.icsr.info/publications/papers/1245345445AneSkovBirkReport.pdf

Boucek, C. 2008. *Saudi Arabia's "soft" counterterrorism strategy: Prevention, rehabilitation and aftercare*. Washington, DC: Carnegie Endowment for International Peace. Last accessed February 5, 2010 from http://www.carnegieendowment.org/files/cp97_boucek_saudi_final.pdf.

Canadian Association of Chiefs of Police. n.d. *Building community resilience to violent ideologies: A discussion paper.* Ottawa, ON: Canadian Association of Chiefs of Police. Last accessed April 15, 2010 from https://www.cacp.ca/media/committees/efiles/16/422/RadicalizationEng.pdf

The Change Institute. 2008. *Study on the best practice in cooperation between authorities and civil society with a view to the prevention and response to violent radicalisation*. London, UK: The Change Institute. Last accessed February 4, 2010 from http://www.communities.gov.uk/documents/corporate/pdf/430934.pdf

000185

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Council of Australian Governments. *Council of Australian Governments' Special Meeting on Counter-Terrorism 27 September 2005*. 2008. Last accessed April 16, 2010 from http://www.coag.gov.au/coag_meeting_outcomes/2005-09-27/index.cfm#Action

Counter-Terrorism Implementation Task Force. n.d. *First report of the working group on radicalisation and extremism that lead to terrorism: Inventory of state programmes.* Last accessed March 31, 2010 from http://www.un.org/terrorism/pdfs/radicalization.pdf

Demant, F., M. Slootman, F. Buijs, and J. Tillie. 2008. *Decline and disengagement: An analysis of processes of deradicalisation*. Amsterdam: Institute for Migration and Ethnic Studies. Last accessed February 8, 2010 from http://www.imes.uva.nl/about/documents/IMESReportDeclineandDisengagement-layoutKKenFD.pdf

Department for Communities and Local Government. 2007a. *Preventing violent extremism: Community Leadership Fund*. London, UK: Department for Communities and Local Government. Last accessed February 12, 2010 from http://www.communities.gov.uk/documents/corporate/pdf/430934.pdf

Department for Communities and Local Government. 2007b. *Preventing Violent Extremism Pathfinder Fund: Guidance note for government offices and local authorities in England.* London, UK: Department for Communities and Local Government. Last accessed February 3, 2010 from http://www.merton.gov.uk/320330.pdf

Department of Homeland Security. 2010. *Testimony of Margo Schlanger, Officer for Civil Rights and Civil Liberties, before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, "Working with communities to disrupt terror plots".* Last accessed November 5, 2010 from http://www.dhs.gov/ynews/testimony/testimony_1268838948734.shtm

Department of Immigration and Citizenship. 2005. *Chapter 1: Access and equity-Review and future strategic directions.* Last accessed April 16, 2010 from http://www.immi.gov.au/about/reports/access-equity/access-equity-2005/Chapter1.pdf

Department of Immigration and Citizenship. 2009. *National Action Plan.* Last accessed April 16, 2010 from http://www.immi.gov.au/living-in-australia/a-diverse-australia/national-action-plan/nap.htm

Department of Immigration and Citizenship. 2009. *The Australian journey-Muslim communities.* Commonwealth of Australia. Last accessed April 16, 2010 from http://www.immi.gov.au/media/publications/multicultural/pdf_doc/australian-journey-muslim-communities.pdf

Dubois, J. 2009a. *Inside the Federal Centers for Faith-based and Neighborhood Partnerships*. Last accessed April 12, 2010 from http://www.whitehouse.gov/blog/2009/11/17/inside-federal-centers-faith-based-and-neighborhood-partnerships

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Dubois, J. 2009b. *The work of the office: White House Office of Faith-based and Neighborhood Partnerships*. Last accessed April 12, 2010 from http://www.whitehouse.gov/blog/2009/11/17/inside-federal-centers-faith-based-and-neighborhood-partnerships

Englund, C. 2002. *Exit Motala-Case study*. Stockholm: The Expo Foundation. Last accessed March 11, 2010 from http://www.expo.se/www/download/exit_motala_case_study_sweden.pdf

European Commission. 2008. *The EU counterradicalization strategy: Evaluating EU policies concerning causes of radicalization*. The Netherlands: European Commission. Last accessed February 4, 2010 from http://www.transnationalterrorism.eu/tekst/publications/EU%20Counterradicalization%20Strategy.pdf

Goerzig, C., and K. Al-Hashimi. 2007. *Change through debate: Egypt's counterterrosim strategy towards the Gamaa Islamia*. Paper prepared for delivery at the Sixth Pan-European Conference on International Relations, Turin September 12-15, 2007. Last accessed March 23, 2010 from http://archive.sgir.eu/uploads/Goerzig-Change%20through%20Debate%20-%20Turin.pdf

Gunaratna, R., and M. Bin Ali. 2009. De-radicalization initiatives in Egypt: A preliminary insight. *Studies in Conflict and Terrorism, 32*: 277.

Hanniman, W., and A. Smith. 2008. Radicalization and the RCMP Community Outreach Program. *The Gazette*, vol. 70, no. 1, page 38. Last accessed February 3, 2010 from http://www.rcmp-grc.gc.ca/gazette/vol70n1/emer-tend-eng.htm

Hartnub, B. n.d. *Taking responsibility: Breaking away from hate and violence*. Berlin, Germany: Violence Prevention Network. Last accessed January 14, 2010 from http://www.violence-prevention-network.de/mediathek/publikationen/189-brochure-taking-responsibility-breaking-away-from-hate-and-violence

Horgan, J., and K. Braddock. 2010. Rehabilitating the terrorists?: Challenges in assessing the effectiveness of de-radicalization programs. *Terrorism and Political Violence, 22*: 267.

House of Commons Communities and Local Government Committee. *Preventing violent extremism. Sixth report of Session 2009-10*. London: The Stationery Office Limited. Last accessed October 29, 2010 from: http://www.publications.parliament.uk/pa/cm200910/cmselect/cmcomloc/65/65.pdf

Islam and Citizenship Education Project. 2009. *About us*. Last accessed April 14, 2010 from http://www.theiceproject.sdsa.net/about-us

Islam and Citizenship Education Project. 2009. *Our aims*. Last accessed April 14, 2010 from http://www.theiceproject.sdsa.net/our-aims

000187

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Islam and Citizenship Education Project. 2009. *Welcome to the Islam and Citizenship Education Project.* Last accessed April 14, 2010 from http://www.theiceproject.sdsa.net/welcome

International Crisis Group. 2007. *"Deradicalisation" and Indonesian prisons. Asia Report Number 142*. International Crisis Group. Last accessed December 21, 2010 from http://www.healthsystem.virginia.edu/internet/ciag/142_deradicalisation_and_indonesian_prisons.pdf

Kimmel, M. 2007. Racism as adolescent male rite of passage: Ex-Nazis in Scandinavia. *Journal of Contemporary Ethnography, 35*: 202.

Korn, J. 2009. Taking responsibility: Breaking away from hate and violence. In *An introduction to social entrepreneurship: Voices, preconditions, context*, ed. R. Ziegler, 33-52. Cheltenham, UK: Edward Elgar Publishing Ltd.

Koschmieder, C. and H. Heitmann. 2009. *European Crime Prevention Award and EUCPN Best Practices Annual Conference 2009. Project entry form*. Last accessed January 4, 2011 from http://www.eucpn.org/goodpractice/showdoc.asp?docid=240

Kruglasnki, A.W., M. Gelfand, and R. Gunaratna. 2010. Detainee deradicalization: A challenge for psychological science. *Observer, 23*: 9. Last accessed March 31, 2010 from http://www.psychologicalscience.org/observer/getArticle.cfm?id=2607

Kundnani, A. 2009. Spooked! How not to prevent violent extremism. The Institute of Race Relations. London, UK. Last accessed December 23, 2010 from http://www.irr.org.uk/pdf2/spooked.pdf

Lib for All Foundation. 2009. *Programs overview.* Last accessed March 16, 2010 from http://www.libforall.org/programs.html

Marsden, S.V. 2008. *Stockwell Green Community Services and the SEED and PROSEED projects: The response of a Muslim-led organisation in addressing social exclusion, economic disadvantage and radicalisation*. London, UK. Last accessed February 5, 2010 from http://www.cepprobation.org/uploaded_files/(PRO)SEED%20report.pdf

Ministry of Refugee, Immigration and Integration Affairs. 2010. *The challenge of extremism: Examples of deradicalisation and disengagement programmes in the EU*. Ministry of Refugee, Immigration and Integration Affairs: Copenhagen, Denmark. Last accessed January 4, 2011 from http://www.nyidanmark.dk/NR/rdonlyres/20FBDF6E-43C2-43F1-A770-D908D67AC16C/0/the_challenge_of_extremisme_final.pdf

Ministry of the Interior and Kingdom Relations. 2007. *Polarisation and radicalisation action plan 2007-2011*. Amsterdam: Ministry of the Interior and Kingdom Relations. Last accessed February 4, 2010 from http://www.minbzk.nl/english/subjects/public-safety/publications/@108447/polarisation-and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Mohammed, S. 2009. To deprogram a Jihadist. *Macleans,* February 2, 2009. Last accessed February 3, 2010 from http://www2.macleans.ca/2009/02/02/to-deprogram-a-jihadist/

Montlake, S. 2007. U.S tries rehab for religious extremists: Singapore has reduced its detainee ranks with Islamic re-education. *The Christian Science Monitor*, October 9, 2007. Last accessed March 23, 2010 from http://www.csmonitor.com/2007/1009/p01s04-woap.html

Muslim Community Reference Group. 2006. *Building on social cohesion, harmony and security: An action plan by the Muslim Community Reference Group.* Last accessed April 16, 2010 from http://www.immi.gov.au/living-in-australia/a-diverse-australia/mcrg_report.pdf

National Council for Crime Prevention. 2001. *Exit: A follow-up and evaluation of the organisation for people wishing to leave racist and Nazi groups*. Stockholm, Sweden. Last accessed March 22, 2010 from http://www.bra.se/extra/measurepoint/?module_instance=4&name=0111226980.pdf&url=/dynamaster/file_archive/050120/a33854bebd54eba635246e34050ea1a0/0111226980.pdf

Neumann, P.R. 2010. *Prisons and terrorism: Radicalisation and de-radicalisation in 15 countries*. The International Centre for the Study of Radicalisation and Political Violence. Last accessed October 26, 2010 from: http://www.icsr.info/publications/papers/1277699166PrisonsandTerrorismRadicalisationandDeradicalisationin15Countries.pdf

Porges, M.L. 2010a. Deradicalisation, the Yemeni way. *Survival, 52*: 27.

Porges, M.L. 2010b. *The Saudi deradicalization experiment*. New York: Council on Foreign Relations Expert Brief, January 22, 2010. Last accessed February 5, 2010 from http://www.cfr.org/publication/21292/saudi_deradicalization_experiment.html

Pressman, E. 2009. *Risk assessment decisions for violent political extremism*. Ottawa, ON: Carleton University. Last accessed February 2, 2010 from http://www.publicsafety.gc.ca/res/cor/rep/_fl/2009-02-rdv-eng.pdf

Public Safety Canada. *Terms of reference*. Last accessed April 4, 2010 from http://www.publicsafety.gc.ca/prg/ns/ccrs/ccrstor-eng.aspx

Religious Rehabilitation Group. 2010. *A glimpse of RRG: Reality and experience*. Last accessed March 30, 2010 from http://www.rrg.sg/edisi/data/trans.pdf

Simpson, T. 2007. *Government failing Muslim communities*. Voice Online, July 31, 2007. Last accessed February 5, 2010 from http://www.voice-online.co.uk/content.php?show=11722

Spalek, B., and A. Imtoual. 2007. Muslim communities and counter-terror responses: "Hard" approaches to community engagement in the UK and Australia. *Journal of Muslim Minority Affairs, 27*: 185.

000189

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Spiegel Online. 2010. *Germany to launch Exit Program for Militant Islamists*. Last accessed December 23, 2010 from http://www.spiegel.de/international/germany/0,1518,702103,00.html

Stevens, D. 2009. In Extremis: A self-defeating element in the 'Preventing Violent Extremism' strategy. *The Political Quarterly, 80*: 517.

Thomas, P. 2009. Between two stools? The government's 'Preventing Violent Extremism' agenda. *The Political Quarterly*, 20: 282.

Thomas, P. 2010. Failed and friendless: The UK's 'Preventing Violent Extremism' programme. *The British Journal of Politics and International Relations, 12*: 442.

United States Department of Justice. 2010. *Collaboration*. Last accessed November 5, 2010 from http://www.justice.gov/open/collaboration.html

Wilner, A. 2010. From rehabilitation to recruitment: Stopping the spread of terrorist doctrines within our prisons before it becomes a national security problem. *True North in Canadian Public Policy.* The MacDonald-Laurier Institute for Public Policy. Last accessed October 28, 2010 from http://www.macdonaldlaurier.ca/files/pdf/FromRehabilitationToRecruitment.pdf

The White House. 2009. *Obama announces White House Office of Faith-based and Neighborhood Partnerships*. Last accessed April 12, 2010 from http://www.whitehouse.gov/the_press_office/ObamaAnnouncesWhiteHouseOfficeofFaith-basedandNeighborhoodPartnerships/

The White House. 2010. *About the President's Advisory Council on Faith-based and Neighborhood Partnerships.* Last accessed April 12, 2010 from http://www.whitehouse.gov/administration/eop/ofbnp/about/council

The White House. 2010. *Policy goals: Key priorities for Faith-based and Neighborhood Partnerships.* Last accessed April 12, 2010 from http://www.whitehouse.gov/administration/eop/ofbnp/policy

The White House. 2010. *About the Office of Faith-based and Neighborhood Partnerships.* Last accessed April 12, 2010 from http://www.whitehouse.gov/administration/eop/ofbnp/about

000190

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Citizen Engagement in National Security Issues

A Five Country Review

Compiled by: Sara Guay

November 2010

This report provides a snapshot of citizen engagement programs at the time that this report was created. Major developments in the United Kingdom have already occurred since the completion of this report.

This report is a work product, and the findings presented herein are not to be construed as an official Department of Justice Canada position, unless they are designated as such by other authorized documents and the report is posted on the official Department of Justice Canada Web site.

000191

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Table of Contents

Abstract 5
Executive Summary 6
1.0 Introduction 18
1.1 Objective of this study 18
1.2 Research Questions 18
1.3 Structure of this Research Paper 19
1.4 Methodology 19
2.0 Background/Concepts Section 20
2.1 What is Citizen Engagement? 20
2.2 What are the Benefits of Engaging Citizens? 20
2.3 What Groups of Citizens are Typically Targeted by Engagement Initiatives? 21
2.4 What are the Different ways in which Citizens can be Engaged? 22
2.5 Communication Methods in the 21st century 22
3.0 Citizen Engagement in National Security Issues in the United States 25
3.1 The History of National Security Strategies in the United States 25
3.2 Frequency of issuance over time 25
3.3 National Security Strategies in the Post September 11th Era and the Reviews Thereof 26
3.4 Reviews conducted by the Department of Defence 34
3.5 Reviews conducted by the Department of Homeland Security 35
3.6 National Information Sharing Strategies 35
3.7 Outreach Programs by Type 39
3.7.1 National Security Initiatives – General 39
3.7.2 Defence-Related Initiatives 42
3.7.3 Intelligence Initiatives 43
3.7.4 Justice Related Initiatives 44
3.7.5 Science and Technology Initiatives 45
3.7.6 Critical Infrastructure Initiatives 46
3.7.7 Cyber Security Initiatives 49
3.7.8 Border Protection Initiatives 52
3.7.9 Maritime Security Initiatives 53
3.7.10 Aviation Security Initiatives 54
3.7.11 Community Outreach Initiatives 54
3.7.12 Police Based Programs 56
3.7.13 Emergency Planning Initiatives 56
3.7.14 International Outreach 56
3.7.15 Transparency and Open Government Initiative 57
4.0 Citizen Engagement in National Security Issues in Australia 58
4.1 The History of National Security Strategies in Australia 58
4.2 National Information Sharing Strategy 64
4.3 Outreach Programs by Type 65
4.3.1 National Security Initiatives - General 65
4.3.2 Defence-Related Initiatives 66
4.3.3 Science and Technology Initiatives 67

000192

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

4.3.4 Critical Infrastructure Initiatives 67
4.3.5 Cyber Security Initiatives 70
4.3.6 Community Outreach Initiatives 70
4.3.7 Aviation Security Initiatives 72
4.3.8 Chemical Security Initiatives 72
4.3.9 Emergency Management Initiatives 73
5.0 The Influence of the European Union on Member States 75
6.0 Citizen Engagement into National Security Issues in the United Kingdom 78
6.1 The History of National Security Strategies in the United Kingdom 78
6.2 National Information Sharing Strategy 87
6.3 Outreach Programs by Type: 88
6.3.1 National Security Initiatives - General 88
6.3.2 Defence-Related Initiatives 88
6.3.2 Science and Technology Initiatives 89
6.3.3 Critical Infrastructure Initiatives 89
6.3.4 Cyber Security Initiatives 90
6.3.5 Community Outreach Initiatives 90
6.3.6 Police Based Programs 91
7.0 Citizen Engagement in National Security Issues in the Netherlands 93
7.1 History of National Security Strategies in the Netherlands 93
7.2 National Information Strategy 104
7.3 Outreach Programs by Type 104
7.3.1 National Security Programs - General 104
7.3.2 Aviation Security Initiatives 106
8.0 Citizen Engagement in National Security Issues in France 107
8.1 History of National Security Strategies 107
8.2 Outreach to Groups – by Type 110
8.2.1 National Security - General 110
8.2.2 Defence-Related Initiatives 111
8.2.3 Science and Technology Initiatives 111
8.2.4 Cyber Security Initiatives 111
9.0 Best Practices and Lessons Learned 112
9.1 How to Determine the Appropriate Level of Engagement 112
9.2 Recommended Strategies Based on Desired Level of Engagement 113
9.3 Advantages and Disadvantages of the Different Methods 114
9.4 Citizen Engagement Checklist 115
9.5 Best Practices in Community Engagement 118
9.6 Clues to Good Community Engagement 119
9.7 What works in Community Cohesion – A Review of Six Case Studies 121
10.0 Lessons Learned From Previous Evaluations – by Topic 123
10.1 Use of the Internet in Engaging Citizens 123
10.2 Private Industry's Role in Maritime Security 123
10.3 Private Industry's Role in Aviation Cargo Security 124
10.4 Ensuring Safety of Imported Products at the Source 124
10.5 Best Practices in Managing Risks to Critical Infrastructure 124

000193

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

10.6 Findings of Evaluations of Community Outreach Initiatives in the United States 125
10.7 Evaluations of Community Outreach initiatives in the United Kingdom..... 127
A major shift has occurred in the United Kingdom's approach to citizen engagement programs since this report was completed. As such, it is important to note that the information below reflects only a snapshot in time. 127
10.8 Effectiveness of Information Sharing Strategies 129
10.9 Evaluations of HSIN's - Public Transit Security Information..... 131
10.10 Best Practices in Emergency Planning 132
10.11 Unifying the National Effort to Combat Home-grown Jihadist Terrorism..... 132
11.0 Conclusions..... 134
Appendix A: Abbreviations 136
Appendix B: Definitions..... 142
References:..... 148

000194

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Abstract

This study provides an overview of the methods and strategies which have been implemented in a select group of countries namely: the United States, the United Kingdom, Australia, the Netherlands and France in order to engage citizens in issues related to National Security. Some discussion regarding the initiatives of the European Union has also been included due to the fact that three of the countries examined are member states. This research paper will begin by defining the main concepts, and the purpose of engaging citizens. This will be followed by a brief synopsis of the strategies, speeches or documentation which have been released to date in the pursuit of this goal along with any information strategies which are aimed a facilitating the free exchange of information between the governments of these countries and their citizenry and/or private sector. Thirdly, it will provide a brief description of the programs and initiatives which have been implemented in order to either: inform, consult with or encourage active participation with either the society at large or specific groups of individuals or organizations. And finally, this study will conclude with an overview of the 'lessons learned' or 'best practices' which have been developed as a result of a review of existing programs in order to provide guidance in the development of future programs. This report provides a snapshot of citizen engagement programs at the time that this report was created. Major developments in the United Kingdom have already occurred since the completion of this report.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Executive Summary

This report provides a snapshot of citizen engagement programs at the time that this report was created. Major developments in the United Kingdom have already occurred since the completion of this report.

Citizen engagement in the creation or evaluation of public policy is not a new concept. In fact, we find its origins in Ancient Greece at the very beginning stages of *demokratia* or democracy, and while the level of engagement, particularly in issues related to 'National Security' has fluctuated over time, engaging citizens has always been seen as an important and valuable part of a successful democracy. Therefore, the objective of this research paper was to examine how a select group of countries, namely: the United States, the United Kingdom, Australia, the Netherlands and France; have engaged their citizens in issues related to National Security.

However, it became clear, while researching this paper that this form of engagement has been increasing in recent years, particularly since the terrorist attacks of September 11th, 2001, not just in the United States, but in almost all countries which were examined. The reason for this shift seems to be that these attacks, among others, have brought to light the fact that the terrorist organizations of late have evolved from using traditional weapons of mass destruction to also employing a multitude of different methods in order to attack, and consequently, there are exponentially more dangers in the 21st century, then ever before.

This knowledge has lead to governments to examine in new potential vulnerabilities and to develop action plans in order to address them. The most recent of which is the identification that threats may exist from a Cyberspace perspective to sectors of the economy which have been deemed part of the countries 'Critical Infrastructure'. The realization has prompted many governments to begin to collaborate with the private sector since the majority of the companies within these sectors are private owned; and technology, particularly with respect to weaponry and Cyberspace is advancing at an alarming rate, therefore it became more important than ever before to collaborate with industry in order to remain abreast of the latest technologies in these areas.

In addition to the above, the Internet has provided more opportunities for terrorist organizations to recruit new members and to raise financial support from individuals all over the world without leaving their 'safe houses". This fact has prompted many levels of government within these countries to develop programs and initiatives in order to inform the general public of 'warning signs' and have established 'Hot-lines' to give citizens an opportunity to report suspicious behaviour. It has also prompted the governments of many countries to establish outreach programs and initiatives aimed at providing citizens a positive method of voicing their 'grievances' with the appropriate level of government so that action can be taken to resolve these issues before they escalate to violence.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Finally, the Internet has also led to a new World which is inter-connected, both internally and internationally. This fact has mandated the need for international collaboration in order to resolve issues which transcend borders.

It is these main factors which have lead governments to collaborate or engage with many different groups of citizens including: leading academics; industry leaders; community leaders; other nations as well as the general public at large; in the interest of preserving National Security. Through these collaborations, governments can achieve the following (among others):

- Information in regard to the latest, most cutting research and technology which can be used to defend or attack a nation;
- To identify the potential risks which currently exist, and develop an action plan to address them;
- To diminish the duplication of efforts;
- To develop strategies which address issues or threats which require international agreement;
- To work with individuals or organizations to revolve grievances; and
- To identify and apprehend terrorists before they strike.

It is for these reasons that citizen engagement has become an important part of *National Security Strategies* in the modern world.

Below you will find an overview of the strategies and programs which have been identified to date in the aforementioned countries and some insight into the 'best practices' or 'lessons learned which have been established to date.

Engagement with Citizens by the United States Government

National Security Strategies in the United States began under the authority of the *National Security Act of 1947 (NSA).* This act laid the foundations for the creation of the National Security Council and the Central Intelligence Agency, but with the issuance of the *Goldwater-Nicols Department of Defence Reorganization Act of 1986*, came the requirement to produce a National Strategy on an annual basis.

From 1986 to 2001, the Administrations of the US government did not always deliver a Strategy annually; however, they were delivered frequently. However, since 9/11, there have been more than 30 National Security Strategies which have been both created and disseminated to the general pubic. Some of these strategies have been broadly based, such as the *National Security Strategy* of 2002 and 2006, and the *National Strategy for Homeland Security* which was released in 2002 and 2007. However, many others have been released over the last 9 years in order to address specific issues in greater detail such as: the *National Strategy to Combat Terrorism*; the *National Strategy for the Protection of Critical Infrastructure and Key Assets* and the *National Strategy to Secure Cyberspace*.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

In addition to the release of these National Security Strategies, the US government has also developed several National Information Strategies aimed at creating a more collaborative environment between government departments as well as with the private sector in order to change the previously held view that information should only be shared on a "need to know" basis, to one which takes the view that government institutions have a "responsibility to share" wherever possible. The Information Sharing strategies which were developed in order to facilitate this shift in thinking include, but are not limited to, the following: the *Information Sharing Environment Plan*; the *National Strategy for Information Sharing; the Defence Information Strategy*; *Intelligence Community Information Sharing Strategy* and most recently, the *National Framework for Strategic Communication of 2010.*

While the United States government has always been committed to outreach to its citizens, and has had programs in place such as the National Academy of Science, which was established more than a century ago and the Joint Civilian Orientation Conference which has been in place for more than 60 years; it cannot be denied that the amount of programs and initiatives have snowballed since September 11th. An enormous amount of outreach with science and technology professionals; as well as academics and owners and operators of business which fall under the heading of 'Critical Infrastructure' are currently in existence and are managed by the Department of Homeland Security which was created in response to the release of the National Security Strategy of 2002. However, many other programs have also been created which have included outreach to address with other specific issues related to the protection of National Security from an air, maritime, border, space and cyberspace perspectives and well as protection against chemical and biological warfare and weapons of mass destruction.

In December of 2009, President Obama extended this level of outreach with the launch of the *Transparency and Open Government Initiative.* Under the authority of the *Open Government Directive*, President Obama called on all Departments to "re-evaluate their programs to find new ways to increase their transparency and accessibility". Through this initiative, the US government has established the open.gov and data.gov web-sites in order to facilitate and give greater ability for citizens to voice their opinions and access to existing data. In addition, the General Services Association set-up 22 web-sites, each for a separate government department (including the departments of: Homeland Security; Defence and Justice), in order to obtain the feedback of citizens in the development of their Open Government Plans. All these Open Government Plans were submitted as of April 7th, 2010 and are available through the Open Government Dashboard, which is a web-site that tracks the compliance of each government department with the Open Government Initiative. Under this initiative there have also been an array of other blogs and social media accounts set-up in order to facilitate a greater exchange of ideas however, the most interesting of these, from a National Security perspective, was the creation of the National Security Dialogues. These Dialogues were set-up to obtain feedback from the general public on 6 main issues related to National Security which were grouped as follows: Counterterrorism and Domestic Security Management; Border Security; Enforcement of Immigration Laws; Preparing for and responding to disasters; the Homeland Security National Risk Assessment and Homeland Security Planning and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Capabilities. Once the preliminary discussion of these topics were completed, they were followed by a more in-depth discussion into how best to prioritize and achieve the identified goals, and finally the final products were also submitted for review and feedback.

Engagement with Citizens by the Australian Government

In Australia, the release of documents related to National Security began with the release of the *Defence and Industry Strategic Policy Statement* in June of 1998, and since the turn of the century, it has released Defence White Papers almost biannually. In 2005, following the terrorist attacks in London, the then Prime Minister met with the leaders of Muslim communities to develop a 'Statement of Principles' which was later used to develop a *National Action Plan* to combat violent extremism; and in 2006, the first White Paper which dealt specifically with terrorism and acknowledged the importance of engaging citizens, *Protecting Australia from Terrorism*, was released.

Following this, in 2007, two more documents were released, the first was an information package for businesses to help them prepare for, prevent and recover from a range of hazards including terrorism; and the second was the *Attorney General's Security Environment Update*. However, the first official *National Security Statement* which was ever released in Australia was in December of 2008. Since then, the Australian government has released a great deal of documents related to National Security which include the following: *Securing Cyberspace,* the *National Security Science and Innovation Strategy, Changes to the Critical Infrastructure Protection Program, the Lexicon of Terrorism* and the first ever *National Aviation Policy* Statement. In 2009, the Australian government also launched an Information Strategy aimed at changing the mindset of government officials to one which is conducive to sharing so that information could be shared more freely with the private sector. The most recent release was a Counter-terrorism a document entitled: *Securing Australia: Protecting Our Community*, which was announced on February 23rd, 2010.

Over this same time period, a great many programs and initiatives have been put into place in order to outreach with the private sector and groups and inform the general population in the interest of protecting National Security. Initiatives such as: *the National Security Public Information Campaign, National Security Hotline* and the *Let's Look Out for Australia* advertising campaign were launched and were intended to raise awareness of the terrorism and to encourage the general population to get involved and report suspicious or questionable behaviour, as well programs such as: *the Chemical Security Management Framework, the Critical Infrastructure Program, CERT Australia, the Business Government Advisory Group* and the *Aviation Security Advisory Forum,* all aimed at working with business to identify and prevent against terrorist attacks.

The Influence of the European Union on Member States

Following the terrorist attacks in Madrid, the European Council began to examine the interdependencies of Member States in terms of 'Critical Infrastructure' and called on

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Members States to develop action plans to protect Critical Infrastructure not only within their borders but also in terms of 'European Infrastructure', i.e. threats which involve at least one other member of the European Union. Since this Declaration was made by the Council in March of 2004, all Member States have participated in the development of several initiatives aimed at protecting European Infrastructure. Information regarding these programs has been included in this research paper since the United Kingdom, France and the Netherlands are part of the European Union and therefore, participated in these programs and launched their own initiatives as a result.

Engagement of Citizens by the British Government

A major shift has occurred in the United Kingdom's approach to citizen engagement programs since this report was completed. As such, it is important to note that the information below reflects only a snapshot in time.

Since the development of the CONTEST Strategy in 2003, which was updated in 2009, the United Kingdom has been involving their citizens in issues related to National Security. The CONTEST Strategy, which was designed to be a long-term Strategy aimed at countering international terrorism, is organized around four pillars: Pursue (to stop terrorist attacks); Prevent (to stop people from becoming terrorists); to Protect (to strengthen protection against terrorist attacks) and Prepare (to mitigate the impact when the attack can not be stopped). The UK government conducts outreach with private sector in pursuing all of the above objectives. This Strategy was updated in 2009. Other documents related to this Strategy which have been released include the documents: *Preventing Violent Extremism: A Strategy for Delivery and Security, Prevent: A Communications Guide, Working Together to Protect Crowded Places, and the Safer Places: A Counter Terrorism Supplement.*

In addition to the CONTEST Strategy, the UK government released its first ever *National Security Strategy* in March of 2008, entitled Security in an Interdependent world. This Strategy was updated in 2009 and a progress report on this updated Strategy was released in March of 2010. Other strategies which have been released since including the documents: *Eliminating World Poverty: Building a Common Future* (more efforts to decrease the drivers of terrorism in fragile states); *The Road to 2010* (enhancing nuclear security measures); the U*K's Science and Technology Strategy for Countering International Terrorism*; the *Cyber Security Strategy* and finally the Defence Green Paper entitled *Adaptability and Partnership.*

Under the guidance of the CONTEST Strategy and in accordance with these National Security Strategies, there have been a great deal of programs which have been created in order to combat violent extremism and outreach with industry. Some examples of outreach to groups include: *The National Security Forum, the Critical Infrastructure Resilience Program, CERT* and also the *National Risk Registe*r. The programs which have been developed in order to combat violent extremism include: the Neighbourhood Policing project; Building Networks; the Channel Programs; the DELPHINUS Program; Operation Nicole and the Islam and Citizenship Education program, to name a few.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Engagement of Citizens by the Dutch Government*

The first National Security Strategy in the Netherlands was released in 2007; however, other documents related to National Security begin around the turn of the century. However, after the September 11th attacks, the Dutch has undertaken a great deal of research into understanding the phenomenon of extremism. These documents have been made publicly available for information purposes primarily on the Ministry of the Interior and Kingdom Relations and the National Coordinator for Counterterrorism web-site. Like many of the other governments examined in this report, the Dutch government has also developed an *Information Strategy* aimed at improving the dissemination of information among safety partners. As with the United Kingdom, the Dutch government has instituted several programs which include working with owners and operators of Critical Infrastructure, and other programs such as: *the Netherlands against Terrorism Campaign* and *The Hague against Terrorism*.

Engagement of Citizens by the French Government*

The first *National Defence White Paper* was issued by the French government in 1972. Since then, two other White Papers have been released, one in 1994 and most recently in 2008 at which time a Press Kit was also issued in order to provide an explanation of the key concepts in 'layman's terms'. In addition to these White Papers, the French government has released a few other documents which are related to National Security, these include the *Vigipirate Renforcé Plan*, which was drafted in response to the events of September 11th, and was a two-phased plan aimed at protecting Critical Infrastructure. The French government also issued a *Biotox Plan* in 2001, which provided a foundation for collaboration between the French government and civilian agencies in protecting France from biological threats of all kinds; the *Military Programme Bill of Law 2003-2008*, laid the framework for French Defence Policy for the years 2003 to 2008; and finally the *Non-Proliferation Policy* speech which was given in March 2008 which encouraged disarmament of all biological and chemical weapons. In the way of programs, the French government has instituted several programs in order to engage with citizens or groups into issues of National Security. These groups include: *The White Paper Commission* which included members of academia and think tanks as well as solicited feedback from the general public in the drafting of the *Defence White Paper* of 2008. Also several advisory and cooperative councils have been established to deal with issues of National Security which include: the *Advisory Board of Defence and National Security; the Economic and Scientific Security Council, the Civil-Military Cooperation in Defence of France*, and the *Security of Information Security Agency*.

Best Practices in Creating a Community Engagement Program

Through the evaluation of some existing programs, some documentation has been produced primarily by the UK and Australian governments. Through these evaluations, the following have been identified as the key elements of developing an effective Strategy:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Identifying the key stakeholders;
- Using the SMART test;
- Understanding your audience;
- Ensuring that your messages are clear and consistent;
- Ensuring that the language that is used in communicating with your audience is communicated correctly and is sensitive to your audience;
- Ensuring that the spokesperson which is chosen has good knowledge of the subject area, is appropriately dressed, and has a good track record of dealing with the community;
- Projects aimed at young people are seen as key;
- Taking a bottoms-up approach;
- Maximize the role of voluntary and community groups; and
- Ensuring long-term funding is essential.

In addition, the Queensland government in Australia developed a checklist for community engagement in policy making, which identified the following major steps: Identify the issue, the participants, the decision making and approval process, decide of the level of engagement, choose the engagement method and technique, maximize the ability of stakeholders to participate, create a method of quality control, estimate the necessary resources, formulate a timetable, implement Strategy which is based on recommendations of the group, provide an opportunity for participants to give feedback and evaluate the engagement process.

Lessons Learned:

In terms of "Lessons Learned", there have several reviews which have been conducted to date into existing programs, in particular, in the United States and the United Kingdom through which much can be applied to existing programs in other countries as well as is in the development of new programs and initiatives. These findings include the following:

- **Use of the Internet:** In the 21st century, the Internet is the most common vehicle for communication because it is the least expensive option. However, since the Internet not available to everyone, governments will need to employ a combination of the strategies in order to inform the entire population if this is the desired effect. Also, using the Internet can present risks to the security of the information held on these sites and therefore, careful review and management of these tools is required by individuals who have the necessary skills and expertise in order to ensure these tools remain productive and do not present a security risk.

- **Private Industry's Role in Airline and Maritime Security:** The recent discovery of explosives in the cargo hold of an airplane bound for Chicago, has drawn attention to the need for tighter security measures in regard to cargo, aboard airplanes and also cargo ships. Recent evaluations of the scope of the issue and current programs which are in place, have determined that due to the shear volume of packages shipped annually, that collaboration between the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

government and the private sector stakeholders is in fact a necessity, since neither entity would be capable of managing the security of this volume of packages alone. Therefore, while existing programs have achieved a certain level of success, compliance is voluntary at present which has meant that the level of security, to date, has fallen short of the original targets. Therefore, experts recommend that these security measures be legislatively mandated in order to ensure compliance.

- **Ensuring Safety of Imported Products at the Source:** Since threats to food supply has been identified as a component of 'Critical Infrastructure' the United States government has taken steps to prevent issues at the source, by establishing offices overseas in order to provide training, answer questions and provide other assistance in order to help them foreign companies adapt their systems and in order to improve compliance with FDA regulations..

- **Community Outreach to Minority Groups:** Evaluations have been conducted into existing programs aimed at outreach to particular segments of the population in both the United States and the United Kingdom, both resulted in similar findings.

  Evaluation of US based policing programs

  This study was conducted by the US Department of Justice and consisted of a review of the police-based outreach programs with Arab-American communities currently in place in the US. This evaluation found four key obstacles hindering outreach between U.S. Arabs (Christian and Muslim) and law enforcement:

  - "Distrust between Arab communities and law enforcement;
  - Lack of cultural awareness among law enforcement officers;
  - Language barriers; and
  - Concerns about immigration status and fears of deportation."

  Terrorism expert Marc Sageman cautions 'that engagement can be perceived as a government focus on Muslim communities and he suggests that 'an important role at the federal level is to lead efforts to combat discrimination against Muslim-Americans'. Mohamed Elibiary the President of the *Freedom and Justice Foundation*, a Muslim community group based in Carrollton, Texas also expressed the view that: 'outreach may be most effective when U.S. Muslim communities initiate it and community government contact revolves around countering the extremist messages popular among home-grown violent jihadists.'

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Findings of the UK House of Commons' Communities and Local Government Committee re: The Prevent Program

Similar concerns were voiced in the extensive review which was conducted by the UK House of Commons' Communities and Local Government Committee's into the *Prevent* program. The main findings of this Committee were as follows:

- Some witnesses felt that these programs were solely associated with counter-terrorism efforts and therefore intended for surveillance purposes;
- Many witnesses reported that programs which focused on neo-jihadist terrorism has led to a feeling of stigmatization and a sense of alienation among Muslim communities;
- Also, as a consequence of the focus being placed on Muslim communities, this has led to feelings of resentment in non-Muslim communities due to perceived 'favouritism';
- Identified a need for clearer program objectives in order to allow for more effective evaluations to be conducted; and
- As a result of these findings, many questioned the role of Department of Communities and Local Government as the led for this program, since this department is mandated with promoting cohesiveness, and many of the witnesses believed that *Prevent* has undermined cohesiveness in the communities.

Recommendations Made by the UK House of Commons' Communities and Local Government Committee

Other recommendations made by the Committee include:

- The Committee felt there may be too much emphasis on the theological basis of extremism and more attention may need to be placed on other factors, such as politics, policy and socio-economics, which may play an even greater role in the process of radicalisation;
- The Committee also suggested that the Government should take into account current research on the risk factors for radicalisation and update CONTEST to reflect the fact that there are other factors, beyond theological causes, that are associated with radicalisation;
- The Government should continue to prioritize investment into alleviating socio-economic deprivation;
- Universities and prisons be included in risk assessments and that work with these institutions be better co-ordinated with the Prevent program;
- The Government should provide more opportunities for empowerment and civic engagement to strengthen the engagement of all excluded groups and felt that some of funding for Prevent should be allocated towards "encouraging participation in democratic means of debate";
- That the Government seek the advice of independent academics and the Muslim community in the development of strategies to provide a counter-narrative to extremist views and in the development of new programs; and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- That more cultural awareness training and support be provided to front-line workers, including police and teachers.

Effectiveness of Information Sharing Strategies: In the past, information flow between critical infrastructure stakeholders has been restrained, or nonexistent, for at least three reasons: 'a natural bureaucratic reluctance to share information, technological difficulties associated with compatibility, and legal restraints to prevent the misuse of information for unintended purposes'. However, in the wake of September 11, many information strategies were drafted in order to mandate the sharing of information across government and Fusion centers were set-up across the US to facilitate the exchange of this information. These Information sharing arrangements were evaluated by the GAO and they came to the following conclusions:

- It is unclear how open the private sector and the government have been in sharing information;
- The private sector primarily wants from government information on specific threats which the government may want to protect in order not to compromise sources or investigations;
- Much of the threat assessment done by the federal government is considered classified and therefore cannot be shared; and
- The private sector, too, is concerned about whether providing this information might lead to future regulatory action or other liabilities.

Therefore, successful information sharing will depend on the ability of each side to demonstrate it can hold in confidence the information exchanged. In addition, the degree to which some of the activities are mandated varies across sectors. For example, Nuclear power plants must meet very specific standards for assessing their vulnerabilities while sectors such as information and telecommunication, oil and gas, and commercial, sharing is encouraged but not mandated, which is an issue which could be examined by governments in the future.

- **Evaluations of HSIN's - Public Transit Security Information:** A survey conducted by the GAO identified several duplications were occurring in the exchange of information form source agencies, and therefore, a need to streamline the information which was provided to stakeholders. The GAO also found that a greater proportion midsize agencies, non-rail industries who were unaware of this information. As a result, Federal and industry officials formed a working group to assess the effectiveness of the information-sharing mechanisms, including developing options to streamline current strategies.

- **Best Practices in Emergency Planning**: FEMA has developed standards that call for validation, review, and testing of emergency operation plans, because their evaluation have concluded that this offers the best way to determine if such plans are understood and work. FEMA also recommends that officials use functional and full-scale emergency management exercises to evaluate plans. Also

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

regularly scheduled drills, exercises and follow-up activities are critical components of emergency planning.

- **National Effort to Combat Home-grown Jihadist Terrorism;** Many experts believe that combating violent extremism must include efforts to counter extremist narratives. Governments therefore, may wish to consider creating a mandate a Strategy of this kind as well, because according to the Government Accountability Office (GAO) of the United States, "A clearly-articulated national strategy or framework can prioritize activities, assign responsibility for specific tasks among departments and agencies at the Federal level, and harmonize efforts to manage tension and eliminate duplication of efforts".

Conclusions:

This paper has shown that the Strategy of engaging citizens in National Security has been implemented by all of the countries we examined to some degree. Common threads which have been identified between the countries which we have examined from the Western World include the following:

- A broader definition of the concept of 'National Security' has been adopted;
- Sharing of information is quintessential in preventing attacks on 'critical infrastructure' due to the fact that 85% of these companies are privately owned, and their high rate of interdependence, an attack on one company could cause a chain reaction, having a much larger, even catastrophic effect if an attack were to occur;
- *National Information Strategies* have been created in order to facilitate the free exchange of information to the extent that this exchange does not compromise National Security[1];
- Governments have engaged citizens in the protection of National Security in order to prepare for and prevent attacks from occurring and also to mitigate the effects should an attack occur. They have achieved these goals in the following ways:
    - By collaborating with industry and academics to identify potential risks to Critical Infrastructure and the development and implementation of action plans to mitigate these risks;
    - By collaborating with industry experts particularly in the fields of cyberspace and defence technology to identify and mitigate risks from new technologies;
    - By collaborating with first responders at the regional level in order to identify risks at the regional level so that these can be addressed by a National Action Plans and Strategies

[1] An information sharing strategy could not be located for France at this time but this may simply be due to insufficient search terms being used due to language barrier.

000206

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- By implementing outreach programs for members of marginalized communities in the hopes of identifying and de-radicalizing members of the community who are at risk of resorting to extremism;
- By working with other countries on an international level to identify and mitigate risks which cross borders and require international collaboration; and finally,
- By informing and outreaching to the general public in order to raise awareness of and identify potential threats as they emerge to avoid a terrorist act coming into fruition.

There are lessons to be learned from evaluations which have been conducted into existing programs, including the following:

- Proper evaluations of potential threats and vulnerabilities is necessary for preparedness planning;
- Tests of emergency systems should be conducted periodically to identify and address weaknesses;
- Information as to potential threats as well as the tools and information necessary to prevent attacks are a necessary component of a National Security Strategy in the 21st century and as such, governments, may need to consider drafting legislation to mandate compliance of businesses to recommended security measures and sharing of information in order to ensure the free exchange of information and that security measures are universally employed;
- Governments should consider drafting a National Security Strategy to Combat Extremist Narratives; and
- Governments should continue to collaborate with minority groups however, it may be best if these initiatives are led by grassroots community organizations in order to avoid the perception of favouring or conversely scrutinizing a segment of the population.

It is in these ways that these governments have achieved and will continue to achieve, National Security goals in the 21st century.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

1.0 Introduction

The idea of engaging citizens in the governance of the country, is not a new concept, in fact we find its foundations in Ancient Greece in order to ensure a well-rounded society (www.historyguide.org).

In the modern world, engaging citizens has grown to become viewed as a quintessential to the protection of National Security, and consequently, many countries have made great strides as of late in engaging their citizens in multitude of different ways and to varying degrees.

1.1 Objective of this study

The goal of this research paper is to provide an overview of citizen engagement initiatives and strategies which have been put into place in the following countries: United States, the United Kingdom, Australia, France and the Netherlands aimed at engaging citizens in national issues. Through this research, we will attempt to provide answers to the research questions listed below.

1.2 Research Questions

The research questions which are examined through this paper are as follows:

1) What efforts have been taken by the United States, the United Kingdom, Australia, France and the Netherlands to engage their citizenry on National Security issues, including minority groups who may feel targeted by the respective countries' anti-terrorism legislation? These efforts include (a) initiatives/programs/projects to outreach to communities on National Security; and (b) efforts by these countries to engage its citizens on issues of National Security by publishing discussion papers on possible legislative public consultations and the publication of a National Security statement.

2) Are these projects/programs/initiatives part of an over-arching community engagement Strategy on National Security issues? If such a Strategy exists, what is the policy?

3) What levels of government or government departments are involved? Who are the members of the community who are involved (i.e. community leaders, business owners)?

4) How long have these projects/programs/initiatives been in existence?

5) What is the purpose or mandate of the projects/programs/initiatives?

6) Has this project/program/initiative been evaluated? Is so, what are the results and "lessons learned"?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

7) Have other governments or agencies developed "best practices" strategies in regard to the establishment of these types of associations or projects/programs/initiatives? And if so, what are these best practices?

1.3 Structure of this Research Paper

In order to answer these questions, this paper will begin by providing an overview of the different forms of citizen engagement and the methods which can be used in order to achieve each of these types. This will be followed by a country by country overview of how this select group of countries have employed these strategies for the purpose of engage their citizens in National Security issues. Finally, this paper will provide some guidance as to the best forms of engagement to use based on the desired level of engagement and the outcome of previous evaluations which have been conducted into existing programs. These recommendations are included to provide guidance to be used in the development of future initiatives.

1.4 Methodology

The research, programs and strategies which have been included in this paper were found using such sources as: the web-sites of the Federal government departments charged with the responsibility of protecting National Security for the above mentioned countries; the Federal government departments with the responsibility to review and audit existing programs; searches of non-government organizations and strategic think tanks and Google searches using the following search terms: 'citizen engagement'; 'community outreach'; 'citizen outreach'; 'critical infrastructure'; 'national security'; 'national security strategy'; 'cyber strategies'; 'defence strategies'; 'terrorism strategies'; 'private sector partnerships'; 'partnerships with business'; 'partnerships with academia'; 'partnerships with industry'; and 'partnerships with the general public'.

000209

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

2.0 Background/Concepts Section

This section will outline the main concepts of citizen engagement and will provide a general overview of the methods which can be used in achieving these different forms of engagement.

2.1 What is Citizen Engagement?

According the to Queensland government, citizen engagement can be defined as "the many ways in which government connects with citizens in the development and implementation of policies, programs and services". (Queensland government web-site, 2010)

2.2 What are the Benefits of Engaging Citizens?

When conducted effectively these initiatives create a "win-win" situation where governments are able to capitalize on the expert advice and expertise of citizens and citizens gain a feeling of inclusion and a sense of ownership in the decisions which are made

According to the OECD the benefits of citizen engagement are as follows:

> "Strengthening relations with citizens is a sound investment in better policy-making and a core element of good governance. It allows government to tap new sources of policy-relevant ideas, information and resources when making decisions, equally important, it contributes to building public trust in government, raising the quality of democracy and strengthening civic capacity. Such efforts help strengthen representative democracy, in which parliaments play a central role."

Therefore, there are many reasons why a government may choose to engage their citizens or groups thereof into policy issues generally, which can be grouped into the following categories:

1) **To increase the Political Knowledge of Citizens**: The goal of this type of engagement is to provide their citizens information regarding the political issues currently facing their nation, and the direction the current government plans to take to resolve these issues. This is usually achieved through advertising campaigns, public releases such as: National Security statements or action plans.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

2) **To increase Political Participation**: The goal of this type of engagement is to receive feedback or information either from the general public, or particular stakeholders or academics in private industry. Programs which aim to increase political participation usually includes: roundtable discussions with members of particular interest groups, academics or industry leaders; but could also include: referendums and most recently could come as a request for ideas and comments through Internet blogs which are posted on government web-sites.

3) **To increase Trust in Current Government**: Governments which are interested in increasing trust or public confidence could do so by increasing the "transparency" of the government, i.e., making more information and public documents available.

4) **To provide the government with the opportunity to gain expert advice** on complex issues.

5) **To enable the government to gain a better understanding of the issues which are most relevant to the citizenry** of their nation.

6) **To provide the government with valuable feedback to improve or eliminate programs which are not longer effective**.

7) **To provides an opportunity for co-learning**, for both the community and the government.

8) **To achieve better outcomes by generating behavioural changes within the government and the community**.

9) **To raise community awareness of important issues**; and finally,

10) **To promote a better democracy.**

(Queensland government web-site, 2010)

2.3 What Groups of Citizens are Typically Targeted by Engagement Initiatives?

Generally speaking, programs aimed at engaging citizens usually aim to either engage:

1) **All Citizens**: These are programs or initiatives which have been put into place in order to inform or engage all citizens; or

2) **Business owners, experts or particular groups within the general population:** These are instances where programs or initiatives which have been implemented in order to resolve a specific issue: such as protection of critical infrastructure, working groups on advancements in defence technology or

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

sciences, or outreach to members of the general population to provide a counter narrative to extremist views, to name a few.

2.4 What are the Different ways in which Citizens can be Engaged?

In a Policy Brief by the OECD entitled "*Engaging Citizens in Policy-Making: Information, Consultation and Public Participation*", gave the following overview of the types of relationships which can occur between a government and its citizens with the intended purpose of raising civic participation. They are as follows:

- **Information only**: This is a one-way relationship between a government and its citizens in which the government produces and delivers information to citizens. This can be 'passively', which requires a citizen to request the information and 'actively' which means that the information is distributed to all members of the society equally.

- **Consultation**: Programs which fall under the consultation category generally relate to a two-way relationship between the citizens and the government provides information surrounding the issue and requests the opinion or feedback about this issue from its citizens.

- **Active participation**: This is a partnership in which citizens actively participate in the policy-making process, although the final decision ultimately rests with the government. (OECD, 2001)

2.5 Communication Methods in the 21st century

In our modern world, there are many modes of communication, which a government can employ in order to outreach to its citizens on a national, group or individual level. Below is a list of some of the most popular modes used by governments. Less commonly known terms have been defined in the Appendix A section at the end of this document.

1) **Use of the Internet** by employing one or many of the following vehicles:

- Government home pages;
- Web-sites;
- Internet discussion boards;
- Internet-based forums;
- 'Open Space' Technology;
- Social networking sites i.e. Facebook and MySpace;
- Video streaming such as You Tube and Flickr;
- Mobile instant messaging;
- Viral marketing;
- Blogs;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Web chats;
- Wikis;
- Micro-blogs – i.e. Twitter and
- And pod casts.

2) **National media**, such as:

- National newspapers;
- National radio broadcasts;
- National television broadcasts; and
- National advertising campaigns which include advertisements utilising all or one of the above forms of media.

3) **Public speeches or dissemination of material such as**:

- Public Speeches by senior officials which are addressed to the general public;
- Briefings, and
- The release of documents for public use (either through the Internet or in hard copy).

4) **Public opinion research,** such as:

- Polls;
- Referendums;
- Focus groups and
- Other forms of 'Action Research'.

5) **Discussion groups at the national level** which include members of academia, specific groups or organization which are relevant to a particular topic, such as:

- Advisory boards, councils and committees;
- Summits;
- Deliberative retreats;
- Policy action teams;
- Charettes; and
- Citizen Panels.

6) **Local media** to address issues or inform citizens in a specific region by using local media such as:

- Local newspapers;
- Local radio;
- Community radio;
- Local television;
- Speciality press;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Community newsletters; and
- Notice boards in community centres.

Discussion groups at the community level, such as:

- Community meetings;
- Stakeholder segmentation;
- Community reference groups; and
- Learning circles.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

3.0 Citizen Engagement in National Security Issues in the United States

The United States has long been a world leader in engaging their citizens in policy making decisions by holding community meetings and referendums on important issues, which has only increased in the 9 years in the wake of the terrorist attacks of September 11th, 2001. Therefore this paper will explore the following:

1) **The National Security Strategies which were released in the pre-September 11th era**;

2) **The National Security Strategies which have been released in the Post September 11th era**:

3) **The National Information Strategies which have been introduced in order to facilitate greater sharing of information between agencies as well as with the general public;**

4) **The Transparency and Open Government Initiative and programs which have launched as a result**; and finally

5) **A brief overview of the Outreach programs which have been launched to date to address National Security issues in a broad sense or a facet thereof**. These outreach programs will be organized first by topic and by the year of initiation.

3.1 The History of National Security Strategies in the United States

The emergence of National Security Strategies in the United States began under the authority of the *National Security Act of 1947 (NSA).* (Dale, 2008) This legislation laid the foundations for the creation of the National Security Council, the Central Intelligence Agency, the Department of Defence, and a separate Department for the Air Force and a permanent Joint Chiefs of Staff. The *NSA*, was then changed under Goldwater-*Nichols Department of Defence Reorganization Act of 1986*, which made the requirements that each National Security Strategy be presented annually by the President (Dale, 2008).

3.2 Frequency of issuance over time

Since the *Goldwater-Nichols Act*, National Security Strategies have not always delivered annually but have been made frequently. The first submitted by the Reagan Administration was in 1987 and then in 1988. The Bush Administration which followed (George Bush, Sr.) submitted three (1990, 1991, and 1993); and the Clinton

000215

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Administration submitted seven (1994, 1995, 1996, 1997, 1998, 1999, and 2000). (Dale, 2008)

3.3 National Security Strategies in the Post September 11th Era and the Reviews Thereof

In the case of the United States government, they have developed more than 30 other national strategies in specific topic areas to add greater depth in areas of great importance. The National Security strategies which have been released to the public since 9/11 are as follows (in order of first release):

- *The National Security Strategy* issued in 2002, an updated version was released in March of 2006 and the most recent version was released in May of 2010;
- *The National Strategy for Homeland Security* first released in July 2002, the updated version was released in October of 2007;
- T*he National Strategy to Combat Weapons of Mass Destruction* first released in December 2002, and the updated version was released in February of 2006.
- *The National Money Laundering Strategy* was released in 2002 and 2007;
- *The National Strategy to Combat Terrorism* released in February 2003 and the updated Strategy was released in 2006;
- *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* released in February 2003;
- *The National Strategy to Secure Cyberspace* was released in February 2003;
- *The National Military Strategy* was released in 2004;
- *The National Border Patrol Strategy* was released in 2004;
- *The 9/11 Commission Report* which was released in July of 2004 and the *9/11: Five Years Later: Successes and Challenges* which was released in 2006.
- *The National Defense Strategy* was first released in 2005 and the updated versions was released in 2008;
- *The National Counter-Intelligence Strategy of the United States of America* was released in March 2005;
- *The National Defense Strategy and Civil Support* was released in June 2005 and the updated version was released in 2007;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- *The National Strategy for Maritime Security* was issued September 2005;

- *The National Intelligence Strategy* was issued October 2005 and the updated version was released in 2009;

- *The National Military Strategy for Cyberspace Operations* was created in 2006 but was only recently released since it was initially classified as secret;

- *The National Military Strategic Plan for the War on Terrorism* issued February 2006;

- The National Military Strategy to Combat Weapons of Mass Destruction, issued February of 2006;

- *The National Security Strategy to Combat Terrorist Travel* was issued in May 2006;

- *The National Space Policy* first issued in 1996, updated in 2006 and most recently released in June of 2010;

- *The National Strategy for Aviation Security* issued in March of 2007;

- *The Small Vessel National Security Strategy* was first released in January of 2008 and then an updated version was released in April of 2008;

- *The National Strategy for Countering Biological Threats,* which was issued November 2009; and

- *An Overview of the reviews which have been conducted of the National Defense Strategy and the National Strategy of Homeland Security since September 11th.*

The following section will provide a short description of the purpose of each of these strategies. For more information on any one particular Strategy, please refer to the reference guide for a link to the complete document.

The National Security Strategies (NSS) of 2002, 2006 and 2010

The recent Bush Administration (under George W. Bush, Jr.) submitted two documents both of which were entitled *National Security Strategy of the United States of America*, the first in September 2002 and the second in March of 2006. (Dale, 2008) The latest National Security Strategy was released in May of 2010 by the Obama Administration.

These *National Security Strategies* provide an overview of the challenges or threats to National Security which are (and were) currently facing the United States government at the time of their issuance, and these strategies take into account other significant socio-economic incidents which have occurred from the last issuance for example: the effects

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

of Hurricane Katrina, global economic crisis, the War in Afghanistan, and other external influences; assesses their impact on National Security, and provides an overview of the ways in which the United States government intends to address these issues. (National Security Strategies of 2002, 2006 and 2010)

National Strategies for Homeland Security – 2002 and 2007

Shortly after 9/11, President Bush created the Office of Homeland Security at the White House. The first responsibility of this new division was to produce a *National Strategy for Homeland Security* (NSHS). This Strategy was first issued in July of 2002 and the purpose of this document is provide information as to the threats which pose the greatest risk to homeland security and to proposed specific initiatives to address these risks related to six "critical mission areas", which are as follows:

1) Intelligence and Warning;
2) Border and Transportation Security;
3) Domestic Counterterrorism;
4) Protecting Critical Infrastructure and Key Assets;
5) Defending Against Catastrophic Threats; and
6) Emergency Preparedness and Response.

In addition, the 2002 NSHS called for the creation of the Homeland Security Council (HSC) and established the Department of Homeland Security (DHS), in order to meet these objectives. While the 2002 version of the NSHS did not establish a requirement for the National Strategy for Homeland Security to be updated, the NSHS of 2002 did require the HSC to provide policy oversight and engage in assessment.

The second iteration of the NSHS was released in October of 2007. This updated Strategy built on its 2002 predecessor, but also included some updates which were made in response to the issuance of the *National Security Strategy of 2006;* and the *National Strategy to Combat Terrorism (NSCT)* issued the same year, and 'lessons learned, from other world catastrophes such as Hurricane Katrina.

Finally, in 2007 Congress established a new requirement mandating the Secretary of Homeland Security to conduct a Quadrennial Homeland Security Review (QHSR), on the model of the Quadrennial Defense Review (QDR) at the Department of Defense. The legislation requires that the QHSR be conducted every four years, beginning in 2009, therefore, future iterations of this Strategy are expected. (Dale, 2008)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The National Strategy to Combat Weapons of Mass Destruction of 2002 and 2006

The *National Strategy to Combat Weapons of Mass Destruction* (NSCWMD) was first introduced in December 2002 and was updated in 2006. The NSCWD provided a National Strategy to combat weapons of mass destruction through three major efforts:

1) Non-proliferation;
2) Counter proliferation; and
3) Consequence management in weapons of mass destruction incidents.

National Strategy to Combat Terrorism of 2003 and 2006

The *National Strategy for Combating Terrorism (NSCT)* was first issued by President Bush Jr. in February 2003. This Strategy was a follow-up document to the *National Security Strategy (NSS) of 2002*. The division of responsibility between the *NSCT* and the *National Strategy for Homeland Security*, was addressed in the *NSCT* and was explained as follows: 'the National Strategy for Homeland Security is responsible for providing strategies to 'prevent terrorist attacks from occurring within the United States," while the *NSCT* was responsible for "identifying and defusing threats before they reach our borders." (Dale, 2008)

The NSCT was updated in 2006, in response to the issuance of a new National Security Strategy in March 2006 included revisions based on 'lessons learned' over the three-year time period.

National Money Laundering Strategy (NMLS) of 2002 and 2007

First issued in 2002, The *National Money Laundering Strategy (NMLS)* is intended to support planning for the efforts of law enforcement agencies, regulatory officials, the private sector, and overseas entities to combat the laundering of money generated from criminal activities.

This Strategy was updated in May of 2007 in response to the first-ever interagency U.S. Money Laundering Threat Assessment. Additionally, the 2007 Strategy focuses on levelling the 'playing field' internationally, helping to ensure U.S. financial institutions are not disadvantaged through the implementation of controls and standards to combat money laundering and terrorist financing. (MLS, 2002 and 2007)

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets of 2003

The *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets Strategy (NSPPCIKA),* was issued in February of 2003, and provided a statement that expressed the US government's commitment to protecting 'critical infrastructure and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

key assets' from terrorist attacks. This Strategy was based on eight guiding principles, including:

- "establishing responsibility and accountability;
- encouraging and facilitating partnering among all levels of government and between government and industry; and
- Encouraging market solutions wherever possible and government intervention when needed.

This Strategy also establishes three strategic objectives. The first is to identify and assure the protection of the most critical assets, systems, and functions, in terms of national level public health and safety, governance, and economic and National Security and public confidence. The second is to ensure protection of infrastructures and assets facing specific, imminent threats. The third is to pursue collaborative measures and initiatives to ensure the protection of other potential threats. (NSPPCIKA, 2003)

The National Strategy to Secure Cyberspace of 2003

Issued in February of 2003, The *National Strategy to Secure Cyberspace* (NSSC) is intended to provide an initial framework for both organizing and prioritizing efforts to protect against threats in cyberspace. This Strategy provides direction to federal departments and agencies that have roles in cyberspace security in order to identify steps which need to be taken by State and Local governments, private companies and organizations, and individual Americans to improve the Nation's collective cyber security. The Strategy is organized according to five national priorities, with major actions and initiatives identified for each. These priorities are (NSSC, 2003):

(1) National Cyberspace Security Response System;
(2) National Cyberspace Security Threat and Vulnerability Reduction Program;
(3) National Cyberspace Security Awareness and Training Program;
(4) Securing Governments' Cyberspace; and
(5) National Security and International Cyberspace Security Cooperation.

The National Military Strategy of 2004

The National Military Strategy (NMS) entitled the *National Military Strategy of the United States of America: A Strategy for Today, a Vision for Tomorrow* and was issued in 2004. Among other things, this document stated purpose is to provide strategic guidance for how military operations can support the aims of the *National Security Strategy (Dale, 2008).*

The National Border Patrol Strategy (NBPS) of 2004

The *National Border Patrol Strategy (NBPS)* was issued in 2004 and remains an important element in the protection of National Security because it provides guidance for

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the protection the U.S. border from: illegal trafficking; the importation of firearms and weapons of mass destruction; and the immigration of terrorists. (NBPS, 2004)

The 9/11 Commission Report and the 9/11: 5 Years Later

This report was drafted by the *National Commission on Terrorist Attacks upon the United States*, which was created in November of 2002. The mandate of this commission was to investigate the facts and circumstances related to the terrorist attacks September 11, 2001, 'in order to provide the fullest possible account of the events surrounding these attacks and to identify lessons learned'. In pursuing this goal, this commission reviewed more than 2.5 million pages of documents and interviewed more than 1,200 individuals in ten countries (9/11 Commission Report, xv). This report was followed up in 2006 with the release of the 9/11: 5 Years Later: Successes and Challenges document which provides an overview of the successes which have been achieved in the 'War on Terror' over the 5 year period following the September 11th attacks and outlines the challenges for the future. (9/11 Commission Report, 2006)

The United States National Defence Strategy (NDS) of 2005 and 2008

The *National Defence Strategy (NDS)* is produced by the Department of Defence (DOD) under the authority of the National Defense Authorization Act (NDAA) and the National Security Strategy. The National Defense Strategy explains how the DOD will provide support for the objectives outlined in the NSS in order to support a broader overall National Security Strategy.

This Strategy was updated in 2008. The 2008 version reflects the results from the *Quadrennial Defence Review (QDR) of 2006* and 'lessons learned' from on-going operations in Iraq, Afghanistan and elsewhere. The 2010 QDR was released in February of 2010; therefore, an updated version of the National Defence Strategy will likely follow in the near future. (NDS, 2005 and 2008).

The National Counterintelligence Strategy (NCIS) of the United States – March 2005

The *National Counterintelligence Strategy (NCIS)* of the United States was issued on March 1, 2005, under the authority of the *Counterintelligence Enhancement Act* of 2002. This Strategy includes defensive and offensive activities conducted at home and abroad to protect against the traditional and emerging foreign intelligence threats of the 21st Century. (NCIS, 2005)

The Strategy for Homeland Defense and Civil Support (SHDCS) of 2005 and 2007

The SHDCS was first released in 2005 in order to provide strategic direction for the DOD to: 'dissuade, deter and defeat attacks on Critical Infrastructure'; support civil authorities in the prevention and recovery from a disaster or attack; and to enable share expertise and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

technology across military and civilian boundaries, domestically and internationally where appropriate.

This Strategy was updated in 2007 to include the following: 'a theory of war that addresses the National Defence Strategy (NDS); the desired effects and end states of operations; a description of how operations will be conducted; assessments of associated risks and how they will be mitigated; and to identify and prioritize the capabilities needed to conduct the desired operations. (SHDCS, 2005 and 2007)

Maritime Security Policy (MSP) of 2005 and 2008

The MSP was first issued in 2005 and was updated in 2008. The MSP provides direction for the coordination of maritime security programs and initiatives involving appropriate Federal, State, local, and private sector entities to protect the US from a Maritime perspective. (MSP, 2005 and 2008)

The National Intelligence Strategy of the United States of America (NIS) - Oct 2005

The *National Intelligence Strategy (NIS)* was released in October of 2005 and was built on the new concept of "National Intelligence" which was codified in the *Intelligence Reform and Terrorism Prevention Act (IRTPA)* of 2004. The NIS provided the 'mission' and 'enterprise' objectives for the 'intelligence community' for the following four years: The mission objectives were as follows: 'combat violent extremism; counter weapons of mass destruction proliferation; provide strategic intelligence and warning; integrate counterintelligence; enhance cyber security; and support current operations.'

The enterprise objectives were as follows: 'enhance community; mission management; strengthen partnerships; streamline business processes; improve information integration & sharing; advance science and technology research and development; develop the workforce and improve acquisitions. (NIS, 2005)

National Military Strategy for Cyberspace Operations (NMSCSO) 2006

The NMSCSO was developed in 2006 but was classified as 'secret' until just recently. The purpose of this Strategy was to provide a comprehensive Strategy for US Armed Forces to establish a common understanding of cyberspace and sets forth a strategic military framework to be used as a reference to: plan, execute and resource cyberspace operations. (NMSCSO, 2006)

National Military Strategic Plan for the War on Terrorism of February 2006

The *National Military Strategic Plan for the War on Terrorism (NMSP-WOT)* was created to provide a comprehensive military plan for the Armed Forces to prosecute the Global War on Terrorism (GWOT). The guiding principles of this plan are: 'to protect

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

and defend the US; to attack terrorists and their capacity to operate effectively at home and abroad; and to support mainstream efforts to reject violent extremism'. (NMSP-WOT, 2006)

The National Military Strategy to Combat Weapons of Mass Destruction (NMS-CWMD) of 2006

The purpose of the *National Military Strategy (NMS) to Combat Weapons of Mass Destruction (CWMD)* was to provide the Department of Defence with a 'strategic framework for combating weapons of mass destruction'. The Strategy employs an "ends, ways, means" approach to planning, executing and resourcing, and emphasizes those combating WMD missions in which the military plays a prominent role. (NMS-CWMD, 2006)

National Strategy to Combat Terrorist Travel (NSCTT) - May 2006

The 9/11 Commission noted that 'constraining the mobility of terrorists should be a key focus of the US Government's counterterrorism initiatives over the coming years.' Therefore, in regard to this recommendation and under the authority of the *Intelligence Reform and Terrorism Prevention Act* of 2004, the National Counterterrorism Center (NCTC) drafted this National Strategy To Combat Terrorist Travel (NSCTT) which as released in May of 2006. (NSCTT, 2006)

U.S. National Space Policy (NSP) of 1996, 2006 and 2010

The first ever National Space Policy was issued in September of 1996, but was updated in 2006 and the latest version was released in June of 2010. The goals of the 2010 NSP were as follows: 'energize competitive domestic industries; expand international cooperation; strengthen stability; increase assurance and resilience of mission-essential functions; pursue human and robotic initiatives to develop innovative technologies; and improve space-based Earth and solar observation to support disaster response and recovery. (NSP, 2010)

The National Strategy for Aviation Security (NSAS) of 2007

The NSAS was issued in 2007 and was designed to align the Federal government aviation security programs and initiatives into a national effort involving appropriate Federal, State, Local, and Tribal governments and the private sector to provide active layered aviation security for the United States. This Strategy was developed as a collaborative interagency effort and includes input received from aviation stakeholders. (NSAS, 2007)

The Small Vessel National Security Strategy (NVNSS) of 2008

This NVNSS was developed as a result of a Summit where approximately 300 small vessel maritime stakeholders and top Federal, State, and Local government officials came together to share concerns about small vessel operations, safety, and security. Using the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

recommendations from the National Summit, a DHS working group developed the *Small Vessel Security Strategy*, which was published in April 2008, to address the risks of small vessels to National Security. (NVNSS, 2008)

The National Strategy for Countering Biological Threats (NSCBT) - November, 2009

In this Strategy, President Obama established a commitment wherein 'the United States Government will work with domestic and international partners to advance the health security of all people by mitigating the misuse of biological weapons while having as little impact as possible on the beneficial uses of these weapons.' He recognized that in order to reduce the risks of deliberate or accidental release of biological weapons requires close coordination is needed among all sectors of government as well as effective partnerships among public and private institutions both nationally and internationally. (NSCBT, 2009)

3.4 Reviews conducted by the Department of Defence

The United States Department of Defence and the Department of Homeland Security are legislatively mandated to review their policies every 4 years. In addition to these reviews, these departments have also conducted a few other reviews of other policies which are also related to National Security. Please see below for a brief overview of the recent reviews which have been conducted by these two departments:

- **Quadrennial Defence Review (QDR)**: the most recent version of the QDR was released in February of 2010. This review assesses the current threats and challenges that are of greatest importance at the moment for the US government and then revises the long-term strategies and resource allocation of the DOD forces accordingly.
- **Ballistic Missile Defence Review (BMDR)**: the BMDR was released in June of 2010. This Strategy also identifies the most important threats in relation to ballistic missile defence and outlines the DOD Strategy in order to address current and future challenges.
- **Nuclear Posture Review (NPR)**: The NPR was released in April of 2010. This review of the US Nuclear Policy assesses the current threats of greatest importance and establishes the US Nuclear Strategy and outlines the resources which will be allocated in order to achieve these goals over the next five to ten years.
- **Space Posture Review (SPR)**: The SPR was legislatively-mandated by the FY09 National Defense Authorization Act. The SPR 'analyzes the relationship between military and national security space strategy and assesses space acquisition programs, future space systems, and technology development'. This review was conducted jointly by the Secretary of Defense and the Director of National Intelligence, and covers a 10 year period, beginning in February of 2010. (DOD web-site, 2010)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

3.5 Reviews conducted by the Department of Homeland Security

The Department of Homeland Security has also released two reviews recently, related to National Security issues. They are as follows:

- **Quadrennial Homeland Security Review Report (QHSR):** The most recent quadrennial review was released in February of 2010, and it 'outlines the strategic framework to guide the activities of participants in homeland security toward a common end' (DHS web-site, 2010)
- **Bottom's Up Review Report (BUR):** The BUR provides the results of an unprecedented Department-wide assessment of the Department of Homeland Security, which began in November 2009. The goal of this review was to align the Department's programmatic activities and organizational structure with the mission sets and goals identified in the QHSR. (DHS web-site, 2010)

3.6 National Information Sharing Strategies

The National Security Strategies which have been released in the United States since 9/11 have noted the need for collaboration with individuals and/or the private sector in the pursuit of their objectives. In order to facilitate this collaboration, the US government recognized that this would require a shift in the way in which information was shared between departments as well as with the general public. In order to rectify this potential obstacle, several documents have been released for the purpose of providing senior government officials with guidance and a framework to facilitate a shift in the way information is exchanged, not only across government departments but also within: international partners, private sector companies, community organization and the general public. The Strategies which have been issues in order to facilitate this shift are as follows:

- *The Information Sharing Environment (ISE) Implementation Plan*, of November 2006;
- *The National Strategy for Information Sharing: Successes and Challenges to Improving Terrorism-related Information Sharing*, released in 2007;
- *The Department of Defence Information Strategy*, of 2007;
- *The 100 and the 500-day plans*, of 2007;
- *The Intelligence Community Information Sharing Strategy* of 2008; and
- *The National Framework for Strategic Communication* of 2010.

Below you will find a brief description of each of these Strategies.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Information Sharing Environment Implementation Plan - 2006

This plan was developed by the *Information Sharing Council* (ISC). The purpose of developing this plan was to meet the specific objectives of the goals set by the Congress in the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), and by the President in his memorandum, *Guidelines and Requirements in Support of the Information Sharing Environment*, of December 2005 which called for the creation of an "Information Sharing Environment (ISE)", specifically, for the purpose of 'sharing of terrorism information in a manner consistent with National Security and with applicable legal standards relating to privacy and civil liberties'. The IRTPA further requires that the ISE provide and facilitate "the means for sharing terrorism information among all appropriate Federal, State, Local, and Tribal entities, and the private sector" and to the greatest extent practicable consist of "a decentralized, distributed, and coordinated environment" that:

- Connects existing systems where appropriate, providing no single points of failure, and allowing users to share information among agencies, levels of government, and, as appropriate, the private sector;
- Ensures direct and continuous online electronic access to information;
- Facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations, and operations;
- Builds upon existing systems capabilities currently in use across the Government;
- Employs an information access management approach that controls access to data, rather than just systems and networks, without sacrificing security;
- Facilitates the sharing of information at and across all levels of security;
- Provides directory services, or the functional equivalent, for locating people, organizations, and information;
- Incorporates protections for individuals' privacy and civil liberties; and
- Incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.

This Strategy also created the *Common Terrorism Information Sharing Standards* (CTISS) and the *Framework for Sharing Information outside of the Federal Government*. Please see below for further detail regarding these two initiatives. (Information Sharing Environment Implementation Plan, 2006)

Common Terrorism Information Sharing Standards (CTISS), Version 1.0

In April of 2006, the ISC established a working group to define common standards that support how terrorism information is acquired, accessed, shared, and used. A product of this working group is the *Common Terrorism Information Sharing Standards (CTISS), Version 1.0*. The CTISS provides the framework for 'developing and implementing business process-driven ISE functional standards for use universally across all levels of government, the private sector, and foreign partners. These standards also support the domains of intelligence, law enforcement, homeland security, foreign affairs, and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

defence'. The document entitled *Information Sharing Environment Implementation Plan, 2006* contains a graphic image of the CTISS framework located on page 66. This document can be found at: http://www.ise.gov/docs/ISE-impplan-200611.pdf.

The Framework for Sharing Information outside of the Federal Government

The *Framework for Sharing Information outside of the Federal Government* was developed in response to Presidential Guideline 2 which was to 'establish a coordinated, collaborative structure through which terrorism information is shared between and among participating Federal, State, Local, Tribal governments, as well as private sector organizations to support a variety of different activities, including preventive and protective actions, immediate actionable response, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events'. A graphic image of the *Framework for Sharing Information outside of the Federal Government* can be found in the document entitled *Information Sharing Environment Implementation Plan, 2006* on page 71. This document can be found at: http://www.ise.gov/docs/ISE-impplan-200611.pdf.

The National Strategy for Information Sharing (NSIS): Successes and Challenges in Improving Terrorism-Related Information Sharing – October 2007

This NSIS was issued in 2007 and was created as a guide to improve the sharing of information at all levels including the private sector, particularly in terms of protection of the nation's Critical Infrastructure. The basic, underlying premise of this Strategy was that there is 'no single source of information related to terrorism; it comes from a broad range of sources.' Therefore, there was a need to create a new way of sharing information while still preserving National Security (NSIS, 2007). A graphic image of the *Foundations of the National Strategy for Information Sharing* can be found on page 5 of the document *Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, which can be found at the following website: http://www.fas.org/sgp/library/infoshare.pdf.

Intelligence Community Information Sharing Strategy (ICISS) of 2008

The ICISS was also created under the authority of the *Intelligence Reform and Terrorism Act* of 2004. This Strategy was drafted to facilitate a shift in thinking among intelligence agencies form sharing information with others on a 'need to know' basis, to a model which emphasized the principle that all government officials had a 'responsibility to provide' all effected parties with the security information they require in order to ensure homeland security, of all forms. This Strategy emphasized that government departments and personnel were not the 'owners of the data' which they currently possess, but should act more as 'stewards' of the data and information they possess and were responsible to disseminate the data and information they possess under the principles which were outlined in the *National Strategy for Information Sharing*. The ultimate goal of this

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Strategy is to provide a new perspective on intelligence information sharing, and that is to provide for the maximum amount of knowledge of potential threats and how to prevent against them to be disseminated to the maximum number of stakeholders or interested parties without compromising the interest of National Security in order to reduce duplication of effort, to maximize efficiency and minimize threats.

For a visual representation the new 'responsibility to provide' information sharing model, please refer to the image on page 9 of the document *United States Intelligence Community Information Sharing Strategy*. This document can be found at: http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf.

Department of Defense Information (DOD ISS) of 2007

The Department of Defence Information Sharing Strategy (DOD ISS) was developed in response to the Quadrennial Defence Review and was released in May of 2007. The purpose of the DOD ISS was to provide 'a common vision' among all the components of the Department of Defence (DOD) so that efforts to share information with other government departments, international partners and the private sector could be 'synchronized' to support the *National Strategy on Information Sharing (NSIS)*. In pursuance of this goal, this document established an Information Sharing Senior Steering Group and defined near-term actions and milestones in order to achieve the objectives of the NSIS. (DOD Memo, May 4, 2007). Please see the following document for a figure depicting the Department of Defence's Information Sharing Model: http://cio-nii.defense.gov/docs/InfoSharingStrategy.pdf.

The 100 and 500 Day Plans

The 100 and 500 Day Plans were also released with the objective of integrating the Intelligence Community. (100 Day plan, 2007: 2) The 100 Day Plan prioritized and accelerated six enterprise integration priorities, namely: creating a culture of collaboration; fostering collection and analytic transformation; build acquisition excellence and technology leadership; modernize business practices; accelerate information sharing; and clarify and Office of the Director of National Intelligence's (DNI) authorities. (100 Day plan, 2007: 2)

The *500 Day Plan: Integration and Collaboration* was released in 2007 in order to build on the objectives of the *100 Day Plan* which constituted the first phase of this plan. An explanation and graphic depiction of how the 500 Day Plan was intended to help implement the National Security Strategy can be found on page 2 of the *500 Day Plan: Integration and Collaboration* document, which can be found at: http://www.dni.gov/500-day-plan/500-day-plan.pdf.

The National Framework for Strategic Communication of 2010

This framework was created as a result of the requirements specified in *The Duncan Hunter·National Defense Authorization Act for Fiscal Year 2009* for the President to 'to

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

submit to the appropriate committees of Congress a report on a comprehensive interagency strategy for public diplomacy and strategic communication'. This report describes the terms 'strategic communication' as well as what is meant by 'deliberate efforts to communicate and engage with intended audiences. This report also provides detail as to the positions, processes, and interagency working groups which have created to improve the US government's ability to 'coordinate communications and engagement programs and activities; and recognizes the need to ensure an appropriate balance between civilian and military efforts in preserving National Security. As a result, a review process of existing programs is underway to develop short-, medium-, and long-term options for addressing issues pertaining to resources and thought is put into the need for existing programs to be evaluated and how such evaluations should be conducted. Please see the 'Best practices' section of this document for further detail. (National Framework for Strategic Communication document, 2010)

3.7 Outreach Programs by Type

Below is a list of the programs and initiatives which have been identified to date which have been enacted by some level of the United States Government in order to engage citizens in issues related National Security to some degree. These outreach programs have been organized by subject and then by date to facilitate reading.

3.7.1 National Security Initiatives – General

Advisory Committees-FACA

The *Federal Advisory Committee Act* (FACA) was enacted by Congress in 1972 to illuminate how agencies make decisions based upon the advice and recommendations from individuals outside of Government. The Department of Homeland Security (DHS) currently has 27 Federal Advisory Committees, comprised of more than 700 DHS stakeholders that are established and operate under the provisions of the FACA. To date, FACA committees have submitted roughly 2,448 recommendations to the Department of Homeland Security for their consideration.

The FACA committees engage with the public by providing the opportunity for the general public to personally attend a meeting; to mail or email the Committee directly with thoughts and concerns and meetings are broadcast on-line so the general public has the opportunity to view a meeting if they so wish. (DHS web-site, 2010)

Homeland Security Advisory Council (HSAC):

The HSAC Council is comprised of leaders from State and Local government, first responder communities, the private sector, and academia, and provides advice and recommendations to the Secretary of Homeland Security on matters related to homeland security issues. The HSAC currently has six active subcommittees, which are as follows (DHS web-site, 2010):

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Academy and Policy Research Senior Advisory Committee;
- Emergency Response Senior Advisory Committee;
- Private Sector Senior Advisory Committee;
- State and Local Officials Senior Advisory Committee;
- Quadrennial Homeland Security Review Advisory Committee; and
- Sector Partnership Advisory Council.

Homeland Security Information Network Advisory Committee (HSINAC):

The Homeland Security Information Network Advisory Committee (HSINAC) provides independent advice and recommendations the Department of Homeland Security, particularly the Director of the Office of Operations Coordination and Planning (OPS), on the requirements of end users within State, Local, Federal, and Tribal governments and the private sector regarding the Homeland Security Information Network (HSIN). (National Strategy for Information Sharing, 9-10)

Homeland Security Information Network (HSIN)

'The Homeland Security Information Network (HSIN) is a national secure and trusted web-based portal for information sharing and collaboration between Federal, State, Local, Tribal, Territorial, private sector, and international partners engaged in the homeland security. HSIN is made up of a growing network of communities, called Communities of Interest (COI). COIs are organized by state organizations, federal organizations, or mission areas such as: emergency management, law enforcement, critical sectors and intelligence.

Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging and document sharing. HSIN allows partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate (DHS web-site, 2010). Features of this system include:

- 24/7 availability;
- Document libraries;
- Instant-messaging tool;
- Web conferencing;
- Incident reporting;
- Common Operational Picture (COP) provides situational awareness and analysis
- Integrated Common Analytical Viewer (iCAV) gives geographical visualization;
- Announcements;
- Discussion Boards;
- Task Lists;
- Requests For Information/For Your Information (RFIs/FYIs);
- Calendars;
- Really Simple Syndication (RSS) Feeds; and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Online training materials.

Please see page 12 of the document *Public Transit Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach* for an interactive figure of mechanisms for sharing public transit security information. This document can be found at the following website: http://www.gao.gov/new.items/d10895.pdf

FUSION Centres

Since 2001, all 50 states and some local governments have established fusion centres, where homeland security, terrorism and other intelligence information is shared. Currently, there are a total of 72 Fusion centres in operation; however Fusion centres have expressed a need for additional funding from the DHS in order to meet their baseline objectives and functions to support the National Information Sharing Network. Currently, a nationwide assessment of the baseline capabilities of Fusion centres is underway by the Department of Homeland Security, the Program Manager for the Information Sharing Environment and the Department of Justice, which is slated to be completed in October 2010. The goal of this study is to provide federal agencies and fusion centres with more accurate information in regard to efficiencies and identify gaps in order to develop strategies to resolve issues. (DHS web-site, 2010)

National Security Dialogues

As part of the Quadrennial Homeland Security Review (QHSR) process in 2009, the Department of Homeland Security conducted what they referred to as online *National Security Dialogues.* These *Dialogues* were open to the public and subject matter experts across the country, through Internet forums which were set-up specifically for this task. These forums were held in three parts, each referred to as a *Dialogue*:

Dialogue 1: This was an initial forum to gain feedback from the general population on the goals and objectives developed by Department of Homeland Security study groups. These groups were divided into six topic areas, namely:

- Counterterrorism and Domestic Security Management;
- Securing our Borders;
- Smart and Tough Enforcements of Immigration Laws;
- Preparing for, Responding to, and Recovering from Disasters;
- Homeland Security National Risk Assessment; and
- Homeland Security Planning and Capabilities.

Participants were provided with information regarding the mission and goals of the six topic areas and then were permitted to: view, vote, rate or comment on the ideas of the DHS or others and to post their own ideas.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Dialogue 2: Provided an opportunity for a deeper discussion into how best to prioritize and achieve the proposed goals and objectives.

Dialogue 3: Consisted of a review of the final products of each study group and the feedback received from participants and identified the next steps.

These dialogue discussions were open between July 16th and October 4, 2009, and more than 20,000 stakeholders from all 50 U.S. states and the District of Columbia participated. The comments and ideas were used directly to inform the study groups tasked with writing the QHSR for the Department of Homeland Security, which was submitted to Congress in February 2010. (DHS web-site, 2010)

3.7.2 Defence-Related Initiatives

The Joint Civilian Orientation Conference (JCOC):

The Joint Civilian Orientation Conference (JCOC) is the oldest existing Pentagon outreach program. This conference has been held more than 76 times since 1948. It is a program which is sponsored by the Secretary of Defence. The JCOC conference allows participants to attend Pentagon briefings and then join military personnel in the field to observe exercise and participating in training. JCOC alumni are encouraged to share their experiences with their circles of influence when they return home. A principal goal of this conference is to increase understanding of the mission of the Department of Defence and the U.S. defence posture and capabilities by increasing public exposure to, and understanding of, military personnel, facilities, equipment, and programs. (USDOD web-site, 2010)

DoDTechipedia

Launched on October 1, 2008, DoDTechipedia was developed to improve the Department of Defence's ability to keep pace with innovation and to make existing science and technology (S&T) accessible to Department of Defense decision makers. The DoDTechipedia Family of Services currently has 4 components (Whitehouse web-site, 2010):

- **'DoDTechipedia Limited** for internal collaboration;
- **A classified version of DoDTechipedia**;
- **DefenseSolutions.gov** which allows entrepreneurs in industry and academia to get innovative solutions funded; and
- **a future public version of DoDTechipedia**, which, consistent with the framework and guidelines of National Security, will enable informal collaboration between government S&T personnel, large and small companies, research organizations and sole proprietors with emerging technologies and products'.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Biological Threat Reduction Prevention (BTRP) Program–FSU:

Through the Cooperative Biological Research (CBR) program, The US Department of Defence works with institutes and scientists previously involved in biological weapons research to employ them in peaceful research. By engaging former biological weapons scientists, CBR helps to prevent the proliferation of biological weapons, scientific expertise and pre-empt potential "brain drain" of scientists to rogue states (USDOD web-site, 2010).

3.7.3 Intelligence Initiatives

Global Trends

In fall 1996, the *National Intelligence Council* (NIC) and the Institute for National Strategic Studies (INSS) held a series of conferences at National Defence University to identify key global trends and their impact on major regions and countries of the globe. The exercise was designed to help describe and assess major features of the political world as they will appear in the year 2010.

Participants in the conferences included members of academic institutions, journalists, business, the representatives of the US Government, and other professions. Members of the National Intelligence Council (NIC) collaborated with INSS and other conference participants in crafting the agenda of the conferences. Although the proceedings were unclassified, the distribution list was very limited, but has since been made available due to on-going interest. Since then, four other *Global Trends* documents have been drafted, namely *Global Trends 2015, 2020 and 2025* which are also publicly available. (NIC web-site, 2010)

Federal Bureau of Investigation (FBI) Initiatives Related to Intelligence

There have been several programs initiated by the Federal Bureau of Investigation in order to collaborate with members of the community, in a variety of areas. The programs which are related to the concept of 'intelligence' in some form are listed below, while others are included under their designated topic areas.

- The **Counterintelligence Strategic Partnerships Program**: This program 'builds relationships between private industry, academia, government agencies, the FBI, and its counter-intelligence community partners to identify and protect projects of great importance to the U.S. government. The initiative is led by our Counterintelligence Division at FBI Headquarters, with local programs in each of field office' (FBI web-site, 2010).
- The **Domestic Security Alliance Council** (DSAC)—this program has been modeled after the U.S. Department of State's *Overseas Security Advisory Council* and is led by the FBI's Criminal Investigative Division. The DSAC was created

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

in October 2005 in order to 'strengthen information-sharing with the private sector to help prevent, detect, and investigate threats impacting American businesses. Today, DSAC enables an effective two-way flow of vetted information between the FBI and participating members (FBI web-site, 2010).

- **InfraGard** is a FBI program that began as a local effort in the Cleveland Field Office in 1996, in order to gain assistance from the information technology industry and academia for the FBI's investigative efforts in cyber space. The program expanded to other FBI Field Offices and in 1998 and was assigned to the Cyber Division of the former National Infrastructure Protection Center (NIPC) in 2003. Today, InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants who are 'dedicated to sharing information and intelligence to prevent hostile acts against the United States'. The InfraGard Chapters are geographically linked with FBI Field Office territories and each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, who works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C (InfraGard web-site, 2010)

CIA Archives

In response to numerous Freedom of Information requests, a collection of formerly Top Secret analytic monographs and reference aids, referred to as the CAESAR, ESAU, and POLO series, have been declassified and are now publicly available on the CIA web-site. While there are some documents in the series which are still considered to be sensitive and therefore have been withheld, there are a total of 147 documents in this collection which are publicly available, amounting to over 11,000 pages of analysis, written between 1953 and 1973. These monographs and reference aids highlight the CIA's efforts from the 1950s through the mid-1970s to pursue in-depth research on Soviet and Chinese internal politics and Sino-Soviet relations. (CIA web-site, 2010)

3.7.4 Justice Related Initiatives

Statistics on Unsealed International Terrorism and Terrorism-Related Convictions

The National Security Division of the United States Department of Justice has been responsible for tracking convictions resulting from international terrorism investigations conducted since September 11, 2001, in a tool called the *International Terrorism and Terrorism-Related Statistics Chart*. This chart includes investigations of terrorist acts planned or committed outside the territorial jurisdiction of the United States. Criminal cases arising from international terrorism investigations are divided into two categories:

- **Category I** cases involve violations of federal statutes that are directly related to international terrorism and that are utilized regularly in international terrorism matters.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- **Category II** cases include defendants charged with violating a variety of other statutes where the investigation involved an identified link to international terrorism. These Category II cases include offences such as those involving fraud, immigration, firearms, drugs, false statements, perjury, and obstruction of justice, as well as general conspiracy charges.

The chart includes the defendant's name, district, charging date, charges brought, classification category, conviction date and conviction charges. If a convicted defendant has been sentenced, the relevant date and sentence imposed is included. The chart does not include defendants whose convictions remain under seal, nor does it include defendants who have been charged with a terrorism or terrorism-related offence but have not been convicted either at trial or by guilty plea. This chart also does not include convictions related solely to domestic terrorism. There are more than 150 defendants classified in Category I and more than 240 defendants classified in Category II and the chart is organized by conviction date with the most recent convictions first. The decision to add defendants to the chart is made on a case-by-case basis. (USDOJ web-site, 2010)

3.7.5 Science and Technology Initiatives

National Academy of Sciences

The National Academy of Sciences was established by Congress more than a century ago to provide scientific and technological advice to the nation. Over the years, the Academy has evolved to incorporate four distinguished organizations: the *National Academy of Sciences*, the *National Academy of Engineering*, *the Institute of Medicine*, and the *National Research Council*, known collectively as the National Academies.

The National Academies provide science and technology advice to federal government officials. This advice can take the form of: written reports by expert committees; organizing symposiums to engage large audiences in discussion of national issues; conferences and workshops; or "white papers" on policy issues of special interest. Each project is conducted or overseen by a committee serving pro bono, whose members are selected for their expertise on the subject.

The National Academy of Sciences (NAS) formed the *Committee on International Security and Arms Control (CISAC)* in 1980. The CISAC, which is a part of the *Policy and Global Affairs Division*, draws from 'the nation's finest scientific, technical, engineering and medical talent to advise the government and inform the public about scientific and technical issues related to International Security and arms control'. Below is a list of the committees which fall under the umbrella of the National Academy of Science which are related to terrorism (National Academies web-site, 2010).

- **Board on Global Science and Technology (BGST)**: The BGST is sponsored by the Office of the Director, Defence Research and Engineering (DDR&E) and is charged with helping DDR&E assess the implications of global advances in science and technology. This Board seeks to 'build and sustain an international,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

interactive community of scientists, engineers, medical and health researchers, and entrepreneurs who are engaged in the research and development of emerging technologies' (National Academies web-site, 2010).

- **Committee on Science, Technology and Law (CSTL):** The CSTL was established in 1998 by the Science, Technology, and Law Program, (now called the Committee on Science, Technology, and Law) to bring together the science and the legal community to: explore pressing issues, improve communication and help resolve issues between theses two communities. A major activity for the program has been the convening of a distinguished committee chosen for their knowledge and expertise and who represent a wide range of organizations including federal courts, the legal community, industry, academia, and government to discuss these important issues (National Academies web-site, 2010).
- **Science & Technology Directorate:** The Science and Technology Directorate is a vehicle through which members of the Federal government collaborate with national laboratories, other government agencies, academia, and the private sector, both domestic and international to identify and develop scientific solutions and technological countermeasures to address a wide variety of terrorist and natural threats to the homeland. Divisions of this Directorate are as follows: Borders and Maritime Security; Chemical and Biological; Command, Control, and Interoperability; Explosives; Human Factors Behavioural Sciences; and Infrastructure and Geophysical (National Academies web-site, 2010).

3.7.6 Critical Infrastructure Initiatives

National Cyber-Forensics & Training Alliance (NCFTA)

The NCFTA was established in 1997, and is a non-profit corporation, which evolved from one of the US government's first High Tech Task Forces. The NCFTA 'has established an expansive alliance between subject matter experts (SMEs) in the public and private sectors (more than 500 worldwide) with the goal of addressing complex and often internationally-spawned cyber crimes. These SMEs, are from industry, academia and government, and each bring specific talents and experiences to the partnership. Evaluations of these relationships are conducted periodically to ensure all members continue to add value and attain the objectives of the NCFTA (NCFTA web-site, 2010).

Critical Infrastructure Sector Partnership Advisory Council (CISPAC)

This council is lead by the Department of Homeland Security Office of Infrastructure Protection (IP) in close coordination with public and private-sector critical infrastructure and key assets (CIKA) partners, in an effort to mitigate risk to the nation's CIKR. This council provides a framework for owner and operator members of the Sector Coordinating Councils (SCC) and Members of the Government Coordinating Councils (GCC) to engage in cooperation, information sharing, and engagement across the entire range of critical infrastructure protection activities. (National Strategy for Information Sharing, 23):

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- **Sector Coordinating Councils (SCC)**: Sector Coordinating Councils have been set up for each sector of critical infrastructure and are comprised of the owners of operators within this sector . (DHS web-site, 2010)

- **Government Coordinating Councils (GCC)**: Government Coordinating Councils are the government counterpart for each Sector Coordinating Council (SCC) to enable interagency and cross-jurisdictional coordination. The GCC comprises representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of each individual sector. (DHS web-site, 2010)

- **State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC):** The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) serves as a forum to ensure that State, Local, and Tribal homeland security partners are fully integrated as active participants in national CIKR protection efforts, and to provide an organizational structure to coordinate across jurisdictions on state and local government-level CIKR protection guidance, strategies, and programs. (DHS web-site, 2010)

- **National Infrastructure Protection Plan (NIPP)** : The National Infrastructure Protection Plan (NIPP) was developed under the authority of Homeland Security Presidential Directive / HSPD-7. This plan establishes a partnership structure for coordination across 18 CIKR Sectors, and a risk management framework to identify assets, systems, networks and functions whose loss or compromise pose the greatest risk. (DHS web-site, 2010)

The Infrastructure Security Partnership (TISP)

The Infrastructure Security Partnership (TISP) is a non-profit partnership which facilitates public and private-sector collaboration that advances the practices and policies of infrastructure security and resiliency to sustain the nation's resources and its ability to efficiently restore infrastructure when disrupted by any hazard.

At the time of its formation in 2001, the TISP consisted of eleven professional and technical organizations and federal agencies, but membership has continued to grow and now represents nearly two million individuals and firms involved in the planning, design, construction, and operation of infrastructure. Members include representatives from: local, regional, state, and federal governments; foreign agencies; professional associations and industry trade groups; engineering, architecture, and construction firms; codes and standards organizations; educational institutions and universities; planners and economic developers; infrastructure owners and operators; manufacturers; and service providers; whose main purpose is related to security and resiliency of the nation's infrastructure.

The TISP provides opportunities to its members for partnering on projects, for peers to learn from one another, for sharing relevant information during key discussions, and to

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

raise awareness among the decision makers and the general public. Activities include: quarterly technical forums, roundtable discussions and workshops, and co-sponsored events. Additionally, the TISP's communications network helps to raise awareness by showcasing the latest developments and activities in infrastructure resilience through their monthly TISP e-Newsletter and a comprehensive website. (TISP web-site, 2010)

The National Critical Infrastructure Resilience Committee (CIRC)

The Critical Infrastructure Resilience Committee (CIRC) provides a forum for interested organizations and stakeholders to focus on 'Critical Infrastructure Resilience' with an emphasis on organizational and regional risk mitigation, infrastructure management, optimization of cost effective solutions and other related areas. The first meeting was held on October 6th 2009 and the objectives for 2010 were as follows:

- Refocus and expand the original The Infrastructure Security Partnership (TISP) Guide for an Action Plan to Develop Regional Disaster Resilience to cover Critical Infrastructure resilience with emphasis on specialized needs associated with specific scenarios, such as catastrophic events, all hazards disasters and disruptions, deteriorating/aging infrastructure and weapons of mass destruction;
- Identify other organizations for potential sponsorship or collaboration on CIR events and projects ;
- Work with the federal Government Coordinating Councils to support and share information with interested federal organizations;
- Develop and conduct, an Annual Infrastructure and Regional Resilience Conference each fall that brings together the wide range or organizations interested in CIR and related aspects of resilience; and
- Work with other TISP Committees to determine ways to undertake outreach to state and local governments, private sector and other key stakeholder organizations on CIR issues, particularly the public-private collaboration and information sharing to promote and enhance resilience. (TISP web-site, 2010)

Regional Disaster Resilience: TISP Guide for Developing an Action Plan

This guide was developed by the TISP and was released in 2006. The Guide provides a Strategy to develop the necessary level of preparedness for communities to 'manage major disasters in today's complex and interdependent world'. (TISP web-site, 2010)

Regional Resiliency Assessment Program (RRAP)

In 2009 the Department of Homeland Security (DHS) developed the RRAP which 'evaluates [critical infrastructure and key resources] CIKR on a regional level to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective to identify dependencies, interdependencies, cascading effects, resiliency characteristics, and gaps. In conducting the RRAP, DHS does an analysis of a region's CIKR, protection and prevention capabilities, and focuses on (1) integrating vulnerability and capability assessments and infrastructure protection planning efforts; (2) identifying security gaps

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

and corresponding options for considerations to improve prevention, protection, and resiliency; (3) analyzing system recovery capabilities and providing options to secure operability during long-term recovery; and (4) assessing state and regional resiliency, mutual aid, coordination, and interoperable communication capabilities.

RRAP assessments are to be conducted by DHS officials, in collaboration with other federal officials; state, local, tribal, and territorial officials; and the private sector depending upon the sectors and facilities selected, as well as a resiliency subject matter expert(s) deployed by the state's homeland security agency. The results of specific asset-level assessments conducted as part of the RRAP are made available to asset owners and operators as well as other partners (as appropriate), but the final analysis and report is delivered to the state where the RRAP was conducted (GAO – Critical Infrastructure Protection, 2010, p. 16)

Site Assistance Visits (SAVs)

The SAV is a 'facility-specific "inside-the-fence" vulnerability assessment conducted at the request of asset owners and operators, and is intended to identify security gaps and provide options for consideration to mitigate identified gaps. SAVs are conducted at individual facilities or as part of an RRAP and are conducted by the [Department of Homeland Security's Office of Infrastructure Protection] [IP] assessment teams in coordination with state and local government organizations (including law enforcement and emergency management officials), asset owners and operators, and the National Guard Bureau (GAO – Critical Infrastructure Protection, 2010, p. 17-18)

3.7.7 Cyber Security Initiatives

US-CERT

US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). It is a public-private partnership charged with providing response support and defence against cyber attacks. The US-CERT interacts with Federal agencies, industry, the research community, State and Local governments, and others to disseminate reasoned and actionable cyber security information to the public (US-CERT web-site, 2010).

Assuring a Trusted and Resilient Information and Communications Infrastructure

This policy review paper was the result of a directive given by President Obama to conduct a 60-day, comprehensive, 'clean-slate' review to assess U.S. policies and structures for cyber security. Through this process, the government review team gained input from a broad cross-section of partners, including: industry, academia, the civil liberties and privacy communities, state governments, international partners and the legislative and executive branches. The key findings of this review are as follows (Whitehouse web-site, 2010):

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- 'Cyberspace underpins almost every facet of modern society;
- Dual challenges in maintaining this environment: promoting efficiency, innovation, economic prosperity and free trade while also promoting safety, security and civil liberties;
- US should take a strong leadership role;
- Government should initiate a national public awareness and education campaign;
- Cannot succeed in securing cyberspace if working in isolation: the Federal government should enhance its partnerships with the private sector;
- A strategy is needed that will shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding jurisdiction and force;
- US government needs a comprehensive framework to ensure a coordinated response by government, private sector and international allies to significant incidents; and
- US Federal government needs to articulate coordinated national information and communications infrastructure objectives with the help of private sector and academia.'

National Cyber Security Awareness Campaign Challenge

This Awareness Campaign which carries the slogan '*Stop. Think. Connect'*, was officially launched on October 4, 2010, in Seattle, Washington, as part of National Cyber-security Awareness Month. The event featured Howard Schmidt, White House Cyber-security Coordinator and Special Advisor to the President and Department Deputy Secretary Jane Holl Lute as well as other senior administration leaders, Campaign stakeholders and partners.' (DHS web-site, 2010) Under this campaign, several other campaigns have been launched to engage citizens in the fight to defend cyberspace. They are as follows:

- **Friends of the Campaign Program:** This program encourages the general public to help the DHS educate and empower the American public to take steps to protect themselves and their families online. Activities include: distributing awareness campaign materials; leading or hosting a cyber awareness activity; discussing with friends and family the importance of cyber security; informing their community about the Cyber Security Awareness Campaign and the resources available; and getting schools and community organizations involved and informed on the issue.
- **Cyber Citizen Forums:** Forums will be hosted across the US in collaboration with National Centers of Academic Excellence, at community centers, town halls, colleges and universities to prompt dialogue and inspire action.
- **Cyber Awareness Coalition:** This is coalition of organizations who have agreed to help the Department of Homeland Security to disseminate information regarding the campaign. (DHS web-site, 2010)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Cyber Storm: Securing Cyber Space 2006, 2008 and 2010

Cyber Storm is a biennial exercise aimed at strengthening cyber preparedness in the public and private sectors. This process is mandated by Congress and overseen by the Department of Homeland Security. *Cyber Storm* participants perform the following activities:

- Examines organizations' capability to prepare for, be protected from, and respond to the potential effects of cyber attacks;
- Exercises strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures;
- Validates information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information; and
- Examines the means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or National Security interests.

Each *Cyber Storm* builds on lessons learned from previous real world incidents, ensuring that participants face more sophisticated and challenging exercises every two years.

To date, this exercise has been preformed three times: in February 2006, March 2008, and September 2010 (DHS web-site, 2010).

- **Cyber Storm I - February 2006:** Cyber Storm I included 115 organizations, including federal, state and local governments and the private sector. It allowed participants to respond to a variety of simulated attacks against critical infrastructure and to collaborate at the operational, policy and public affairs levels. It focused on 4 major areas, namely: Information technology; Communications; Energy; and Air transportation.
- **Cyber Storm II - March 2008:** Cyber Storm II involved 5 countries, namely: Australia, Canada, New Zealand, United Kingdom, United States; 18 federal cabinet-level agencies; 9 states; and over 40 private sector companies (including: Juniper Networks, Microsoft, McAfee, Cisco, NeuStar, The Dow Chemical Company, Inc., PPG Industries, ABB Group, Air Products & Chemical Inc., Nova Chemical, Wachovia, etc.). For this exercise, the focus was on the processes, procedures, tools and organizations responses to a multi-sector coordinated attack through and on, the 'global cyber infrastructure'. This allowed players to exercise and evaluate their cyber response capabilities to a multi-day coordinated attack and to gauge the cascading effects of cyber disasters on other Critical Infrastructures; and to test concepts and processes developed since Cyber Storm I. The 4 infrastructure sectors tested in this exercise were as follows: information technology; chemical; communications systems; and rail and pipe transportation.
- **Cyber Storm III – September 2010**: On September 28, 2010, the DHS rolled out its third major exercise to test the US's response to cyber attack. The test lasted three days and included thousands of participants. Cyber Storm III included a

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

much higher involvement of private companies and a higher number of foreign governments. Participants in the program include numerous American federal government departments, 12 partners from foreign countries, 60 large scale private sector companies, and 11 state governments.

3.7.8 Border Protection Initiatives

Industry Partnership Program (IPP)

The goal of the Industry Partnership Program (IPP) is to engage the trade community in a cooperative relationship with the U.S. Customs and Border Protection (CBP) in the war on drugs and terrorism. The IPP proactively works with foreign manufacturers, exporters, carriers, importers, and many other industry sectors to provide for a seamless security environment throughout the entire commercial process.

Currently, U.S. Customs and Border Protection have four active IPPs that are designed to deter and prevent narcotics smuggling and terrorist activities via commercial cargo and conveyances, which are as follows (CBP web-site, 2010):

- **Carrier Initiative Program (CIP):** The CIP was established in 1984, and is a joint effort among air, sea, land and rail carriers and the U.S. Customs and Border Protection to address the problem of drug smuggling and terrorism in the United States on board commercial conveyances. By signing the CIP agreement with the U.S. Customs and Border Protection, carriers agreed to enhance their security at foreign and domestic terminals as well as on board their conveyances. Additionally, they agreed to cooperate closely with the U.S. Customs and Border Protection in identifying and reporting attempted or suspected smuggling attempts or other criminal activity. In return, CBP agrees to conduct both domestic and foreign security site surveys, post seizure analysis, and provide training to identify security weaknesses within their company and suggests improvements to better their security systems and measures (CBP web-site, 2010).

- **The Business Alliance for Secure Commerce (BASC):** The BASC is a private sector led and controlled coalition that has been supported by U.S. Customs and Border Protection (CBP) since its creation in 1996. As a non-profit organization incorporated in the State of Delaware, the BASC is an international business alliance created to promote supply chain security in cooperation with government agencies and international organizations (CBP web-site, 2010).

- **The Americas Counter Smuggling Initiative (ACSI):** The ACSI was established in 1988 by CBP, to build upon the success of CIP and BASC by strengthening and expanding the anti-narcotics and anti-terrorism security programs with industry and government. ACSI is made up of teams of CBP inspectors and agents charged with assisting business in developing their security programs and initiatives that safeguard legitimate shipments from being used as vehicles for drug smuggling or terrorist actions. The target countries are the same

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

as those where BASC chapters exist. The ACSI teams travel to each target country approximately four times a year to provide hands-on training and site surveys to BASC members in the trade industry (CBP web-site, 2010).

- **Customs-Trade Partnership Against Terrorism (C-TPAT) Program**: In 2001, CBP introduced the C-TPAT program. This program demonstrates CBP's ongoing participation in a joint effort with importers, carriers, brokers, warehouse operators, manufacturers, and other industry sectors to develop a seamless security-conscious environment from manufacturing through transportation and importation to ultimate distribution (CBP web-site, 2010).

3.7.9 Maritime Security Initiatives

Under the authority of the *Maritime Security Strategy*, the Secretaries of Homeland Security, Defence, State, Commerce, and Transportation, consult with industry representatives, to ensure national security from a maritime perspective through the following programs:

- **Maritime Infrastructure Recovery:** to develop comprehensive national maritime infrastructure recovery standards and plans, which are complementary to the national preparedness goals and standards. (DHS web-site, 2010)

- **Maritime Transportation System Security**: to make improvements to the national and international regulatory framework with respect to licensing, carriage, communications, safety equipment, and other critical systems for all private vessels, including commercial vessels, operating in the maritime domain in order to ensure national security from a maritime perspective. (DHS web-site, 2010)

- **Maritime Commerce Security**: to define supply-chain contingency plans which would ensure the continued flow of commerce in the event of an incident necessitating total or partial closure of U.S. borders to maritime commerce. (DHS web-site, 2010)

Outreach under the authority of the Small Vessel Security Strategy

The Small Vessel Security Strategy and Implementation Plan identified some existing programs and processes that the DHS could use to combat the risks posed by small vessels which include the following:

- **America's Waterway Watch:** This program is intended to serve as a tool for the maritime industries, recreational boating communities, and the public to report suspicious and unusual maritime activity via a 24-hour hotline. (DHS web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- **Citizen's Action Network:** The Citizen's Action Network also seeks to obtain the general public's active participation to report suspicious and unusual maritime activity but it differs from America's Waterway Watch in that it acquires information from vetted, trained members in addition to the general public. The Citizen's Action Network can track both the outcomes of the information provided and the degree of member participation, and therefore can evaluate the overall effectiveness of the program (DHS web-site, 2010).

3.7.10 Aviation Security Initiatives

Air Domain Surveillance and Intelligence Integration Plan (ADSII)

The ADSII Plan stipulates that any Air Strategy must include coordination with state and local government authorities and consultation with appropriate private sector persons and entities in order to have effective knowledge of threats to the United States and U.S. interests in the air domain. Therefore the U.S. Government developed this plan in order to coordinate with appropriate stakeholders on the requirements, priorities, and implementation of national air surveillance resources and the means to share information. (DHS web-site, 2010)

3.7.11 Community Outreach Initiatives

Outreach to Minority Groups by the FBI

The Community Relations Unit of the FBI and the community outreach specialists stationed around the US, work to create and strengthen relationships between the FBI and minority groups, religious and civic organizations, schools, non-profits, and other groups to dispel misconceptions, share information and ideas, and raise awareness and understanding. (FBI web-site, 2010)

Outreach to Minority Groups by the Department of Justice

The Civil Rights Division of the US Department of Justice hosts a bi-monthly meeting that brings together leaders from the Muslim, Arab, Sikh and South Asian communities with officials from the Departments of Justice, including the FBI, Homeland Security, Treasury, Transportation and State along with the Equal Employment Opportunity Commission to discuss the civil rights issues that have faced these communities since the terrorist attacks of Sept. 11, 2001. The idea behind the meeting is to bring together a wide range of federal agencies whose policies impact these communities and allow the communities to raise a range of cross-cutting issues in a single forum. Issues addressed have included hate crime prosecution, federal anti-discrimination laws, watch lists, no-fly lists, profiling by law enforcement, visa and immigration issues, among many others.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Outreach to Minority Groups by the Department of Homeland Security

The Office for Civil Rights and Civil Liberties (CRCL) Engagement Team (E-Team) conducts public outreach and engagement initiatives with American Arab, Muslim, Sikh, South Asian, Somali, Middle Eastern, and other ethnic and religious communities in eight metropolitan areas, namely: Washington, Houston, Chicago, Los Angeles, Boston, Detroit, Columbus, and Minneapolis/St. Paul.

The majority of this activity consists of leading roundtable meetings between community members and federal, state, and local government officials. The E-Team's work also includes broader outreach and engagement events in these areas, which are often linked to or associated with the community roundtables. Key initiatives of the E-Teams are as follows (DHS web-site, 2010):

- **Community Roundtables in Key Cities.** As stated above, the Office for Civil Rights and Civil Liberties hosts regular roundtable meetings with religious and community groups in the eight cities mentioned above.

- **Roundtable with Young Leaders.** The Office for Civil Rights and Civil Liberties has hosted four "Roundtables on Security and Liberty: Perspectives of Young Leaders Post-9/11" with representatives from the Arab, Muslim, Sikh, South Asian, and Middle Eastern American communities. These took place in Los Angeles (November 2008); Houston (June 2008); and Washington, DC (July 2007 and June 2008).

- **Incident Communication Coordination Team.** The E-Team manages an "Incident Community Coordination Team" that will allow the CRCL to engage with Arab, Muslim, Sikh, Middle Eastern, Somali, and South Asian American community leaders in the aftermath of any future terrorist act or homeland security incident. (Similar to Gold Groups in the UK).

- **Cultural Competency Training.** Based on recommendations from key communities, CRCL has worked to improve the cultural competency of Department of Homeland Security personnel. For example, this group developed a training DVD on basic aspects of Arab and Muslim cultures, has created a training poster on the Kirpan, a Sikh article of faith. CRCL has recently created a more formal training program for federal, state, and local law enforcement. Discussion topics include: misconceptions and stereotypes of Islam and Muslims; effective policing without the use of ethnic or racial profiling; and a best practices approach to community interaction and outreach.

- **Improving the Diversity and Critical Language Skills of the Department.** One significant aspect of CRCL's engagement effort is promoting thecivil service at job fairs, conferences, and in media outlets serving ethnic and religious communities. As a result, community leaders have begun encouraging young people in their communities to seek employment with the federal government. This has allowed the Department of Homeland Security to create the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

'National Security Internship Program', a partnership between the FBI and the Department of Homeland Security (DHS web-site, 2010).

3.7.12 Police Based Programs

Operation Cooperation

Prior to September 11, the International Association of Chiefs of Police (IACP), National Sheriffs' Association, and ASIS International (formerly the American Society for Industrial Security) joined together, with funding from the U.S. Department of Justice, to launch "Operation Cooperation," a national effort to increase collaborative efforts between the private sector, particularly private security, and state and local law enforcement agencies to address issues related to: crime-and-disorder; homeland security-related issues and the prevention of future terrorist acts. (Operation Cooperation, 2000)

Auxiliary Police Program (APP)

The APP was created in 1986, to enhance public-private security cooperation. While it started with only 30 private security organizations, it now boasts more than 1,000. Since September 11, APP's mandate has widened and taken on new importance. Since New York City is a high-priority target for terrorists, the New York City Police Department operates with APP to review police security alertness at member facilities. (Operation Cooperation document, 2000)

3.7.13 Emergency Planning Initiatives

FEMA – National Response Framework

The *FEMA National Response Framework* provides the guiding principles that enable all emergency response partners to 'prepare for and provide a unified national response to disasters and emergencies - from the smallest incident to the largest catastrophe.' The *Framework* establishes a comprehensive, national, all-hazards approach to domestic incident response (FEMA web-site, 2010).

3.7.14 International Outreach

The Overseas Security Advisory Council (OSAC)

The Overseas Security Advisory Council is a Federal advisory committee that promotes security cooperation between American business and private sector interests worldwide. It currently encompasses a 34-member core Council, an Executive Office, over 100 Country Councils, more than 3,500 constituent member organizations and 372 associates (NSIS 2007: 23).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

3.7.15 Transparency and Open Government Initiative

Upon taking office in December 2009, President Obama's first order of business was to announce the Open Government Initiative in his *Transparency and Open Government Speech.* In this speech, President Barack Obama stated the following (Whitehouse web-site, 2010):

> "My Administration is committed to creating an unprecedented level of openness in Government. We will work together to ensure the public trust and establish a system of transparency, public participation, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government."

Open Government Directive

With this speech, President Obama announced the launch of the *Open Government Directive* which initiated the following;

- Launched the open government web-site;
- Mandated all federal government departments to reevaluate their programs to find new ways to increase their transparency and accessibility;
- Mandated all federal government departments to draft and release their own Open Government Plans within 120 days ;
- Launched Data.gov website which provides for data to be made publicly accessible; and
- Called upon on the Chief Technology Officer and Chief Information Officer to create an Open Government Dashboard to track the progress of each department in meeting these objectives and to provide a hub where all Open Government Plans could be stored and accessed. (Open.gov web-site, 2010)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

4.0 Citizen Engagement in National Security Issues in Australia

The release of National Security Strategies in Australia is a fairly recent phenomenon, beginning with the release of the first *Defence Policy Statement* in 1998. However, since the turn of the century, there have been a great deal of documents released by the Australian government to date in order to inform the general public and partnerships have been formed with members of industry and academia in order to address issues of National Security. Therefore a brief overview of these documents and programs will be provided as follows:

1) This section will begin with an overview of the National Security Strategies and documentation which have been released at date aimed at combating terrorism;
2) Followed by an overview of the Australian Information Strategy; and finally
3) Will conclude with a brief description of the programs which have been enacted in Australia with the purpose of informing, consulting or to encourage active participation among its citizenry grouped by topic.

4.1 The History of National Security Strategies in Australia

As noted previously, this body of this paper will merely provide a brief overview of the statements and strategies which have been released. A list of which has been attached below in order of issuance.

- *Defence and Industry Strategic Policy Statement of June 1998;*
- *The Defence White Paper of 2000;*
- *The Defence White Paper of 2003;*
- *Critical Infrastructure Protection National Strategy 2004;*
- *Protecting Australia Against Terrorism of 2004;*
- *The Defence White Paper of 2005;*
- *Protecting Australia Against Terrorism of 2006;*
- *The Attorney General's Portfolio Security Environment Update (2007/2008);*
- *The Defence and Industry Policy Statement of 2007;*
- *The Defence White Paper of 2007;*
- *The National Security Statement of 2008;*
- *Good Security –Good Business booklet (2008);*
- *The Defence White Paper of 2009;*
- *The 2009 Defence Capability Plan: Public Version (2009);*
- *The Strategic Reform Program – Delivering Force 2030 (2009);*
- *The Cyber Security Strategy: Securing Cyberspace (2009);*
- *The National Security Science and Innovation Strategy (2009);*
- *The National Security Science and Innovation Directory (2009);*
- *The Lexicon of Terrorism (2009);*

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- *The National Aviation Policy Statement (2009);*
- *The Countering Violent Extremism in Our Community Media Release (2010); and*
- *Protecting Australia Against Terrorism* of 2010

Defence and Industry Strategic Policy Statement – June 1998

This Policy Statement referred to working with industry as 'a fundamental component' of the protection of national security. The ultimate goal is for the Department of Defence to 'work with industry together as partners to maintain National Security and a truly sustainable defence industry base' and it outlined the Australian Government's vision for change and improvement, which were as follows: integrate industry into capability development; enhance industry's contribution to the nation's capability edge; reform procurement procedures; establish new ways to involve Australian industry in Defence business; increase Australian exports and materiel cooperation; and commit to cultural change and improved communication (Australian DOD web-site, 2010).

Defence White Paper of 2000, 2003, 2005 and 2007

The first *Defence White Paper* released to the pubic by the Australian government was issued in the year 2000. In this White Paper the Australian government committed to review of its defence posture periodically to ensure Australia continued to have "the appropriate mix of concepts, capabilities and forces to meet new challenges as they arise" (Australian DOD web-site, 2010).

Just over two years later (2003) the Australian government released a new Defence White Paper, which focused on the development of capabilities for the Defence of Australia in two major areas: terrorism and the spread of Weapons of Mass Destruction.

The second update to the *Defence White Paper* of 2000 was released in 2005. This version outlines the following: provides an overview of previous successive reviews of global and regional security issues; describes Australia's strategic environment at present; provides an evaluation of the challenges which were facing the Australian government at the time; and finally describes the measures that the Department of Defence plans to put into place in order to respond.

The 2007 version of the Defence White paper was a further update to the previous iterations and provided detail on the following: lessons learned from recent initiatives; Australia's strategic environment at the time of issuance; evaluate the challenges which were facing the Australian government at the time; and finally described the measures that the Australian Department of Defence planned to take in order to respond (Australian DOD web-site, 2010)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Critical Infrastructure Resilience Strategy (CIRS) of 2004 and 2010

The 2004 CIRS Strategy was intended to provide an overarching statement of principles for Critical Infrastructure Protection in Australia, and outlined the major tasks and the actors responsible in pursuit of these principles. This strategy was used by both the Australian government and the owners and operators of infrastructure and provided guidance for the medium term in the implementation of plans by governments and industry sectors.

This strategy was updated in July of 2010 and the latest version recognizes that the best way to enhance the resilience of critical infrastructure is to partner with owners and operators to share information, raise the awareness of dependencies and vulnerabilities, and facilitate collaboration since the majority of critical infrastructure operations are privately owned. This strategy has six complementary strategic imperatives to build critical infrastructure resiliency (CIR) and achieve the Australian Government's aim and objectives:

- Operate an effective business-government partnership with critical infrastructure owners and operators;
- Develop and promote an organizational resilience body of knowledge;
- Assist owners and operators of critical infrastructure to identify, analyze and manage cross-sectoral dependencies;
- Provide timely and high quality policy advice on issues relating to critical infrastructure resilience;
- Implement the *Australian Government's Cyber Security Strategy* to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators, and
- Support the critical infrastructure resilience programs delivered by Australian States and Territories, as agreed and as appropriate. (Australian Attorney General's web-site, 2010)

White Paper: Protecting Australia against Terrorism 2004, 2006 and 2010

The White Paper *Protecting Australia Against Terrorism* was first released in 2004 and has been updated twice since then, in 2006 and in 2010. *The Protecting Australia Against Terrorism* series of White Papers provide an overview of Australia's domestic and international counter-terrorism strategy.

The 2006 version of *Protecting Australia Against Terrorism* was comprised of two parts. Part I describes Australia's national counter-terrorism strategy. Part II, provides functional details about Australia's national counter terrorism capabilities.

The 2010 Strategy included four key elements:

- **Analysis**: an intelligence-led response to terrorism driven by a properly connected and properly informed national security community;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- **Protection:** taking all necessary and practical action to protect Australia and Australians from terrorism at home and abroad;
- **Response:** providing an immediate and targeted response to specific terrorist threats and terrorist attacks should they occur; and
- **Resilience:** building a strong and resilient Australian community to resist the development of any form of violent extremism and terrorism on the home front. (Australian Department of Prime Minister and Cabinet web-site, 2010)

Attorney General's Portfolio Security Environment Update of 2007/08

This update was given by the Australian Attorney General in 2007. During this speech, he reiterated that the public plays a "crucial role in protecting Australia against terrorism and that counter terrorism efforts cannot succeed without the assistance of well informed and engaged Australians. Information from the public could prove vital to law enforcement and intelligence officers by providing the breakthroughs needed to disrupt terrorist activities" (Australian Attorney General's web-site, 2010).

National Security Statement of 2008

On December 4th, 2008, the Prime Minister delivered Australia's inaugural *National Security Statement* to the Parliament. The Statement outlined five enduring National Security interests that constitute the Australian Government's National Security objectives. They are as follows (DPMC web-site, 2010):

- Maintaining Australia's territorial and border integrity;
- Promoting Australia's political sovereignty;
- Preserving a cohesive and resilient society and strong economy;
- Protecting Australians and Australian interests both at home and abroad, and
- Promoting a stable, peaceful and prosperous international environment, particularly in the Asia Pacific region, together with a global rules-based order which enhances Australia's national interests.

Good Security – Good Business

In 2008 the Australian Government released the *Good Security-Good Business* booklet. This booklet emphasizes the importance for small and medium sized businesses to be 'prepared to deal with a range of hazards, including terrorism, and the value of having risk management and business continuity plans in place and enables companies to respond and recover as quickly as possible' and provided business with the information necessary to ensure this preparedness (Australian Attorney General's web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The 2009 Defence White Paper- Protecting Australia in the Asian Pacific Century Force 2030

This new *Defence White Paper,* which was released in 2009, explained how the Government planned to strengthen the foundations of Australia's defence. It sets out the Government's plans for Defence for the next few years, and how it will achieve those plans (Australian DOD web-site, 2010).

2009 Defence Capability Plan (DCP): Public Version

The purpose of disseminating this document was to provide an account of Major Capital Equipment proposals that are currently planned for the Australian Government's consideration for the 2009-2013 time period. This document was first released in July of 2009, and an updated document was released in February of 2010. (Australian DOD web-site, 2010)

The Strategic Reform Program of 2009 – Delivering Force 2030

The *Strategic Reform Program* aimed at improving efficiency and effectiveness of the Australian Defence Force (ADF) by identifying areas which could be cut so that these resources could be reinvested in other areas. This program has three key elements:

- **Improved Accountability in Defence**: providing much greater transparency;
- **Improved Defence Planning**: improving strategic and corporate level planning; and
- **Enhanced Productivity in Defence:** by implementing smarter, more cost effective business processes and practices.

This project is overseen by the *Defence Strategic Reform Advisory Board,* which is chaired by an independent professional, external to the Department of Defence and includes a balance of government and non-government professionals. (Australian DOD web-site, 2010)

National Aviation Policy Statement

On December 16, 2009 the Australian Government released the first *National Aviation Policy*. This policy statement brought together all strands of aviation policy into a single, forward-looking document providing planning, regulatory and investment certainty for the aviation industry out to 2020 and beyond. (Australian Department of Infrastructure and Transport web-site, 2010)

Cyber Security Strategy – Securing Cyberspace

On November 23, 2009, the Attorney-General of Australia launched the first ever Australian Cyber Security Strategy entitled: *Securing Cyberspace*. This new Strategy outlines the security challenges which are related to the Internet and explains how the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Australian government plans to address them. In addition to this Strategy, a brochure has also been produced for home users and small businesses (Australian Attorney General's web-site, 2010).

National Security Science and Innovation Strategy of 2009

The Australian government launched the *National Security Science and Innovation Strategy* (NSSIS) in November of 2009. The goal of the NSSIS is to enhance the application of science and innovation to National Security, including counter-terrorism efforts. The NSSIS builds on the expertise and capabilities available within Australian government agencies, universities and private sector organisations to ensure that Australia's National Security science and innovation efforts are informed and prioritized to reflect the areas of greatest need. (Australian Department of Prime Minister and Cabinet (DPMC) web-site, 2010)

The National Security Science and Innovation Directory (NSSID)

This directory, which was released at the same time as the NSSIS, provides a brief description of the organisations and coordination mechanisms relevant to National Security-related science and innovation (Australian Department of Prime Minister and Cabinet web-site, 2010).

Lexicon of Terrorism

The project, which was launched in July of 2009, looks at the impact of terrorism-related language on government relations with select minority groups. The goal of this project was to provide a document compiling socially acceptable terminology to be used by government officials when speaking about terrorism-related issues so as not to inadvertently glorify terrorism or conversely to alienate ethnic or religious groups. This project is led by Victoria Police, in partnership with the Victorian Department of Premier and Cabinet, the Australian Multicultural Foundation and the Commonwealth Attorney-General's Department (AAG web-site, 2010).

Countering Violent Extremism in Our Community

On May 11th, 2010 the Australian Attorney General, announced that an additional $9.7 million will be invested in combating violent extremism in Australia. This budget will be distributed between the National Counter-Terrorism Committee; the Diversity and Social Cohesion program the Australian Human Rights Commission and the Department of Foreign Affairs. The priorities for these programs have been specified as the following (AAG web-site, 2010):

- Identifying and diverting people at risk of violent extremism;
- Supporting rehabilitation and de-radicalisation programs conducted by State and Territory police and correctional services;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Engaging with communities to improve social cohesion and resilience, including through local meetings and focus groups;
- Developing mentoring programs for 'at risk' youth in partnership with relevant community groups;
- Examining the role of the Internet in the radicalisation process; and
- Improving responses to violent extremist messages and ensuring they are evidence-based and appropriate to Australian circumstances.

4.2 National Information Sharing Strategy

Information Strategy in Australia - Defence Information and Communications Technology Strategy (ICT) 2009

The ICT Strategy was developed to address shortcomings in governance, planning and control frameworks for ICT (Australian Government Department of Defence 2009). To achieve these objectives this strategy is based on four strategic imperatives:

1) Optimise the value of Defence's ICT investment through cost transparency, improved stakeholder communication, prioritisation of spending and efficiency in ICT activities;
2) Closer alignment with stakeholders through a stakeholder-centric organisation model;
3) Provide agreed, priority solutions through the establishment of a Defence-wide ICT Operating Model and Enterprise Architecture promoting standardisation and consolidation; and
4) Strengthen ICT capabilities through improvements to culture, leadership, processes, skills, sourcing and resource planning (Australian Government Department of Defence 2009, 5).

A graphical representation of Australia's ICT defence strategy can be found on page 6 of the document *Defence Information and Communications Technology Strategy 2009*, which can be found at:
http://www.defence.gov.au/publications/DefenceICTStrategy2009.pdf.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

4.3 Outreach Programs by Type

Below is a list of the outreach programs which could be located to date, initiated by the Australian government in order to engage their citizens in issues related to national security. As with the United States, these outreach programs have been organized by type and then by date.

4.3.1 National Security Initiatives - General

National Security Adviser (NSA)

The *National Security Adviser* provides direct advice to the Prime Minister on policy matters relating to the nation's security, including international policy issues. This involves engagement with the relevant Commonwealth Ministers, heads of departments and agencies at the Commonwealth and State and Territory levels, as well as key representatives from business, industry and academia. The NSA's duties also include:

- Developing effective partnerships within the national security community;
- Improving the national security community's strategic direction;
- Supporting whole-of-government security policy development and crisis response;
- Overseeing the implementation of all national security policy arrangements;
- Promoting a cohesive national security culture; and
- Leading the *National Security and International Policy Group* within the Department. (Department of the Prime Minister and Cabinet (DPMC web-site, 2010)

National Security Public Information Campaign

The *National Security Public Information Campaign* kicked off in 2002, with the launch of the *National Security Hotline* and the set up of the *Every Piece of Information Helps* web-site. This campaign encourages the Australian public to remain vigilant and report possible signs of terrorist activity to the National Security Hotline. To this end, it has launched many advertising campaigns on radio and television since its inception in order to encourage citizens to become involved. For more information on the National Security Hotline, please see below (Australia's National Security web-site, 2010).

National Security Hotline

The National Security Hotline commenced operations on December 27, 2002. The Hotline operates 24 hours a day, seven days a week, and allows members of the public to report any suspicious or unusual activity or behaviour. Information provided to the Hotline is passed on to relevant police and security agencies.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The first phase of the National Security Public Information Campaign called '*Let's Look Out For Australia'* was launched in December 2002. It used television, radio and press advertising to give the public information on what the Australian Government was doing to protect Australia against terrorism. The campaign also involved the distribution of the *Let's Look Out For Australia* booklet to which was distributed to 7.8 million Australian households.

The second phase of the campaign, *Every Piece of Information Helps*, was launched in September 2004 to remind Australians about the National Security Hotline that was discussed above (Australia's National Security web-site, 2010).

National Research Infrastructure Council

The *National Research Infrastructure Council* (NRIC) was formed in 2009, to provide strategic advice on future research infrastructure investments, including those to be funded through the *Super Science Initiative*. This Council is made up of leading researchers from across a wide range of research disciplines and provides strategic planning and mapping across all categories of research infrastructure and contribute policy advice to the government. It facilitates coordination across different levels of investment in research infrastructure from institutional to national and landmark and provides advice to the *Education Investment Fund Advisory Board* (NRIC web-site, 2010).

4.3.2 Defence-Related Initiatives

Capability and Technology Demonstrator Program (CTD)

The CTD program was established in 1997 as a result of the Defense Efficiency Review. The aim of the program was to provide an opportunity for the Australian Department of Defense to collaborate with industry to provide the government with 'capability advantages' (Australian DOD web-site, 2010).

Rapid Prototyping, Development and Evaluation (RPDE) Program

The Rapid Prototyping, Development and Evaluation (RPDE) Program is a collaborative venture between the Australian Department of Defence, industry and academia. It aims to enhance the Australian Defence Force (ADF) war fighting capacity through accelerated capability change in the Network Centric Warfare environment, through a cooperative think tank (Australian DOD web-site, 2010).

Defence Science Access Network (DSAN)

The *Defense Science Access Network* (DSAN) has been established to encourage more collaboration between industry, particularly small and medium-sized enterprises (SMEs) and *Defense Science and Technology Organization* (DSTO). Through this network, the DSTO engages with industry through a range of commercial and collaborative

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

arrangements that: build strong working relationships, provide industry access to DSTO research, facilities and expertise, and allow the transfer to industry of DSTO intellectual property for commercialization through the Business and Commercialization Office.

In collaborating with industry, DSTO meets the following objectives:

- To assist industry to become better able to support the capabilities needed to defend Australia and contribute to national wealth; and
- To enhance Defense capabilities by working with industry, universities, and other research organizations. (DSTO web-site, 2010)

4.3.3 Science and Technology Initiatives

The Prime Minister's Science, Engineering and Innovation Council (PMSEIC)

The Prime Minister's Science, Engineering and Innovation Council (PMSEIC) was established in 1997 and the mandate of this Council is to act as the Government's principal source of independent advice on issues in science, engineering and innovation and relevant aspects of education and training. The Council meets twice a year, to discuss major national issues in science, engineering and technology (Australian Department of Innovation, Industry, Science and Research (DIISR) web-site, 2010).

National Security Science and Innovation Advisory Board (NSSIAB)

The *National Security Science and Innovation Advisory Board* provides senior members of the national security and science and innovation communities with a Forum to engage with each other and discuss issues. Members include senior industry, university and research institute representatives to offer independent feedback on national security science and innovation. The Board meets annually and includes senior representatives from the government and is chaired by the National Security Adviser. (DPMC web-site, 2010)

4.3.4 Critical Infrastructure Initiatives

Business-Government Ministerial Forum- June 2004

This forum was held in June of 2004, and the purpose of the forum was to strengthen the partnership between business and government with the ultimate goal of protecting Australia from attacks to critical infrastructure. It was the first opportunity for most senior leaders of key sectors of Australian business to come together in an open forum to discuss security issues face-to-face with senior Government ministers.

Business leaders expressed a strong desire to continue engaging directly with government on national security issues and the *Business-Government Advisory Group* on National Security was established as a result (Emergency Management Australia (EMA) web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Business Government Advisory Group on National Security

This advisory group, which was formed as a result of the *Business-Government Ministerial Forum* of 2004, is chaired by the Australian Government Attorney-General and has a number of other senior Ministers also representing the Australian government. Members are drawn from leaders of major business whose companies or organisations are responsible for significant infrastructure assets. This allows these industry leaders to advise the government on a broad range of national security issues and complements the strategic objectives of the *Critical Infrastructure Advisory Council* and the *Trusted Information Sharing Network* (Australian Attorney General web-site, 2010).

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)

The TISN is a forum where the owners and operators of critical infrastructure-related companies/businesses work together and share information on the security issues that affect them. It provides an environment where industry and government can share vital information. As part of this network the Australian government has created 9 *Infrastructure Assurance Advisory Groups*, one for each sector which has been identified as being part of 'Critical Infrastructure'. For more information on these groups please see the IAAG section below (TISN web-site, 2010).

Trusted Information Sharing Network (TISN) web-site

In addition to providing information regarding the aforementioned groups, this web-site contains a wealth of information for businesses and the general public to help protect themselves against a terrorist attack and to keep them informed of developments. Publications found on the TISN web-site are as follows (among others):

- CIP Modelling & Analysis Program;
- Computer Vulnerability Assessment Program;
- Cyberstorm final report;
- CIP Newsletters;
- E-Security National Public Policy Statement;
- CIP Fact sheets;
- GovCert Fact sheets; and
- Wireless security information.

Infrastructure Assurance Advisory Groups (IAAG)

IAAG groups have been formed for the following sectors:

- *Banking and Finance Infrastructure Assurance Advisory Group;*
- *Communication Sector Infrastructure Assurance Advisory Group;*
- *Emergency Services Infrastructure Assurance Advisory Group;*

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- *Energy Infrastructure Assurance Advisory Group;*
- *Food Chain Infrastructure Assurance Advisory Group;*
- *Health Infrastructure Assurance Advisory Group;*
- *Mass Gatherings Infrastructure Assurance Advisory Group;*
- *Transport Infrastructure Assurance Advisory Group;* and
- *Water Services Infrastructure Assurance Advisory Group.*

Critical Infrastructure Advisory Council

The *Critical Infrastructure Advisory Council* is part of the *Trusted Information Sharing Network for Critical Infrastructure Protection.* This Council oversees the work of *Infrastructure Assurance Advisory Groups* and *Expert Advisory Group*, and advises the Attorney-General on the national approach to critical infrastructure protection. Council members from this group consist of members from each of the *Infrastructure Assurance Advisory Groups*, officials from each of the States, representatives from the *National Counter-Terrorism Committee* and all other relevant Australian government agencies (TISN web-site, 2010).

IT Security Expert Advisory Group

The *IT Security Expert Advisory Group* provides advice on technical solutions to problems identified by the nine *Infrastructure Assurance Advisory Groups*, and identifies emerging trends that have the potential to impact on all industry sectors (TISN web-site, 2010). Please see the following website for a graphic representation of the way in which Australia's Trusted Information Sharing Network has been organized: http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(E794A048FF84C896A06E1D7EC63DF5A4)~TISN+diagram+Dec+07.pdf/$file/TISN+diagram+Dec+07.pdf.

Critical Infrastructure Protection Modelling and Analysis Program (CIPMA)

The *Critical Infrastructure Protection Modelling and Analysis Program* (CIPMA) is a business-government partnership, which delivers strategic support to decision-makers regarding issues related to: critical infrastructure protection, counter-terrorism strategies and emergency management, especially with regard to prevention, preparedness and planning, and recovery (Australian Attorney General web-site, 2010).

ASIO's Business Liaison Unit (BLU)

The *Australian Secret Intelligence Organization (ASIO) Business Liaison Unit (BLU)* was established in late 2005 to provide "an interface between Australian businesses as the Australian intelligence community. The BLU aims to ensure that owners and operators of critical infrastructure and other relevant members of the Australian business community can access timely information on matters affecting the security of the assets and staff for which they are responsible"(ASIO web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

4.3.5 Cyber Security Initiatives

Computer Network Vulnerability Assessment Program

The *Computer Network Vulnerability Assessment Program* (CNVA) was instituted to help Australian organisations that own or manage critical infrastructure to test the security of their computer networks and systems to identify and resolve potential security threats (TISN web-site, 2010).

Australian Internet Security Initiative

The Australian Communications and Media Authority (ACMA) developed the *Australian Internet Security Initiative* (AISI) to help address the emerging problem of compromised computers (sometimes referred to as 'zombies', 'bots', or 'drones'). The AISI was originally piloted in November 2005 with six Australian ISPs, namely: BigPond, OptusNet, Westnet, Uecomm, Pacific Internet and West Australian Networks.

Following an evaluation of the pilot in mid-2006, an extended rollout of the AISI was announced in October 2006 involving an additional 19 ISPs. Some of these ISPs subsequently merged and new ISPs continue to join the AISI, and at present has a total of 78 members (ACMA web-site, 2010)

CERT Australia

The Australian Government bought together Australia's *Computer Emergency Response Team* (CERT) and made arrangements to create a new government operated national CERT, named CERT Australia. CERT Australia, which was announced in November 2009, builds on the work of *Go.cert.au* and is the national coordination point for providing cyber security information and advice to all Australians. It is also the central point of contact for international agencies to notify Australia regarding cyber security issues. CERT Australia is expected to be fully operational by July 2010 (CIRNews, Vol. 7, No1, March 2010).

4.3.6 Community Outreach Initiatives

Prime Minister's meeting with leaders of Australia's Muslim Communities

Following the terrorist attacks in London, the Prime Minister met with leaders of Australia's Muslim communities on August 23, 2005 in order to build an action plan in order to 'improve social cohesion and community harmony' in Australia. Following the meeting, the Prime Minister issued a *'Statement of Principles'* that commits all Australians to work together to protect Australia from extremism and promote tolerance, harmony and understanding. It was also agreed that the Commonwealth would seek the cooperation of the state and territory governments in working towards a national strategy

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

to reinforce social cohesion and combat extremism (Council of the Australian Governments (COAG) web-site, 2010).

Muslim Community Reference Group

In September 2005, the *Muslim Community Reference Group* was established for a one year term to advise the government on Muslim community issues. This group worked with the Australian government in order to identify ways to improve cohesion within Australian society and to also "address radicalisation and extremism". This reference group included seven sub-groups. These subgroups each came up with proposals which were combined into one report. An interim report was released in April 2006 and the final was released in September 2006, entitled: *Building on Social Cohesion, Harmony and Security: An Action Plan by the Muslim Community Reference Group* (Department of Immigration and Citizenship web-site, 2010).

The National Muslim Youth Summit – and Summary Report

The *National Muslim Youth Summit* was held on December 3rd and 4th, 2005, in Sydney. This Summit provided an opportunity for Muslim youth to provide input into the development of the N*ational Action Plan to Build Social Cohesion*. The idea to hold an event of this kind came from the *Muslim Community Reference Group (MCRG)*. Participants of the Summit identified a range of key issues facing young Muslims in Australia and generated 51 solutions. These solutions were included in *Summary Report* which was released in December of 2007 (Department of Immigration and Citizenship web-site, 2010).

Building on Social Cohesion, Harmony and Security: An Action Plan by the Muslim Community Reference Group

The final version of this document was released in September of 2006 and it provides recommendations for government initiatives in order to combat radicalization and extremism as a method of preventing terrorism. Proposals for new programs were grouped into the following categories (Department of Immigration and Citizenship web-site, 2010):

- Volunteering and Leadership;
- Muslim Community Volunteering in Emergency Management;
- Helping Law Enforcement to Address Discrimination;
- Helping Young People to Deal with Discrimination;
- Registration of Imams and Benchmarking of Religious Leadership Skills;
- Recommendation for a Booklet Outlining the Role, Position and Rights of Muslim Women;
- International Literature on Rigid Thinking;
- Crisis Management Workshops;
- Security in Government Conference;
- Emergency Management; and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Engaging with Converts to Islam.

Grants for Living in Harmony

The *Living in Harmony Fund* for community projects program provides additional resources for non-profit organisations that develop projects to help build positive community relations in a culturally diverse society. This program also funds community projects that respond to specific and emerging issues of cultural, racial and religious intolerance (Department of Immigration and Citizenship web-site, 2010).

4.3.7 Aviation Security Initiatives

Aviation Security Advisory Forum

The *Aviation Security Advisory Forum* (ASAF) is a Forum for senior representatives from industry and government to share and discuss views on aviation security matters of an operational, legal, policy and regulatory nature. The Forum is supported by the Office for Transport Security within the Department of Infrastructure and Transport (DIT). (DIT web-site, 2010)

Regional Industry Consultative Meeting (RICM)

The purpose of the *Regional Industry Consultative Meeting* (RICM) is to facilitate discussion between industry and government on issues related to aviation security. There is a web-site which has been set-up for this that is accessible only to members (Chemical Security web-site, 2010).

4.3.8 Chemical Security Initiatives

Chemicals of Security Concern Campaign

On December 3rd, 2009 the Australian Government launched the *Chemicals of Security Concern Campaign*. The premise behind this campaign is that there are many household chemicals which have legitimate uses, but can also have potentially dangerous uses if in the hands of a terrorist. Therefore, the Australian government launched a campaign which targets both industry and the general public to raise awareness of this issue and a hot-line for citizens and businesses alike to report suspicious activity (Chemical Security web-site, 2010).

Chemical Security Management Framework

In October 2008, the *Chemical Security Management Framework* was established. This Framework is intended to reflect the needs and interests of the community, industry and government and provide an effective national system to manage the use of chemicals. The aim is to provide a structured process that will continue to enhance the security of chemicals and is proportionate to the assessed risk of these chemicals in order to help

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

security and law enforcement agencies prevent terrorist acts, while not affecting the ordinary use of these chemicals (Chemical Security web-site, 2010).

National Industry Reference Group on Chemical Security (NIRG)

This group was developed as part of the *Chemical Security Management Framework* and the role of the NIRG is to provide industry advice and assistance to Australian governments on issues related to chemical security. Advice provided by the NIRG will assist in any response required to chemicals of security concern identified during risk assessment (Chemical Security web-site, 2010).

4.3.9 Emergency Management Initiatives

Working Together to Manage Emergencies Initiative

This initiative was launched in 2005 and ended in June of 2008. Through this initiative, the Australian Government provided grants for programs which supported communities, local governments and volunteer organisations to improve community safety and training for volunteers involved in emergency management (EMA web-site, 2010).

National Disaster Resilience Framework

The aim of this framework which came into effect in November 2008 is to put in place support measures to strengthen communities, individuals, businesses and institutions in order to minimise the adverse effects of disasters. This improves the ability to *Prevent, Prepare, Respond to and Recover (PPRR)* from disasters across social, economic, environmental and governance elements (Australian Attorney General's web-site, 2010).

New Emergency Alert System – Emergency Alert

On December 4, 2009, the Australian government launched the new National Emergency Warning System called *Emergency Alert.* This system can deliver up to 1,000 voice messages a minute to landlines and 300 text messages a second to mobile phones and is available 24/7 (Emergency Alert web-site, 2010).

Security Is Your Business – New Security Awareness CD

This new awareness CD was launched at the *Security Professionals Function* on December 9, 2009, and it provides professional, constructive security advice from some of Australia's top experts to be used by businesses in the development of their security strategies. It addresses security issues, risk management and resilience to help businesses better understand the security issues they should consider when specifying their security requirements. This CD was sponsored by the Australian government (Australian Attorney General's web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Emergency Pantry List

Emergency Management Australia (EMA) has set up a web-site to provide information and advice on how to stock your pantry in the event of an emergency. This site provides recommendations on the type of supplies that a family should have on hand in the event of an emergency which interrupts the supply of water, electricity or food supply. (EMA web-site, 2010)

000264

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5.0 The Influence of the European Union on Member States

Following the terrorist attacks in Madrid, the European Council began to examine the interdependencies of Member States in terms of critical infrastructure and called on Members States to develop action plans to protect critical infrastructure not only within their borders but also identify potential threats which would also involve at least one other Member State.

Since this Declaration was made by the Council in March of 2004, all Member States have participated in the development of several initiatives aimed at protecting European infrastructure. Information regarding these programs has been provided below. Even though the United Kingdom and the Netherlands are part of the European Union and are included in this section, they each also have their own section.

The European Council Declaration -March 2004

The European Council Declaration of March 25, 2004 set out the following seven strategic objectives for the *EU's Action Plan Against Terrorism*:

1) To deepen the international consensus and enhance international efforts to combat terrorism;
2) To reduce the access of terrorists to financial and economic resources;
3) To maximise the capacity within EU bodies and Member States to detect, investigate and prosecute terrorists and to prevent terrorist attacks;
4) To protect the security of international transport and ensure effective systems of border control;
5) To enhance the capability of the European Union and of member States to deal with the consequences of a terrorist attack;
6) To address the factors which contribute to support for, and recruitment into, terrorism; and
7) To target actions under EU external relations towards priority Third Countries where counter-terrorist capacity or commitment to combating terrorism needs to be enhanced.

In response to the above plan of action being put into force, about 150 actions were attached to these strategic objectives, many of which were accomplished by the deadlines provided. This plan also mandated this action plan to be reviewed twice a year, beginning in December of 2004. (Council of the European Union web-site, 2010)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The European Programme for Critical Infrastructure Protection (EPCIP)

In June of 2004, the European Council asked the Commission to prepare an overall strategy to protect "European infrastructure" i.e. the entire critical infrastructure within the European Union as a whole since they are interrelated and interdependent. In response, the Commission issued a *Communication on Critical Infrastructure Protection in the Fight Against Terrorism Memorandum* to all member states in October of 2004, putting forward clear suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures.

The Commission then organized two seminars to invite all Member States (MS), to submit their ideas; the first of which was held on June 6th and 7th of 2005. Following this seminar, the Member States provided the Commission with relevant background papers concerning their approach to critical infrastructure protection, and commented on the ideas discussed at the seminar. The 2nd EU CIP seminar was held on September 12 and 13th, in order to advance the discussion on CIP issues. Both Member States and industry associations participated in this deminar. As a result the Commission decided to put forward this green paper outlining the options for EPCIP (Council of the European Union web-site, 2010).

The EPCIP Green Paper - 2005

The main objective of the green paper was to receive feedback concerning the possible EPCIP policy options. Feedback was requested from a broad number of stakeholders including: the owners and operators of infrastructure, professional bodies and industry associations in cooperation with all levels of government (Council of the European Union web-site, 2010).

Report results of the EPCIP green paper consultation: responses of the member states

This report was a synopsis of the official responses provided by the Member States of the European Union to the *EPCIP Green Paper* consultation process which was released in February 2006. (Council of the European Union web-site, 2010)

EPCIP Framework

The EPCIP Framework which was developed as a result of the *EPCIP Green Paper* consultation process is defined as an 'all-hazards approach to responding to threat from terrorism'. The EPCIP framework consists of:

- A procedure for the identification and designation of *European Critical Infrastructure (ECI);*
- A common approach to the assessment of the needs to improve the protection of such infrastructures;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Measures designed to facilitate the implementation of the EPCIP;
- Support for Member States concerning *National Critical Infrastructures* (NCI) which may optionally be used by a particular Member State; and
- Contingency planning. (Council of the European Union web-site, 2010)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

6.0 Citizen Engagement into National Security Issues in the United Kingdom

A major shift has occurred in the United Kingdom's approach to citizen engagement programs since this report was completed. As such, it is important to note that the information below reflects only a snapshot in time.

Since the development of the CONTEST Strategy in 2003, the United Kingdom has been proactively involving their citizens in issues related to national security. Therefore, the structure of this section will be as follows:

1) A brief overview of the National Security Strategies and documentation which have been released at date aimed at combating terrorism;
2) An overview of the United Kingdom's Defence Information Strategy; and finally
3) A brief description of the programs which have been enacted in the United Kingdom with the purpose of informing, consulting or to encourage active participation among its citizenry.

6.1 The History of National Security Strategies in the United Kingdom

Below is a list of the national security strategies and documentation which has been released to date by the United Kingdom in order to: inform or engage their citizens or members thereof. Form more information on any one document; please see the reference section (or the source link) to view the document in its entirety. Here is the list of documents which will be referenced in this paper, in order of issuance:

- *The CONTEST Strategy of 2003;*
- *Security in an Interdependent World;*
- *The Prevent Strategy: A Guide for Local Partners in England;*
- *Preventing Violent Extremism: A Strategy for Delivery;*
- *Self-assessing Local Performance against NI 35:*
- *Working Together to Protect Crowded Places;*
- *Safer Places: A Counter Terrorism Supplement;*
- *Security for the Next Generation: the National Security Strategy;*
- *Cyber Security Strategy;*
- *Eliminating World Poverty: Building a Common Future;*
- *Road to 2010;*
- *Learning Together To Be Safe;*
- *Strategic Framework and Policy Statement of 2010;*
- *Adaptability and Partnership – Defence Green Paper;*
- *Yearly Update on the CONTEST Strategy;*
- *Protecting Europe Against Large-Scale Cyber–Attacks;*
- *National Risk Register;*

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- *Prevent: A Communications Guide;*
- *Channel: Supporting Individuals Vulnerable to Recruitment:*
- *Social and Behavioural Science Booklet;*
- *The UK CBRN Terrorism Strategy;*
- *Response to Lord Carlisle's Annual Report on the Prevention and Terrorism Act;*
- *Report by the Joint Committee on Human Rights; and*
- *Preventing Violent Extremism: Sixth Report of 2009-10.*

CONTEST Strategy of 2003 and 2009

Since early 2003, the United Kingdom has a long-term Strategy for countering international terrorism known as the CONTEST Strategy. The CONTEST Strategy is overseen at Ministerial level by the Cabinet Committee on National Security, International Relations and Development (NSID), which is chaired by the Prime Minister.

The CONTEST Strategy is organized around four pillars. They are as follows:

- ***Pursue***: Under the authority of this pillar, new legislation is enacted in order to provide law enforcement officials with the tools that they need to respond to current terrorist threats and apprehend individuals or organizations involved in terrorist activity before an attack is committed;
- ***Prevent***: Under the authority of this pillar, new programs and initiatives are introduced in order to better understand and address the root causes of radicalisation in order to prevent individuals from resorting to violent extremism;
- ***Protect***: Under the authority of this pillar, programs and initiatives are put into place in order to reduce the possibility of an attack being successfully executed by identifying and addressing vulnerabilities particularly in regard to the protection of critical infrastructure and border security; and finally
- ***Prepare***: Under the authority of this pillar programs and action plans have been put into place in order to have the capability to respond quickly to a range of emergencies, including terrorism, in order to mitigate the impact of an attack or national emergency when it could not have been prevented.

This Strategy was revised in March 2009, and the first Annual Report of the CONTEST Strategy was published in March of 2010 (Prevent: A Communications Guide, 2010) (Home Office web-site, 2010).

Security in an Interdependent world

In March 2008, the government of the United Kingdom published its first national security strategy entitled "*Security in an Interdependent World*". The aim of this Strategy was to outline how the British Government would address and manage the 'security challenges and underlying drivers', both in the immediate future and in the longer term. (Home Office web-site, 2010)

The Prevent Strategy: A Guide for Local Partners in England

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

On June 3rd, 2008 the UK Home Office published *The Prevent Strategy: a Guide for Local Partners in England.* This document was developed with the goal of providing guidance to local partners and authorities in the development and implementation of programs to counter violent extremism (Home office web-site, 2010).

Preventing Violent Extremism: A Strategy for Delivery 2008 and 2009

In June of 2008 this document was also released by the UK government. This document provides a brief overview of the work which has been done by the UK government to counter violent extremism and provides a strategy for the delivering these programs in 2008 and 2009. This document provides useful information for anyone who is simply interested in informing themselves as well as for those who are interested in working in the communities to develop programs of this type. This strategy was updated in August of 2009 (Department of Children, Schools and Family web-site, 2010).

Self-assessing Local Performance Against NI 35: Building Resilience to Violent Extremism. Guidance for Local Partners

To provide some background, in 2006 the UK government released an updated set of national indicators which are to be used by local authorities to report on their performance (alone or in partnership) to the central government. There are a total of 198 national indicators at present and it is Indictor 35, which is defined as "*Building Resistance to Violent Extremism*" which is used to evaluate programs aimed at countering violent extremism. Therefore, this document which was released in April of 2009, provides the assessment framework which is used by the central government to assess the quality of Preventing Violent Extremism projects. This assessment framework has 4 main themes and uses a 5 point scale to assess each. These four themes are as follows (OPM web-site, 2010):

- Understanding of, and engagement with, Muslim communities;
- Knowledge and understanding of the Preventing Violent Extremism agenda;
- Effective development of an action plan to build the resilience of communities and support vulnerable individuals; and finally
- Effective oversight, delivery and evaluation of projects and actions.

Working Together to Protect Crowded Places of 2009 and 2010

This document was released in April of 2009 and was updated in March of 2010. The purpose of this document was to ensure the appropriate level of security is in place in crowded areas in order to minimize the loss of life or serious injury in the event of a terrorist attack or other major emergency. This guide was drafted in part through public consultation and was disseminated with the goal of providing guidance to local partners, including businesses, to help them understand the role they can play in reducing the vulnerability to a terrorist attack and provides advice about how risks will be assessed and local performance managed (Home Office web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Safer Places: A Counter Terrorism Supplement - Consultation Document

The guide, which was released the same day as the *Crowded Places* document, was developed through public consultations and gives practical advice on how best to incorporate counter terrorism measures into proposed new development projects. One example of a key factor which was revealed through the consultation process was the importance of 'designing buildings with counter-terrorism measures in mind while still providing a suitable and inviting work environment' (Home office web-site, 2010).

Security for the Next Generation: The National Security Strategy

The updated version of the *UK National Security Strategy* (NSS) was released in June of 2009 and was entitled: *Security for the Next Generation: The National Security Strategy of the United Kingdom.* This new strategy encouraged the government to work together on security issues, while also increasing transparency and accountability at the same time in order to provide a 'flexible and coordinated response to terrorism'
The 2009 NSS also noted that security challenges may arise in the 'Cyber, maritime and space domains" and as a result, the UK government subsequently released a *Cyber Security Strategy* in June of 2009, began the process of creating a new *National Maritime Information Centre (NMIC)* will be completed in 2010; and finally prompted the Cabinet Office to review of the UK's national security interests in space (Cabinet office web-site, 2010).

Cyber Security Strategy

As mentioned above, as a result of the 2009 NSS, the UK government released a *Cyber Security Strategy* in June of 2009, and established the Office of Cyber Security and the Cyber Security Operations Centre in September of the same year. Other key action items which were identified to be achieved under the authority of this strategy were as follows (Cabinet office web-site, 2010):

- Providing a clear, strategic vision developed in concert with stakeholders across government;
- Establishing a growing network of academic, government and industry experts to consider future technical and social developments;
- Protecting UK businesses;
- Improving awareness and understanding of cyber security while reducing threats;
- Ensuring public sector systems are protected so that essential services can be protected;
- Monitoring developments in cyberspace, analyzing trends and co-ordinating responses to cyber incidents; and
- Developing the new national partnership to deliver Cyber Security Challenge to inspire young people to pursue a career in information security.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Eliminating World Poverty: Building a Common Future:

This document which was released in July 2009, identified the need to focus more efforts in conflict areas and fragile states in order to meet one of the fundamental principles of the NSS, namely a commitment to pay attention to the drivers of terrorism, such as: insecurity, poverty, lack of good governance and competition for scarce natural resources and to address these issues before they escalate (Department for International Development (DFID) web-site, 2010).

Road to 2010

In the *Road to 2010* White Paper which was also published in July of 2009, the UK government put in place a package of enhanced nuclear security measures in order to demonstrate the UK's commitment to tackling the threat of nuclear terrorism and established the *National Nuclear Centre of Excellence* in order to implement these measures (Cabinet office web-site, 2010).

UK's Science and Technology Strategy for Countering International Terrorism – August 2009

The Strategy sets out our approach to ensuring that science and technology are fully harnessed to strengthen the UK's ability to combat terrorism. This Strategy will achieve this in three ways (Home office web-site, 2010):

- By using horizon scanning to understand future scientific and technical threats and opportunities
- By identifying priority science and technology requirements and sharing them with industry and academia so that effective solutions can be developed
- By improving international collaboration on counter-terrorism related science and technology.

Learning Together to be Safe: A Toolkit to Help Schools Contribute to the Prevention of Violent Extremism- November 2009

This toolkit provides background information regarding the threat of violent extremist groups of various kinds and the factors which might make young people vulnerable. This toolkit also provides strategies for schools to minimize or address these potential threats. The most recent version of this toolkit was released in November 2009 (DCSF web-site, 2010).

Adaptability and Partnership

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

This *Defence Green Paper* which published in February 2010 outlines the Ministry of Defence's current thoughts on the future security environment and on other key issues it faces ahead of the upcoming *Strategic Defence Review* (Cabinet office web-site, 2010).

Yearly Update on Progress on Updated CONTEST Strategy

In March 2010, the Prime Minister gave a speech to report on the progress which has been made since the first *National Security Strategy* was announced in March of 2008. As part of his speech, the Prime Minister outlined some the changes which have taken place since the strategy was first announced (Home office web-site, 2010). Namely:

- "The focus is not longer just the protection of state, but also the protection of individuals and their freedom to go about their daily lives with confidence";
- The release of the latest version of the *National Risk Register*, first published in 2008;
- The terrorism threat level is now made publicly available;
- The *Counter Terrorism Strategy of 2009* is now a fully public document;
- The UK government encouraged the establishment of a Joint Committee to ensure that there is transparency and accountability to Parliament;
- And the UK government also established a *National Security Forum* to engage independent experts from a variety of fields into conversation about all issues pertaining to national security.
- In addition the Office of Home Security has completed an urgent review of the UK 'Watchlist system' and as a result, intends to extend it. The UK government has set-up a single Border Agency with police-level powers and new electronic border controls which will be covering 95% of travel by the end of 2010.

Protecting Europe against large-scale cyber-attacks

On March 18, 2010, the *House of Lords European Union Home Affairs Sub Committee* published a report on cyber security. This document identified International engagement as a key aspect to the UK Strategy to send a clear and powerful message about the need for a safe and secure Internet. This document provided a list of recommendations including that CERTs (see Outreach section for definition) should be established in all European Union Member states (UK Parliament web-site, 2010).

National Risk Register (NRR)

Since 2005, the UK Government has carried out classified assessment of the risks facing the UK. These *National Risk Assessments* (NRAs) are done at the local level, by front line personnel to identify geographic specific risks as well as global national risks. These NRAs are then compiled into a larger document which is called the National Risk Register. The full version of the NRR is classified but the first unclassified version was released to the public in 2008. The unclassified version provides the latest assessment of the risk of terrorism, natural hazards, and man-made accidents which may significantly

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

affect human welfare in the UK. The latest version of this register was released in 2010 (Cabinet office web-site, 2010).

Prevent: A Communications Guide

In order to support the delivery of Objective 7 of the Prevent portion of the CONTEST Strategy, namely 'To improve our strategic communications', the UK government has produced a document entitled *Prevent: A Communications Guide*, which was made available March 2010.

This guide was developed by the Research, Information and Communications Unit (RICU) and the Department of Communities and Local Government (CLG) and was designed to be a 'toolkit" to be used by local partners and authorities in order to develop and implement effective communications which adhere to the principles of the Prevent Strategy. According to this document, the role of the communications strategy is to:

- Empower people to play their part;
- Increase public confidence; and
- Influence attitudes and behaviours.

In order to achieve these goals, a local *Prevent Communication Strategy* should include the following components:

- **Establish the Context**: create a local narrative which takes into account local concerns and grievances which will resonate within the community;
- **Objectives**: Set the objectives this Strategy aims to achieve. These objectives will be used to assess the effectiveness of the program in the evaluation component;
- **Develop a Communications Strategy**: this Strategy should outline the objectives and how it will be implemented. Communication plans should begin with an evaluation of the baseline which will also be used in evaluating the effectiveness of the program;
- **Implement the Strategy;** and finally
- **Evaluate the Effectiveness and Document any 'Lessons Learned'**

This paper then outlines each step in the process and provides 'best practices' which should be employed at each step in a clear and concise manner. As part of this strategy, the RICU has compiled a glossary of common terms which are used in order to describe radical extremism and has provided the users with a list of the benefits and risks of using this terminology when communicating with the Muslim community (Home office web-site, 2010).

The Channel Programme: Supporting Individuals Vulnerable to Recruitment by Violent Extremists – March 2010

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The *Channel Programme* was developed under the PREVENT arm of the CONTEST Strategy. This programme uses existing collaborations between local authorities, the police, and statutory partners (such as the education sector, social services, children and youth services and offender management services) and the local community to:

- Identify individuals at risk of being drawn in to violent extremism;
- Assess the nature and extent of that risk; and
- Develop the most appropriate support for the individuals concerned.

The latest version of this document, which was released in April 2010, describes the indicators and causes of violent extremism as well as provides the 'best practices' or 'lessons learned' which have been determined since the implementation of the program (Home office web-site, 2010). Please see page 12 of the document entitled *Channel: Supporting Individuals Vulnerable to Recruitment by Violent Extremists, A Guide for Local Partnerships* for a graphic depiction of the Channel process. This document can be found at the following website: http://tna.europarchive.org/20100419081706/http:/security.homeoffice.gov.uk/news-publications/publication-search/prevent/channel-guidance?view=Binary.

Social and Behavioural Science Booklet – March 15, 2010

This booklet was issued on March 15, 2010 with the intention of engaging academia and industry in the protection of national security in order to reduce the risk to the UK and its interests overseas from international terrorism. This is the first booklet to be issued since the issuance of the new CONTEST Strategy in 2009 (Home office web-site, 2010).

The United Kingdom's Strategy for Countering Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism –March 2010

This strategy, which was issued on March 22, 2010, identified two main objectives in the countering CBRN attacks. They are as follows: to prevent attacks of this nature from occurring; and to have measures already in place to minimize the loss of life in the event that an attack occurs (Home office web-site, 2010).

Government response to Lord Carlisle's 5th Annual Report on the Prevention of Terrorism Act 2005

Since the enactment of the *Prevention of Terrorism Act of 2005*, an independent review of this Act is conducted annually to provide an independent assessment of the operation of this Act and provide recommendations. Upon completion, these reports are submitted to the UK Parliament for their review and response. The fifth annual report of the UK government's response to these recommendations was released on March 25, 2010 and is available on the Office for Security and Counter Terrorism web-site.

Reports by the Joint Committee on Human Rights – 2009/2010 Session

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The *Joint Committee on Human Rights* consists of twelve members appointed from both the House of Commons and the House of Lords. The Committee is charged with considering human rights issues in the UK, in a general sense and reports its findings and recommendations to the House.

The Committee also looks at Government action to deal with judgments of the UK courts and the European Court of Human Rights where breaches of human rights have been found. This Committee has been in existence since 2000, and has produced the following other reports as of late which are related to national security are as follows (UK Parliament web-site, 2010):

- *Counter-Terrorism Policy and Human Rights (Seventeenth Report): Bringing Human Rights Back In;*
- *Legislative Scrutiny: Crime and Security Bill; Personal Care at Home Bill; Children, Schools and Families Bill; and*
- *Counter–Terrorism Policy and Human Rights (Sixteenth Report): Annual Renewal of Control Orders Legislation 2010.*

Preventing Violent Extremism: Sixth Report of 2009-10

This report is a summary document of an extensive evaluation which was conducted into the programs which have been created under the authority of the Prevent arm of the CONTEST strategy. Main topics examined include (UK Parliament web-site, 2010):

- A review of the *Channel Project*;
- The unintended consequences or effects of these programs;
- Risk factors for radicalisation;
- Other forms of extremism;
- The central and local of *Prevent*;
- The overlap between the *Prevent* and *Pursue* arms; and
- The effects of these programs on the cohesion of the UK society.

Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review and the National Security Strategy – November 2010

These two documents were released in order to recognize that the world has evolved and with it, so have the amounts and types of threats to national security facing the United Kingdom. The goals of the *National Security Strategy* were stated in this document as the following:

> 'In an age of uncertainty, we need to be able to act quickly and effectively to address new and evolving threats to our security. That means having access to the best possible advice, and crucially, the right people around the table when decisions are made. It means considering national security issues in the round, recognising that when it comes to national security,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> foreign and domestic policy are not separate issues, but two halves of one picture (Ministry of Defense (MOD) web-site, 2010).

The Strategic Defence and Security Review details how the Armed Forces will be reshaped to tackle emerging and future threats, namely:

- To ensure that the mission in Afghanistan is protected; and
- To make sure the UK emerges with a coherent defence capability in 2020.

6.2 National Information Sharing Strategy

Defence Information Strategy (MODIS) of 2000 and 2009

The first *Defence Information Strategy* was released in 2000, and was updated in 2009. This *Information Strategy* sets the high-level context for Defence to collectively transform the way we use and manage information. This Strategy outlines the UK government's new 'Defence Information Vision' which is based on four pillars:

- Strategic Alignment;
- Information Exploitation;
- Value for Money; and
- Accessibility and Trust.

Please see page 7 of the document *MOD Information Strategy 2009* for a graphical representation of the Defence Information vision. This document can be found at: http://www.mod.uk/NR/rdonlyres/530403AF-FC89-41E0-852F-4D2934C15001/0/2009_MODIS.pdf.

In order to achieve these goals, the UK government has recognized that this will require a change in the way information transfer is viewed. In light of this, this document provides a list of 'Guiding Principles' in order to achieve these objectives. These guiding principles are as follows:

- **Information is a strategic defence asset** and therefore it needs to be managed in a structured way;
- **Strong information governance is necessary** to gain best value;
- **An enterprise approach will improve the efficiency** and effectiveness of information capabilities;
- **A skilled, agile workforce is required** to enable defence to fully exploit its information;
- **Information has more value when it is shared**, securely;
- **Establishing the correct balance between openness and security will be a constant challenge**; and finally
- **Information capability is improved through learning from others**, therefore the Department of Defence will proactively engage with wider Government,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

industry, academia and allies in order to identify, share and learn from best practice.

Please refer to page 6 of the *MOD Information Strategy 2009* document for a graphic depiction of the changes which the UK Ministry of Defence aims to achieve with this Strategy.

6.3 Outreach Programs by Type:

6.3.1 National Security Initiatives - General

The National Security Forum

The *National Security Forum* was established by the UK Prime Minister on March 8th, 2009. This Forum has met on several occasions and consists of a body of experts who provide independent advice to the UK government on matters related to national security. Topics which have been discussed have included:

- The national security implications of the economic downturn;
- The UK government's strategy in relation to Afghanistan and Pakistan; and
- Security in relation to: energy suppliers, space, nuclear energy, non-proliferation, soft power and maritime security.

The advice which was submitted by this Forum has contributed significantly to the development of the annual update of the *National Security Strategy* and the UK's *Cyber Security Strategy*. The Prime Minister has been involved in these Forum discussions on a number of occasions (National Security Forum web-site, 2010).

6.3.2 Defence-Related Initiatives

UK Defence Forum

According the web-site: 'The UK Defence Forum was created in 1996 to inform the defence, security and peace debate by enabling politicians, diplomats, senior members of the armed forces, public servants, defence professionals, academics and others with an interest in defence and security to exchange information and views on the future challenges of Britain's defence, by preparing and publishing research papers, including the Defence Viewpoints blog, and by facilitating study visits. It is a non-partisan and not-for-profit organisation which holds no views of its own, and supports All Party Parliamentary Groups covering the Armed Forces at their request'. Please see below for information related to initiatives of this Forum (UK Defence Forum web-site, 2010):

- **Defence Viewpoints:** This web-site and blog has been created and is maintained by the UK Defence Forum. It is comprised of defence and security information consisting of: original research papers and reports by think tanks and academics, reviews and opinion pieces from newspaper and magazine articles which have been reproduced with the author's permission. Visitors of the site are invited to add their own comments, and can search the site.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- **Defence Red Box**: The *Defence Red Box* is an initiative of the *UK Defence Forum*. Through this initiative, members of the general public can subscribe to receive daily alerts of headlines and the 'best' of blogs from industry; global defence and security organization and the UK parliament on topics which relate to the defence or protection of the United Kingdom (UK Defence Forum web-site, 2010)

6.3.2 Science and Technology Initiatives

Technical Advisory Board

The *Technical Advisory Board* (TAB) is a non-departmental public body that advises the Home Secretary on whether the obligations imposed are reasonable (Home office web-site, 2010)

6.3.3 Critical Infrastructure Initiatives

The Security and Resilience Industry Suppliers Council (RISC)

The UK Government has a strong relationship with the defence industrial base but this is now being extended by expertise in other key areas of national security through its strategic partnership and dialogue with the UK security industry through the *Security and Resilience Industry Suppliers Council* (RISC). The RISC brings together the industrial community in the UK to support the Government in creating a more secure and safe environment. RISC has five Industrial Advisory Groups to allow for advice on key areas of national security. They are as follows:

- *Chemical, Biological, Radiological and Nuclear Protection;*
- *Information and Communications Technology;*
- *Protection of Critical National Infrastructure;*
- *Stand-off Detection of Suicide Bombers*; and
- *Olympics and Paralympics.*

RISC also has an international group that meets regularly to consider how other countries and international institutions can play a role in meeting the national security objectives of the UK and RISC also has a communications group which is responsible for the distribution of information about RISC to industry members, the UK government and the general public (RISK web-site, 2010).

The Critical Infrastructure Resilience Programme:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

This program is based upon collaboration between Government, regulators, owners and operators of critical infrastructure in the nine national infrastructure sectors. The first products of this program were published in March 2010 and included the following:

- **Strategic Framework and Policy Statement:** to communicate the policy intent, timescales and expectations for this programme;
- **Sector Resilience Plan for Critical Infrastructure 2010:** This provides an overview of the assessment of the vulnerabilities of the UK's Critical Infrastructure in all nine categories.

6.3.4 Cyber Security Initiatives

Computer Emergency Response Teams (CERTs)

A Computer Emergency Response Team, or CERT, is an organisation that studies computer and network security in order to provide incident response services to victims of attacks, to publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.

In the United Kingdom there are a number of CERTs. CERTS are a critical part of dealing with Internet incidents, as they have the relevant expertise and experience to deal rapidly with any problems (UK CERT web-site, 2010).

6.3.5 Community Outreach Initiatives

Preventing Violent Extremism Community Leadership Fund

The Preventing Violent Extremism Community Leadership Fund was launched in 2007 and is aimed at national level projects on preventing violent extremism. The initial fund was £650,000 and an additional £25 million was later added. The program's goal is to help Muslim communities find the means to fight extremism and feel welcome in British society (Communities and Local Government 2007). The program focuses on three key areas:

- Increasing the leadership capacity of Muslim leaders through support;
- Organizational capacity, which is aimed at "building the capacity of organizations in the Muslim community to actively resist the influence of violent extremists" (Communities and Local Government 2007, 3); and
- To develop the capacity of Muslim women so they are able to help young Muslims who are at risk of radicalization (The Change Institute 2008; Communities and Local Government 2007).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

6.3.6 Police Based Programs

Neighbourhood Policing

A *Neighbourhood Policing* approach to law enforcement came into effect in the United Kingdom with the enactment of the *Police Reform Act* in 2002. This approach became the framework underlying the entire PREVENT Strategy, and helped to ensure a common approach to a whole range of community issues, including radicalization and violent extremism. At the core of policing strategy are *Safe Teams* (SNTs), which consist of a mix of sworn police officers and *Police Community Safety Officers* (PCSOs). These PCSOs have limited police powers, but provide a uniformed presence within the communities. While the primary focus of these SNT teams is preventing crime, they are often also in a position to identify persons at risk of engaging in violent extremism and therefore able to intervene before reaching a crisis point due to their involvement at the community level (CACP document).

Building Networks

Through the *Building Networks* Program, Borough Commanders in the United Kingdom are taking active steps to build extensive networks of trusted faith and community leaders and other influential persons within the neighbourhoods they police.

Sometimes referred to as "*Gold Groups*," such networks can be assembled quickly and kept briefed in the aftermath of a terrorist incident, or a major series of terrorism-related arrests. Gold Group-type networks are excellent sources of real-time expert advice on crisis management, especially when police / community relationships are at their most fragile. The very process of keeping them informed can do a great deal to allay suspicions and anxieties and to reassure the community (CACP document).

The DELPHINUS Program

The DELPHINUS Program was originally developed by the London Metropolitan Police in the aftermath of the 7/7 bombings and has now been adopted throughout the United Kingdom. This program requires close engagement between the police, community leaders and local authorities in order to ensure that intelligence and other counter-terrorism information is provided to community, patrol and investigative units where possible (CACP document).

Operation NICOLE

Operation NICOLE invites community members who have some degree of influence in the community to take on the role of a senior police officer investigating a terrorist incident.

It is a tabletop exercise which has two objectives:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- To give the police insight into the community impact of counter terrorist policing; and
- To give community members insight into the decisions that the police have to make during investigations.

In addition, Operation NICOLE serves as a platform for all parties to debate core issues of law, civil rights, and the nature of the response to violent extremism (CACP document).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

7.0 Citizen Engagement in National Security Issues in the Netherlands

The release of National Security Strategies in the Netherlands began in 1999 with the *Disaster Control and Crisis Management* document. Since then, many other reports have been released, particularly on the phenomenon of radicalization. In addition, as seen with the other countries examined thus far, an Information Strategy has also been developed with the goal of widening the lines of communication between government and the private sectors. As well, many programs have been put into place with the goal of engaging their citizenry or members thereof, on some level. Therefore, the following section will provide an overview of these documents in the following fashion:

1) Provide a brief overview of the *National Security Strategies* and documentation which have been released at date aimed at combating terrorism;
2) Provide an overview of the Dutch Information Strategy; and finally
3) Provide a brief description of the programs which have been enacted in the Netherlands with the purpose of informing, consulting or encouraging active participation among its citizenry.

Note to the reader: While many strategies and programs were found during this review, it is worth noting that much of the information on the Dutch web-site was in Dutch only and, therefore, there may be other programs which exist in the Netherlands which are not included here due to a language barrier.

7.1 History of National Security Strategies in the Netherlands

See below for a list of the strategies and documentation which have been identified to date. You will note that a great deal of emphasis has been made in the Netherlands on combating radicalization including: Islamic, Salafist, Right-wing and Animal rights.

- *Disaster Control and Crisis Management 1999;*
- *Citizen and government in the information society;*
- *Progress Report Countering NBC attacks by terrorists;*
- *Recruitment for Jihad – 2002;*
- *Terrorism and Protection of Society 2002-2003;*
- *Counterterrorism in the Netherlands – 2003;*
- *Background of jihad recruits – 2004;*
- *Critical Infrastructure Protection in the Netherlands, 2004 and 2009;*
- *Combating Terrorism Policy Statement 2004;*
- *Annual reports of the AIVD;*
- *Espionage and security risks, 2004;*
- *Performing together for public safety and Security, 2004;*
- *Saudi Influences in the Netherlands, 2004;*
- *Animal Rights Activism in the Netherlands, 2004, 2007 and 2009;*
- *From Dawa to Jihad – 2004 and The Radical dawa in Transition, 2007;*

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- *Radicalism and Radicalization, 2005;*
- *Summary DTN – Terrorist Threat Assessment;*
- *Progress report: Policies and Integration, 2006;*
- *Violent Jihad in the Netherlands, 2006;*
- *Guide to Counter-terrorism at the local level, 2006;*
- *First inventory of policy and Counterterrorism: Germany, France, Italy, Spain, the United Kingdom and the United States, 2006:*
- *Scenario Planning for Critical Infrastructure Protection, 2007;*
- *The Strategy and Work Programme, 2007-2008;*
- *Polarization and Radicalization Action Plan 2007-2011;*
- *Jihadists and the Internet, 2007, 2009 and 2010;*
- *High-tech crime, different crime types and perpetrators;*
- *Salafism in the Netherlands, 2008;*
- *Factsheet: Advisory report on large-scale evacuation 2008;*
- *National Risk Assessment Method Guide 2008;*
- Psychosocial effects of threat and protection – March 2008;
- *National Safety and Security;*
- *Speech at the Global Initiative to Combat Nuclear Terrorism;*
- *Second Report on Critical Infrastructure Protection, 2009;*
- *Guidance Methodology to National Safety and Security Strategy, 2009;*
- *Jihadist terrorism in the Netherlands, 2010;*
- *Ideology and Strategy of Jihadism;*
- *Fact sheet: National Safety and Security Strategy, 2010;*
- *Countering Violent Extremist Narratives, 2010;*
- *Islamic and Extreme Right Radicalization, 2010;*
- *Three publications on espionage from AIVD and MIVD;*
- *Resilience and Resistance 2010; and*
- *Speech of May 25th, 2010: Counterterrorism coordinators seek cooperation with IT industry*

Disaster Control and Crisis Management in the Netherlands -1999

This brochure includes an overview of the disaster control and crisis management systems which were in place the Netherlands (as of 1999). It provides a description of the overall organization of disaster control, and a summary of the tasks of the various departments. It was intended to be used by first responders as well as to inform the general public (MIKR web-site, 2010).

Citizen and Government in the Information Society - The Need for Institutional Innovation – 2001

This report was released by the Dutch government in 2001, after the September 11th attacks, and calls for change in the way that the government communicates with the Dutch citizenry. It calls for the government to strengthen its role in the information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

society and to create new relationships between citizens and government (MIKR web-site, 2010).

Progress Report Countering NBC attacks by terrorists

This report provides an overview of counter-terrorism programs which were in place as of 2002, and indicates measures required to supplement the existing structure for combating disasters and crisis management, in light of the events of September 11th (MIKR web-site, 2010).

Recruitment for the Jihad in the Netherlands - 2002

This paper outlines the phenomenon of recruitment for the jihad in its broader (NCTb web-site, 2010).

Counter-terrorism in the Netherlands - 2003

This is a report which, was written by the then Director Democratic Legal Order General Intelligence and Security Service of the Netherlands (AIVD), in 2003. This report discusses the current understanding of Islamic terrorism and the counter-terrorism strategies which were in place at the time of the creation of this report. This report recommended that a 'wider approach' be taken to the development of counter-terrorism strategies and that strategies should be tailored to a specific target group or target person. As such, this paper divided citizens into 4 groups which were referred to as the "Ring Model" (MIKR web-site, 2010). Please see page 6 of the document entitled *Counter-Terrorism in the Netherlands* for a graphic depiction of the Ring Model. This document can be found at: http://www.fas.org/irp/world/netherlands/ct.pdf.

Background of Jihad Recruits in the Netherlands – March 2004

This memorandum gives a brief characterisation of persons in the Netherlands who are going through a process of recruitment for the violent jihad. This memorandum includes background information on the following:

- The ideology;
- The foreign and domestic motives; and
- How individuals are recruited.

Critical Infrastructure Protection in the Netherlands -2004 and 2009

The Dutch government released its first strategy for the protection of critical infrastructure in 2004 and released a subsequent strategy in July of 2009. These reports give an overview of the Dutch approach to the protection of their critical infrastructure. They provide background information about how the Netherlands have organized their strategies in order to protect their critical infrastructure and their relationship with businesses which have been identified as being part of their critical infrastructure.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

During the first phase of the project a 'quick scan" was performed to map out the critical sectors, products and services in the Netherlands. The outcomes of the "quick scan" served as the basis for the next phase of the project. This next phase is elaborated into three sub projects:

- Identifying critical junctions (also in terms of geographic location) between critical sectors and services;
- Mapping out the vulnerability of sectors and junctions. Obtaining insight into protective measures already implemented; and
- Developing a cohesive set of protective measures, including any additional protective measures and embedding the measures to protect critical infrastructures within the standard business operations of the government and business community.

Please see page 13 of the document *Critical (Information) Infrastructure Protection in the Netherlands* for a table of industries which have been identified as being part of the critical infrastructure of the Netherlands. This document can be found at: http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-1.pdf.

In addition, page 16 of the same document provides a depiction of the interdependencies between critical infrastructure sectors.

Combating Terrorism: Counterterrorism Policy Statement of 2004

This policy statement was submitted to the Chairman of the Lower House of the Dutch Parliament in September of 2004. This policy puts forth the idea that it is necessary to gather information and to engage in international cooperation in order to combat terrorism. This document is a follow-up to the *Terrorism and Protecting Society* policy document and includes the following objectives (NCTb web-site, 2010):

- Changes to legislative powers including: updates to the *Criminal Offences Act*; the *Data Protection Act* and the *Weapons and Ammunition Act*;
- The development of a National alerting (early warning) system;
- Tackling entities that support terrorist activities;
- Their plans for International collaboration; and
- How the Dutch government plans to limit 'terrorist breeding grounds'.

Annual Reports of the AIVD

Since the attacks in Madrid in 2004, the AIVD (the Dutch Intelligence Agency) have produced annual reports to provide insight into the threat from international terrorism. These reports describe the relevant risks to national and international security, like the proliferation of weapons of mass destruction and violent activism. These reports have been produced annually since 2004 (which was a review of the 2003 efforts and so on), all of which can be found on the AIVD web-site.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Espionage and Security Risks - Invisible, But Still Existing –March 2004

This brochure provides information about intelligence activities in the Netherlands. The goal of this brochure was to provide people working in both the public and private sectors with information in regards to the risks associated with espionage and to provide tips in order to identify and prevent it from occurring (AIVD web-site, 2010).

Performing Together for Public Safety and Security –October 2004

This brochure contains a brief summary of the Ministry of the Interior and Kingdom Relations responsibilities and the organization of relief assistance in the field (MIKR web-site, 2010).

Saudi Influences in the Netherlands - Links between the Salafist Mission, Radicalization Processes and Islamic Terrorism –March 2004

This report was released in 2004 and it provides some background into the Salafist mission and the relationship with radicalisation processes in the Muslim communities and finally, some context into the then recent developments in both Saudi Arabia and the Netherlands (AIDV web-site, 2010).

Animal Rights Activism in the Netherlands - Between Peaceful and Burning Protest – July 2004, 2007 and 2009

This paper examines the (then) recent history of Animal rights extremism in the Netherlands and was developed as a result of the assassination of Pim Fortuyn by an animal rights activist on May 6thof 2002. Subsequent reports were conducted in 2007 and most recently in 2009. The 2009 report describes the major developments in Dutch animal rights extremism since the June 2007 report was issued, and draws a clear distinction between activism and extremism. The main difference between the two is that activists operate within the law, whilst extremists deliberately commit illegal and sometimes violent actions (AIVD web-site, 2010).

From Dawa to Jihad - The Various Threats from Radical Islam to the Democratic Legal Order - December 2004 and 2007

This paper provides insight into the conceptual foundation of the AIVD's study of radical Islam. This paper starts from the premise that radical Islam is a multiform phenomenon, consisting of many movements and groups that, although related (in particular concerning faith and anti-Western sentiments), may harbour very different views on aims and means.

This paper does not discuss specific threats emanating but provides a conceptual contribution to the broad approach to studying radical Islam and the debate on countermeasures. The updated version of this study is entitled: '*The radical dawa in*

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

transition', which provides an update to the previous version released in 2004, and discusses a new phase in Muslim radicalism called *Islamic neoradicalism*, as coined by the AIVD (AIVD web-site, 2010).

Radicalism and Radicalization - 2005

This memorandum, which was released in September of 2005, describes the importance of a broad-based approach to radicalism and radicalization, as well as the circumstances in which judicial intervention by the government against radicalism is required. It identifies three different form of radicalization of concern within the Dutch society. They are as follows (NCTb web-site, 2010):

- Islamist radicalism;
- Right-wing radicalism, and
- Animal rights activism.

Summery Report on the DTN - Terrorist Threat Assessment Netherlands (DTN)

The DTN is drawn up four times a year by the office of the National Coordinator for Counterterrorism. It is primarily intended to provide the Cabinet Committee on National Security with an up-to-date evaluation of the risks facing the Netherlands at present. The Summary Report of the DTN is also sent to the House's Intelligence and Security Services Committee, so that they are informed as to the potential risks.

For more information regarding the DTN and also the Counter terrorism Alert System, please refer to the Outreach section (NCTb web-site, 2010).

Progress Report: Policies on Integration and Prevention of Radicalizations in the Netherlands - July 2006

This report was released on July of 2006, and was developed by the Minister for Integration and Immigration. It provides a brief summary of the objective and an outline of the integration policy on the prevention of radicalization, which was already in place (NCTb web-site, 2010).

Radicalisation in a Broader Perspective

This publication was distributed at the international conference entitled: *Countering radicalization: perspectives and strategies from around the globe*, which was held in October of 2007 in The Hague. The aim of the conference was to provide a venue for Western and Southern countries that face radicalization to share experiences, perspectives and policies. This publication is a compendium of the ways that different European and Arab nations view radicalization, their methods of dealing with it and the interactions between the different countries. The publication is also available in French (NCTb web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Violent Jihad in the Netherlands: Current Trends in the Islamist Terrorist Threat -2006

This paper is an elaboration of the publication *From Dawn to Jihad*, which was published in 2004; however, this iteration focuses exclusively on violent jihadist movements within radical Islam (NCTb web-site, 2010).

Guide to Counter-Terrorism at the Local Level - 2006

The aim of this guide is to provide local authorities with a basis for developing a local approach to counterterrorism. This guide is intended to provide an overview of counterterrorism in the Netherlands and how it is organised. This guide was updated in 2007 (NCTb web-site, 2010).

Guide Counter-Terrorism for Companies – December 2006

This guide was geared for all businesses and employees, to provide insight into how businesses could be vulnerable to terrorist threats and in what ways (NCTb web-site, 2010).

First Inventory of Policy on Counterterrorism: Germany, France, Italy, Spain, the United Kingdom and the United States – 2006

This report provides the first ever international inventory of measures aimed at combating radicalisation, extremism and terrorism (referred to in this report as Counterterrorism Policy) in Germany, France, Italy, Spain, the United Kingdom and the United States. Commissioned by the NCTb, the WODC (the Research and Documentation Centre of the Dutch Ministry of Justice) and was conducted in early 2006 (NCTb web-site, 2010).

Scenario Planning for Critical Infrastructure Protection Report of the Scenario workshops April 2007

On April 18 and 19th, of 2007 a conference on Critical Infrastructure Protection took place in The Hague. More than 100 experts from all over Europe took part in the proceedings; experts on issues such as energy distribution, civil protection, emergency management, environment and many more (MIKR web-site, 2010).

The Strategy and Work Programme 2007-2008:

The first ever National Security Strategy which was released in the Netherlands was entitled *The Strategy and Work Programme 2007-2008*. The aim of the Strategy is to protect society and citizens within Dutch territory against internal and external threats. Using the working method described in the Strategy, Cabinet was able to determine which threats endanger national security and how to anticipate those threats, irrespective of their origin or nature.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

This Strategy recognizes that "the development of choices made by Cabinet is not only in the hands of the national government. Other public authorities, the business community and social organizations also play a role. In order to enable an integral approach, all parties involved must know and respect each other's role in strengthening national security, follow a shared doctrine, align their working methods to each other and be connected to the same communication network."

Another essential component of the integral approach is the structural exchange of knowledge and information and alignment between the public and private parties – both in a national and an international context – who play a role in protecting national security.

Under this Strategy, the Minister of the Interior and Kingdom Relations is responsible for the implementation of the Strategy in cooperation with other ministries, local authorities, the business community, research institutes, and planning offices (MIKR web-site, 2010).

Polarization and Radicalization Action Plan 2007-2011 – September 2007

This Action Plan has the following goals:

- The prevention of (further) processes of isolation, polarization and radicalization by the (re-)inclusion of people who are at risk of slipping away or turning away from Dutch society and the democratic legal order. This includes such things as, inclusion through education, traineeships and work. (Prevention);
- The early signaling of these processes by administrators and professionals and the development of an adequate approach. (Pro-action); and
- The exclusion of people who have crossed clear boundaries and seeing to it that their influence on others is limited as much as possible. (Repression) (MIKR web-site, 2010).

Jihadists and the Internet – 2007, 2009 and 2010

This report provides an overview of how the Internet is being used by Jihadists for training, in preparing for attacks, and how it is an important means of spreading radical propaganda. This report has been updated twice since the initial report was released, once in 2009 and the second in 2010. These reports provide new information as to how Jihadism is currently using the Internet as a tool to promote their cause (NCTb web-site, 2010).

High-tech crime, different crime types and perpetrators –April 2008

This report consists of the findings of a literature review of the existing knowledge in relation to high-tech crime, the perpetrators of high-tech crime and the involvement of organized crime and thereby aid in the development of efficient and effective policies (NCTb web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Salafism in the Netherlands – July 2008

The goal of this report is to give an overview of and the development of Saudi-inspired salafism in the Netherlands, with a description of its key characteristics. This is the first time a report of this kind has been made available. In addition, the report highlights factors which are important to determining the future of Salafism in the Netherlands (NCTb web-site, 2010).

National Risk Assessment Method Guide 2008

The purpose of the guide is:

- To describe the national risk assessment ; and
- To provide documentation and justification of choices made.

This guide was intended to be a user guide for those who work with the *National Risk Assessment* (NRA) in order to clarify how the methodology operates (MIKR web-site, 2010).

Psychosocial Effects of Threat and Protection – March 2008

The National Coordinator for Counterterrorism (NCTb) commissioned a project team headed by Prof. B.P.R. Gersons from the AMC in Amsterdam to conduct a descriptive, systematic study on the psychosocial effects of threat and protection. The aim of the study was to facilitate a more systematic approach to the support of threatened people and their families, who have been entrusted to the care of the NCTb, and to incorporate the latest insights into that support. It had already become apparent from the NCTb contacts with similar services in other countries that attention is seldom focused on advising protected persons from a psychosocial point of view.

The project group also noted that there is almost no literature on the effects of threat and protection. The group accordingly chose to conduct a literature review on relevant themes, supplemented by findings from interviews with people who are currently being protected or have been protected in the past and from interviews with protection officers. In order to gain insight into the psychosocial effects of threat and protection, an adapted stress model was developed on the basis of the model proposed by Olff, Langeland, & Gersons (2005a, 2005b) (NCTb web-site, 2010). This model can be seen on page 9 of the *Psychosocial Effects of Threat and Protection* document, which can be found at: http://english.nctb.nl/search.aspx?simpleSearch=psychosocial+effects+of+threat+and+protection.

Factsheet: Advisory Report on Large-Scale Evacuation 2008

As part of the 2007-2008 *National Security Work Programme*, the Dutch government commissioned research to evaluate their current capabilities to conduct a large-scale

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

evacuation in the event of a disaster or crisis. This factsheet was the result of this evaluation (MIKR web-site, 2010).

Final Report: National Safety & Security. Responding to Risks to Citizens, Communities and the Nation

This report identifies three key themes related to the national security of a nation (MIKR web-site, 2010):

1) The need to follow a process of identification, assessment and mobilization in any crisis situation;
2) The 'surprise' factor should be reduced as much as possible, i.e. every effort should be made to anticipate every possible vulnerability in order to reduce surprise attacks to the greatest degree possible; And finally,
3) Creating the right political structure in which the leadership is legitimized and has the power to achieve the common goal.

Speech at Global Initiative to Combat Nuclear Terrorism

At the last meeting of the *Global Initiative to Combat Nuclear Terrorism*, which was held in the Netherlands in June of 2009, the Minister of Foreign Affairs, Minister Verhagen, gave a speech where he spoke about the vision of the Dutch government in the areas of: nuclear security; nuclear disarmament and non-proliferation. He also announced they will continue to support the *National Security Fund* and will commit $250,000 Euros to the new Nuclear Security Plan in its first year (MIKR web-site, 2010).

Ideology and Strategy of Jihadism - December 2009

This study provides insight into the Ideology and Strategy of Jihadism. Included in this report is a description of the methods of: production, reproduction, and propaganda which are being used by the Jihadist terrorists in order to promote their views and recruit new members (NCTb web-site, 2010).

Guidance Methodology National Safety and Security Strategy – October 2009

This is the revised guide to the *National Safety and Security Strategy*. The purpose of the guide is:

- To describe the method used for scenario development, national risk assessment and capability analysis;
- To establish and justify the choices made; and
- To provide a guide for people who have to work with the national safety and security strategy.

This guide makes clear to people who have to work with the *National Safety and Security Strategy* how this method works. It should also serve as a foundation for those drawing

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

up incident scenarios and for those carrying out the national risk assessment and capability analysis in 2009 and later (MIKR web-site, 2010).

Jihadist Terrorism in the Netherlands – Jan 2010

This document is a summary report of the WODC report *Jihadist terrorism in the Netherlands*. It reports on the findings of a review which was conducted on twelve large scale closed police investigations which occurred between July 2001 and July 2005. This analysis focused on three dimensions of jihadist terrorism: jihadist corporations, the activities performed in these corporations and the jihadist actors (NCTb web-site, 2010).

Factsheet: National Safety and Security Strategy – Jan 2010

This factsheet which was issued in January of 2010, provides the general public with some information about national security strategies, their importance and use.

Countering Violent Extremist Narratives – Feb 2010 and July 2010

In June of 2009, the NCTb organized an expert meeting in order to explore ways of 'countering narratives against violent extremism. The main focus of the meeting was to understand what is behind violent extremist ideology and to draw up possible counter-arguments. International academic experts and policy advisors attended the meeting and the resulting recommendations were compiled into this report which was released on February 22, 2010. A subsequent version was released in July of 2010 (NCTb web-site, 2010).

Islamic and Extreme Right Radicalization – March 8, 2010

This report presents the results of a literature study on Islamic and extreme right-wing radicalisation in the Netherlands. These two forms of radicalisation are presently considered by the government as the most threatening types of radicalisation. The aim of the study is to offer a comparative analysis of the relevant insights provided by the literature on both types of radicalisation (NCTb web-site, 2010).

Three Publications on Espionage from AIVD and MIVD – March 29, 2010

The AIVD and the MIVD have published three brochures about the risks of espionage. These are: *Espionage in the Netherlands*, *Espionage when travelling abroad* and *Digital espionage*. The publications are primarily aimed at business people and civil servants who may come into contact with information that could be of interest to other countries (AIVD web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Resilience and Resistance – April 2010

This report highlights the current trends and developments relating to Salafism in the Netherlands. This report is a follow-up to the AIVD publication *Radicale dawa in verandering (*'The Radical Dawa in Transition'), which was published in 2007 (AIVD web-site, 2010).

Speech: Counterterrorism Coordinators Seek Cooperation with IT Industry - May 2010

At the *World Congress on Information Technology* (WCIT), the National Coordinator for Counterterrorism, Eric Akerboom, announced an upcoming initiative which seeks to establish closer cooperation between: IT companies, research institutes, and public bodies to set up a 'trusted community' in which public and private parties will share knowledge about IT and terrorism (NCTb web-site, 2010).

7.2 National Information Strategy

The Safety Information Policy: Connections in the Field of Safety

This policy is aimed at improving both the possession and dissemination of information among the safety partners. The goals of the Safety Information Policy are as follows (MIKR web-site, 2010):

- Well-informed care providers;
- Shorter response times;
- A joint situation view for everyone involved;
- Clear communication;
- Swifter assistance; and
- More affordable Information and Communications Technology.

7.3 Outreach Programs by Type

7.3.1 National Security Programs - General

Terrorist Threat Assessment Netherlands

The *Terrorist Threat Assessment Netherlands* (DTN) determines the general threat level for the Netherlands on the basis of a wide range of intelligence and disseminates this information to the general public. These risk assessments are generally categories into 4 categories: minimal, limited, substantial or critical, however no specific information is given as to the reason why a threat level may be elevated (NCTb web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

New Institute for Anti-terrorism in The Hague, the Netherlands

Three Hague-based organisations joined forces to shape a new, independent institute that will contribute to study and policy-making in the field of counter-terrorism. The initiative is financed by the Dutch Ministry for Foreign Affairs and opened in May of 2010. The institute primarily focuses on the preventative and international legal aspects of counter-terrorism (NCTb web-site, 2010).

Netherlands Against Terrorism Campaign - 2006:

This campaign focused its attention on outreach teachers, youth workers, and community police officers who are seen as the front line of defense in preventing terrorism.

In addition, the website www.nederlandtegenterrorisme.nl was expanded with new information for people who work with youth. It includes theme-based teaching materials, developed by experts and intended to help the professionals raise the subjects of terrorism and radicalization in the classroom and informal discussions with young people. The website also features an illustrated Internet game, *Sixteen Million Judges*, in which players deal with three cases of terrorism and radicalization (NCTb web-site, 2010).

The Hague Against Terrorism:

On September 13, 2006 the Municipality of The Hague launched the local public campaign *The Hague against Terrorism'* The campaign is being carried out in conjunction with the national campaign 'The Netherlands against terrorism', which started at the beginning of 2006 (Hague web-site, 2010).

Counterterrorism Alert System

The *Counterterrorism Alert System* was instituted to warn the operational services and economic sectors in the event of a heightened threat. This enables prior measures to be taken quickly in order to minimize the risk of terrorist attacks. Fifteen economic sectors are currently connected to the *Counterterrorism Alert System*, they are as follows:

- Airports;
- Railway;
- Municipal and regional transport;
- Seaports;
- Tunnels and flood defenses;
- Chemical industry;
- Oil industry;
- Drinking water;
- Natural gas;
- Electricity;
- Telecom;
- Nuclear;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Finance;
- Public events; and
- Hotels.

The National Coordinator for Counterterrorism is responsible for the operation and overall management of the system (NCTb web-site, 2010).

7.3.2 Aviation Security Initiatives

Civil Aviation Security Inspectorate (IBB)

The Civil Aviation Security Inspectorate (IBB) oversees the whole security chain and monitors the quality and effectiveness of civil aviation security.

The IBB functions independently of the security chain, enabling it to review the performance of its partners independently. It gathers information from all the partners in the security chain to build an accurate picture of the quality, effectiveness, and organization of airport security (NCTb web-site, 2010). Various partners are involved in civil aviation security, each with its own role:

- The **Civil Aviation Security Department (DBB)** draws up policy for civil aviation security and oversees the aviation sector and Kmar;
- The **Royal Military and Border Police (KMar)** supervise the implementation of security measures; and
- The **aviation sector (airports and aviation-related businesses)** implement the security measures.

000296

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

8.0 Citizen Engagement in National Security Issues in France

The first white paper on National Defence was issued by the French government in 1972. Since then, two follow-up strategies and other documents have been released in order to respond to the changing political and economic climate and emerging issues. As a result, there have been several programs which have been implemented which include engaging French citizens on issues of national security. Therefore, this paper will provide the following:

1) An overview of the Defence White Papers and documentation which have been released to date aimed at protecting national security and combating terrorism; and
2) A brief description of the programs which have been enacted in France with the purpose of informing, consulting or to encourage active participation among its citizenry.

Note to reader: While many strategies and programs were found, it is worth noting that much of the information on the French web-site was in French only and, therefore, there may be other programs which exist in France which are not included here.

8.1 History of National Security Strategies

Le livre blanc' – 1972

The first white paper on national defence was issued by the French government in 1972. This white paper defined the purpose of defence policy as having three levels (Le livre blanc web-site, 2010):

- Security of the national territory and its inhabitants;
- Security of Europe and the Mediterranean; and
- Distant territories around the world that 'show their belonging to French sovereignty.'

In addition, the threat of nuclear weapons and the need for nuclear deterrence strategies were clearly identified.

'Le livre blanc' – 1994 – Part I

In 1994, the French government released an updated version of its *Defence Strategy* to mark the end of the Cold War and also to provide strategies for the 21st century. Part I of this strategy provides an overview of the first four chapters of this white paper which are as follows (Le livre blanc web-site, 2010):

- International perspectives and the evolution of risks;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- The new objectives of the updated defence policy;
- The role of International organizations such as the United Nations and the European Union on the Defence strategies of France; and finally
- An overview of the new strategy for defence.

'Le livre blanc' – 1994 – Part II

Part II of this white paper includes chapters 5 through 9 address the following (Le livre blanc web-site, 2010):

- The capacity of the Armed Forces;
- Human resources strategies to address capacity issues;
- Disarmament and Industrial Strategy;
- Defence efforts; and finally
- The relationship between Defence and Society.

'Le livre blanc' – Defence and National Security – June 2008

Much the same as strategies which have been developed by other Western countries such as the United Kingdom and The Netherlands since the events of September 11th, this updated strategy includes a five pronged approach, all with the goal of preventing and mitigating the effects of an attack. The key concepts of this defence white paper are as follows (Le livre blanc web-site, 2010):

- Knowledge and Anticipation;
- Prevention;
- Deterrence;
- Protection; and
- Intervention.

Vigipirate Renforcé Plan (VRP) Ensuring Physical Protection - September 12, 2001

Former Prime Minister Jospin activated this plan on September 12th, 2001 following the events of September 11th. This plan was enacted in two phases.

- **Phase I**:
  - The Minister of Interior instructed the prefects to strengthen surveillance and controls around: American and Israeli diplomatic premises; airports; public transport stations and public buildings which could be potential targets;
  - The Minister of Defence instituted a reinforced air defence consisting of four patrols of fighter jets on ready alert to intercept attacks in French air space; and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- The Minister of Defence increased security at sensitive locations such as: nuclear plants, large dams and major industrial installations.

- **Phase II** of the Vigipirate called for 'enhanced awareness' among all public services and private partners to increase security to protect critical infrastructure such as: highways, train stations, metro stations, ports, airports, schools, and shopping centres. When initiated, these measures were intended to be in place for a period of two years, which was to end on December 31st, 2003, however, in his speech on March 20th, 2003, then Minister of the Interior, Nicolas Sarkozy, announced that the threat of terrorism had only elevated since 2001, and therefore this plan would continue. In this speech, he called on all private companies involved in critical infrastructure to increase their security efforts in the interest of national security.

Biotox Plan – Addressing Biological Threats – September 2001

This plan, which is under the direction of the French Department of Health, stemmed for an inter-ministerial effort which began in 1999, and was adopted in 2001. The Biotox Plan calls for closer cooperation between civilian and military agencies concerned with biological threats. On September 22, 2001, new arrangements were incorporated to increase security at facilities for the production, storage and transport of hazardous biological materials.

Speech on France's Non-Proliferation Policy - 2008

France has long encouraged disarmament of all biological and chemical weapon arsenals, but on March 21, 2008, French President Nicolas Sarkozy put forward the broadest plan for disarmament since 1991. In addition to increasing transparency on its nuclear disarmament activities, President Sarkozy also indicated that French nuclear forces would be further reduced and that France would soon reduce its allotment of nuclear warheads to a maximum of 300.

Press Kit on the French White Paper on Defence and National Security – 2008

At the same time that the White Paper of 2008 was released, the French government also released a press kit which outlined the key concepts of the White Paper. This document is far more succinct than the original and key concepts are clearly defined in layman's terms.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

8.2 Outreach to Groups – by Type

8.2.1 National Security - General

Vigipirate – French National Security Alert System

This system, which was created in 1978, provides information on the current 'level of threat' of a terrorist attack occurring. There are 4 levels of alert which are as follows:

- **Yellow:** Raise security levels to face real yet still uncertain dangers, through measures that are local and minimally disruptive of normal activity, while preparing to switch to "orange" or "red" within a few days
- **Orange**: Take measures against plausible risks of terrorist action, including the use of means that are moderately disruptive to normal public activities, while preparing to switch to "red" or "scarlet" on short notice where possible
- **Red**: Take measures against a proven risk of one or more terrorist actions, including measures to protect public institutions and putting in place appropriate means for rescue and response, authorizing a significant level of disruption to social and economic activity
- **Scarlet**: Notification of a risk of major attacks, simultaneous or otherwise, using non-conventional means and causing major devastation; preparing appropriate means of rescue and response, measures that are highly disruptive to public life are authorized.

The National Call Centre

This call centre was established to provide general and/or targeted information to the general public in regard to the cause of any event of concern, and to answer questions and using expert advice when necessary (Press Kit for the White Paper of 2008, p.45)

The White Paper Commission

In August of 2007, the French President instituted a Commission who he assigned the task of drafting a new White Paper on Defence and National Security. The Commission was composed of representatives from relevant government agencies and the armed forces, parliamentarians and qualified experts from academia and strategic think tanks. In addition to collaborating collectively, the Commission also solicited feedback from the general public through on-line hearings and numerous closed-door consultations. The outcome of this process was a White Paper which "redefined" the French Strategy. This new strategy responds to the risks emanating form either state or non-state actors and provides an all-hazards approach which responds to deliberate acts as well as natural disasters or catastrophes of an unintentional nature. (Press Kit for the White Paper of 2008, p.3)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

8.2.2 Defence-Related Initiatives

The Advisory Board for Defence and National Security

This Advisory Board was created in response to the Defence White Paper of 2008 and it is composed of independent experts appointed by the President of the Republic and senior civil service experts. The Board meets to discuss various political, financial, operational and international issues and then submits their collective opinions and assessments to the President of the Republic and the Prime Minister for their consideration. (Press Kit for the White Paper of 2008, p. 42)

Civil-Military Cooperation in the Defence of France

This cooperative form of action was created on the premise that the prevention and management of crises is comprised of private citizens as well as military personnel. This group has worked together to create new security zones and to create better emergency action plans. Participants include: first responders, operators of critical infrastructure and military personnel (France DOD web-site, 2010)

8.2.3 Science and Technology Initiatives

The Economic and Scientific Security Council

This Council provides a forum to facilitate dialogue between the various bodies involved in internal security. It is chaired by the Minister of the Interior and includes representatives from: the main research bodies, security operators, technical solution industry suppliers and the representatives from the Departments of the Defence and Research. (Press Kit for the White Paper of 2008, p.47)

8.2.4 Cyber Security Initiatives

The Security of Information Systems Agency

The Agency was created in July of 2009 and is responsible for designing and implementing preventive and reactive defence policy in order to prevent and mitigate the effects of cyber-attacks, cyber-terrorism and cyber-warfare. It is composed of a network of experts in security and information system observatories throughout the territory in defence and security zones. Each group is under the authority of the zones.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9.0 Best Practices and Lessons Learned

The following section will provide some guidance as to the most effective ways in which governments can engage their citizens, based on lessons learned from previous programs.

9.1 How to Determine the Appropriate Level of Engagement

When designing a new program or initiative which aims at including or engaging citizens in one of the methods mentioned above, it may be unclear as to the level of involvement or the type of engagement which is appropriate. Consequently, the Home Office of the United Kingdom, addressed this issue in their '*Prevent: A Communications Guide*', which was released in March of 2010. In this document, the authors provided the graphic below to provide further insight.

Figure 1: Determining the Level of Engagement

Level of Interest

Low ——————————→ High

Power ↓

Inform	Consult
Involve	Partner

(High)

Therefore, where their 'interest' of the individual or group in the topic at hand is high and their level of influence is also high, then a partnership relationship should be considered. However, where their power to influence the group or individual is low in terms of the issue at hand and therefore, so is their interest, then engagement should likely be limited to providing them with information only. (Prevent: A communications guide, 2010)

000302

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9.2 Recommended Strategies Based on Desired Level of Engagement

As illustrated in the *Concepts* section of this document, there are many methods which can be employed by government in order to either: *inform, consult with* or *actively involve* citizens in policy issues. Below is a table which was prepared by the Fife Council in the United Kingdom, which can be used as a quick reference guide to ascertain which strategies would be best suited for the type of initiative based on the desired level of involvement (Fife Council, 2010).

Figure 2: Consultation Table

	Number	Informing	Seeking Views	Participation & Partnership
Campaigns	1	● ● ●	● ○ ○	○ ○ ○
Exhibitions	2	● ● ●	● ○ ○	○ ○ ○
Local press	3	● ● ●	● ○ ○	○ ○ ○
Leaflets & Newsletters	4	● ● ●	● ● ○	○ ○ ○
Circulating Documents	5	● ● ●	● ● ○	○ ○ ○
Customer Comment Cards	6	○ ○ ○	● ● ○	○ ○ ○
Surveys	7	○ ○ ○	● ● ●	○ ○ ○
Public meetings	8	● ● ●	● ● ○	● ○ ○
Conferences	9	● ● ●	● ● ○	● ○ ○
Select Committees	10	● ● ○	● ● ○	● ○ ○
Deliberative opinion polls	11	● ○ ○	● ● ●	● ○ ○
Citizens' panels	12	● ○ ○	● ● ●	● ○ ○
Workshops	13	● ● ○	● ● ●	● ● ○
Focus groups	14	● ○ ○	● ● ●	● ● ○
Open Space	15	○ ○ ○	● ● ●	● ● ○
Community Visioning	16	● ○ ○	● ● ●	● ● ○
User panels	17	● ○ ○	● ● ●	● ● ○
Citizens' juries	18	● ● ○	● ● ●	● ● ○
Partnership approaches	19	● ○ ○	● ● ●	● ● ●

000303

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9.3 Advantages and Disadvantages of the Different Methods

Information Strategies:

The advantages of using methods which are primarily aimed at informing the general public is that they can be done quite cheaply and quickly. They are generally easy to organize and have the ability to reach large numbers of people at one time (Fife Council, p. 2)

The disadvantages of these strategies are that they do not provide an ability to gauge the effectiveness of the campaign in reaching the intended audience, may exclude segments of the population who do not speak one of the official languages or are hearing or sight-impaired and do not typically provide an opportunity for feedback (Fife Council, p. 2)

Seeking Views:

Generally speaking, the best method in order to solicit the views of a segment of, or the entire population, is to conduct a survey. Surveys can be conducted in many ways: they can be sent by mail, face-to-face, over the phone or over the Internet.

The advantages to this method include that they are familiar to most people and they can reach a large group or a targeted group of individuals. In addition, surveys are typically conducted systematically, applying quantitative research principles and therefore, results can be obtained which accurately represent the views of the entire population or a segment of the population.

The disadvantages of conducting a survey are that they can be time-consuming and costly to organize, the collection schedule may be inflexible and therefore, may not be at an optimum time for either the client or the respondent, in order to achieve optimum results. Also, a high level of knowledge with respect to survey design is required, otherwise, the sample size may be too small to provide reliable results or the questions posed may not be understood by the respondents, thereby creating a high level of non-response (Fife Council, p. 22)

Creating Partnership:

Generally speaking, building partnerships with members of the community or the general public if conducted effectively, can have a wide array of advantages, which include the following: it provides both parties with the opportunity to gain insight and expertise into complex issues, allows for resource-sharing to maximize efficiency, it allows both parties (i.e. government officials and members of the general public) to raise relevant issues, and fosters a feeling of trust in the participants and provides the government with valuable feedback regarding the effectiveness of existing programs (Queensland government web-site, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The disadvantages of these programs are that they are expensive and time-consuming. They require a high level of knowledge of the issues among all participants, and if members of the general public do not feel as though their issues are being heard or do not see action taking place as a result of these consultations, then these meetings will be deemed to be wasteful and will have the opposite effect, of making the participants more distrustful of the government then they were prior to the beginning of the process.

9.4 Citizen Engagement Checklist

This checklist was developed by the Queensland government in order to provide some insight to public officials in planning a citizen engagement process around a program or service initiative. These principles can be generally applied by any government in any form of engagement. The principles are as follows:

1. **Identify the program or service issue.**

    - What is the issue?
    - Are there any anticipated risks or challenges?
    - Have any decisions already been made?
    - What are the genuinely non-negotiable issues?

2. **Define the engagement objectives.**

    - What are the objectives of an engagement process?
    - What are the limitations and constraints in the engagement process?
    - Is consensus decision-making a goal?

3. **Identify the engagement participants.**

    - Who are the stakeholders (program/service users, providers, regulators etc.)?
    - Who should be involved in the engagement process?
    - Do specific population groups need to be targeted (e.g. the elderly, youth, people with disabilities, Indigenous Australians or people from a non-English speaking background)?
    - What is the process for effective consultation with key stakeholders internally and across government?

4. **Identify the decision-making and approval process.**

    - Who are the decision-makers?
    - What are the relevant agency decision-making processes?
    - What are the key decision-making milestones?
    - How will decisions be kept?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5. **Decide on the level of engagement.**

    - What level of engagement – information, consultation or active participation – is appropriate to the program/service issue? (See preceding section for more information on this point)

6. **Choose the engagement method/s.**

    - What method/s should be used in the engagement process?
    - Is the chosen method/s appropriate to the objectives and the participants?
    - Have non-traditional method/s been considered?

7. **Choose the engagement technique/s.**

    - What information is required by engagement participants?
    - What mechanisms are appropriate for conveying information to participants? (E.g. pamphlets, letters, PowerPoint presentations, media stories or advertisements etc.)?
    - Is the information relevant, comprehensive and appropriate?

8. **Quality control.**

    - Do those leading the engagement process have effective engagement skills?
    - Would using a skilled facilitator assist in the process?
    - What strategies are to be used to manage expectations or conflict?

9. **Maximise the ability of stakeholders to participate**.

    - What are the possible barriers to participation and the means to overcome them?
    - What are the most appropriate methods to invite participation?
    - Have special interest groups been considered?
    - Has support and advice been obtained from community leaders or organisations on relevant protocols for consulting with community members?

10. **Formulate the timetable**.

    - Is the engagement process a one-off activity, or is it ongoing?
    - Is the timetable realistic?
    - Is the engagement timed to feed into decision-making processes?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

11. Estimate the resources.

- What resources and staff are required?
- Is there a need for staff training?
- Is there a need for external personnel (e.g. a facilitator or mediator)?
- Is there a need to hire a venue, organise catering etc.?

12. **Outcomes and implementation**.

- Are the engagement outcomes clearly defined?
- How will decisions reached through engagement feed into agency decision-making processes?

13. **Feedback to participants**.

- How will engagement participants be provided feedback throughout the process?
- How will they be provided feedback on the final decision and how they contributed to that decision?
- How will the outcomes of the engagement process be conveyed to agency senior management, the Minister and other decision-makers?

14. **Evaluate the engagement process**.

- Has an engagement evaluation process been developed?
- How will a successful engagement process be defined and measured?
- How will the results of engagement be shared across the agency and across government?
- How will the lessons feed into planning for future engagement strategies?

(Engaging Queenslanders: Methods and techniques, 2007)

000307

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9.5 Best Practices in Community Engagement

Below are the best practices which were recommended to local partners under the Prevent Strategy but can be generally applied to all programs involving engagement. They are as follows:

1) **Develop a Strategy;**

2) **Identifying the key stakeholders;**

3) **Use the SMART test**: When determining your objectives it is always helpful to keep in mind the following principles:

   - **Specific**: be clear about what you want to achieve and how you want to achieve it.
   - **Measurable**: have outcomes that can be quantified in some way.
   - **Agreed**: make sure all partners and team members are in agreement regarding the objectives and who will be responsible for carrying out each specific role.
   - **Realistic**: ensure each goal is achievable within the budget and time restraints provided.
   - **Time-Specific**: agree to reasonable time limits and ensure they are specified.

4) **Understand your Audience**: 'Effective communication requires a good understanding of your audience'. Therefore, it is always vital to understand:

   - Who they are;
   - How they prefer to receive information and
   - How they perceive their lives: i.e. potential grievances.

   Once you understand your audience you can determine how to approach your communication Strategy, which will generally fall under one of the concepts below:

   - **Tier 1**: Top line communications – these are communications to everyone.
   - **Tier 2**: Messages tailored to a particular audience or geographic location.
   - **Tier 3:** Messages tailored to an individual with a special interest.

5) **Messages:** When messages are delivered, they should be:

   - Clear and consistent;
   - Should be delivered in partnership with communities;
   - Should take care to ensure that the language used is appropriate for the intended audience; and
   - Should address local concerns.

000308

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

6) **Use of language - What is said versus what is heard**: When drafting a statement which is intended to communicate a specific message it is important to understand that certain words or phases can be interpreted differently by different audiences. Therefore, to prevent your message from being misunderstood or sending the wrong message, be sure to chose your words carefully to ensure they advance your position instead of creating further barriers. To this end, the UK government has created a language guide for government outreach to Muslim communities which can be found in Annex C of the *Prevent: a Communication Guide* published in March 2010. Please see the reference guide for the link.

7) **Establishing credibility**: through previous research it has been found that citizens may be sceptical of government outreach or communications and therefore may be hesitant to trust organizations with a strong-affiliation or funding from the government. However, research has shown the demonstration of the following characteristics has contributed significantly to the credibility of individuals or organizations, particularly in relation to the Muslim community.

- **Credentials**: good level of knowledge of the subject area.
- **Personal characteristics**: Spokesperson should be well/appropriately dressed, charismatic and honest and share some element of their background with the audience, and
- **Track record**: the spokesperson should have a good track record of working with the community and addressing important issues.

(Prevent: A Communications Guide, 2010)

9.6 Clues to Good Community Engagement

According to the Queensland government, the table below set out the elements of good community engagement practices and the facts that support them. They are as follows:

Figure 3: Clues to Good Community Engagement

Elements of community engagement	**Factors that support elements of community engagement**
Will, genuine motivation	Motivation to engage and achieve an outcome Negotiated expectations and limits Preparedness to be influenced by community input Adequate planning and funding
Outcomes focus	Ensuring that engagement processes seek to achieve positive outcomes for both the government and the community Clarity and transparency regarding the way engagement activities link to broader outcomes

000309

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Relationships and trust	Accessibility Reciprocity Communication Consistency Continuity of contact Delivering on promises Responsiveness
Leadership	Shared leadership Collaborative focus for leaders Attitudes and skills of leaders
Decision-making and legitimacy	Legitimacy to influence decisions A decision-making purpose for engagement Internal approvals and support for engagement
Inclusiveness	Diversity of community included Equity of opportunity to participate Processes that are accessible and allow broad participation Information and awareness Capacity-building opportunities for community
Project management structures and procedures	Organisational arrangements Scoping Protocols Techniques and methods Timing, including transitioning and exiting Resourcing Coordination
Accountability	Engagement processes accountable as good practice Government accountability for outcomes from engagement Government and community with mutual obligations
Skills	Refer to Skills section
Satisfaction	Gauging the extent of satisfaction with engagement Managing expectations and distinguishing the process from the outcome Adjusting the process to respond to dissatisfaction
Follow-up, sustainability	Appropriate ongoing engagement Feedback Thanking participants

(Engaging Queenslanders: Methods and techniques, 2007)

000310

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9.7 What works in Community Cohesion – A Review of Six Case Studies

Through the review of six case studies, which were published in the *What works in Community cohesion* document, stakeholders identified a broad range of approaches to developing community cohesion some of which can be applied more broadly to programs aimed at outreach to particular individuals or groups.

1) **Supporting socio-economic well-being of individuals and communities:** Social inclusion and empowerment is seen as key to ensuring individuals have the resources to contribute meaningfully in communities and feel they have a stake. It is also important in avoiding antisocial behaviour and tensions relating to concern over inequitable resource distribution. Key target groups should be the most disadvantaged and those groups where tensions are most likely to arise. This will vary by area and could be a particular demographic or ethnic group.

2) **Projects among young people are seen to be key** – young people represent the future of communities, and include groups especially vulnerable to disengagement and antisocial behaviour therefore targeted initiatives can be helpful.

3) **A focus on supporting new arrivals is important** – their lack of knowledge of the country and local area means they are among the groups most at risk of social exclusion, and they are often a group that is very visible in a community.

4) **Policy makers must be constantly vigilant to the complexity of how different dimensions of community structure interact and compete.**

5) **Promoting perception of fairness in delivery of services to different groups.** Effective communications can play an integral role (discussed further below). As part of this, it is important that the concerns and needs of White working class communities are addressed.

6) **Developing English has to be central to facilitating social inclusion** of non-English speakers, and positive relationships between them and other groups.

7) **Engaging with communities in other languages has to be maintained** as this is vital for tackling disadvantage and avoiding social exclusion and associated cohesion issues.

8) **Projects that facilitate meaningful interaction between people are seen as important in this context.** They are found to be effective in promoting trust, awareness of commonality and positive relationships among participants.

9) **Communication activities to alleviate concerns about other communities must be integrated alongside service delivery work** – for example, addressing concerns arising from myths propagated by certain group or organisations, and concern over perceived unfairness in the distribution of resources.

000311

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

10) **Multi-pronged approaches are helpful.** Mass media campaigns can reach wider audiences, whilst more interactive forums can have the greatest impact on individual views, albeit among smaller numbers of people (i.e. participants). The latter can be achieved through existing groups such as neighbourhood forums, or ad hoc events such as residents' meetings set up for this specific purpose. They can be particularly effective as they provide an arena for people to vent concerns and feel they are listened to, as well as provide an arena where information can be provided to address concerns. Radio phone-ins provide benefits of both wider population coverage and interaction.

11) **Communicating on very specific issues is most effective,** rather than generalised assertions of fairness. Localised and targeted communications and activities can be helpful in enabling this approach to be taken.

12) **'Bottom-up' approach** where policy and initiatives are community led as much as possible, or where at the very least there has been community involvement.

13) **Maximise the role of the voluntary and community sector and faith groups** in leading or delivering cohesion-related initiatives.

000312

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

10.0 Lessons Learned From Previous Evaluations – by Topic

This section provides a synopsis of the general findings of previous evaluations which have been conducted into existing programs and initiatives. The findings have been divided by topic in order to provide some general insight into the 'lessons learned' from these evaluations.

10.1 Use of the Internet in Engaging Citizens

In the 21st century, the Internet is the most common vehicle for communication, in part, because it is the least expensive option. Therefore, Web 2.0 technologies such as blogs, web logs, social networking websites, video and multimedia-sharing sites and wikis are increasingly being utilized by federal agencies to communicate with the public (Wilshusen, 2010).

However, since the Internet is not available to everyone, governments will need to employ a combination of strategies in order to inform the entire population if this is the desired effect. Also, using the Internet can present risks to the security of the information held on these sites and therefore, careful review and management of these tools is required by individuals who have the necessary skills and expertise in order to ensure these tools remain productive and do not present a security risk (Engaging Queenslanders: Methods and techniques, 2007).

10.2 Private Industry's Role in Maritime Security

The recent discovery of explosives placed on board an airplane bound for Chicago on October 29th, 2010, have brought to light the need for increased measures in terms of both air and maritime cargo security. A broad policy question for governments is what the role of the private sector should be in ensuring cargo security. While there are just too many cargo movements for the government to monitor on its own, putting this responsibility on airline owners and shipping companies could force some companies out of businesses. Therefore, collaboration between government and industry is in fact necessary to ensure this security. This collaboration is the central goal of the CBP's C-TPAT program, but Security experts believe that tightening control must be "embedded" into everyday business processes and that a "trust but verify" approach should be considered. (Port and Maritime Security: Background and Issues for Congress Updated, 2005)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

10.3 Private Industry's Role in Aviation Cargo Security

According to Steve Lord, Director of Homeland Security and Justice Issues, in his recent report (June 2010) on Aviation Security: 'Transportation Security Administration (TSA), the security threat posed by terrorists introducing explosive devices in air cargo shipments is significant, and the risk and likelihood of such an attack directed at passenger aircraft is high'. However, the scope of this issue, is enormous. In 2008, it was estimated that approximately 7.3 billion pounds of cargo was transported on U.S. passenger flights—approximately 58 percent of which was transported domestically (domestic cargo) and 42 percent of which was transported on flights arriving in the United States from a foreign location (inbound cargo).

To help enhance the security of air cargo, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) mandated the Department of Homeland Security (DHS) to establish a system to physically screen 50 percent of cargo on passenger aircraft—including the domestic and inbound flights of foreign and U.S. passenger operations—by February 2009, and 100 percent of such cargo by August 2010. However, while the TSA has made progress, they are currently relying on the voluntary participation of industry stakeholders to meet the screening mandate, and to date, far fewer shippers joined the program than TSA had targeted. Therefore, legislation mandating compliance may need to be considered by government (Lord, 2010).

10.4 Ensuring Safety of Imported Products at the Source

The United States Food and Drug Administration (FDA) has established overseas offices with a total of 42 staff, in a select group of countries covering; China, Europe, India, Latin America and the Middle East, in order to build relationships with foreign stakeholders and to share information. These FDA officials have started providing training, answered questions and other assistance to help them improve their systems and better understand FDA regulations. These officials have reported increased interest in these types of services being requested, however could lead to an unmanageable workload. The GAO therefore recommended that the FDA take steps to enhance strategic planning to ensure coordination between overseas and domestic activities and to develop a workforce plan to help recruit and retain overseas staff (Food and Drug Administration: Oversees Offices, 2010)

10.5 Best Practices in Managing Risks to Critical Infrastructure

According to the GAO in their submission of May 27th, 2010 to the Honourable John L. Mica, Ranking member of the House of Representative Committee of Transportation Security:

> 'Since it is neither practical nor feasible to protect all assets and systems against every possible terrorist threat, DHS has called for using risk-informed approaches to prioritize its security-related investments and for developing plans and allocating

000314

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> resources in a way that balances security and commerce. A risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring, (GAO May 27, 2010, p. 5).

10.6 Findings of Evaluations of Community Outreach Initiatives in the United States

The concept of building trust through engagement and partnership in the United States is rooted in the community policing model developed by law enforcement professionals in the 1990's. The US Justice Department defined community policing as:

> "a philosophy that promotes organizational strategies, which support the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime."

One of its key features is the establishment of collaborative partnerships between law enforcement agencies and individuals and organizations they serve to develop solutions to problems and increase trust in police (Critical Infrastructure Protection, 2010).

Muslim Community Activities – in the United States

As United States Attorney General Eric Holder has stated publicly:

> "Members of the American Muslim community have been—and continue to be—strong partners in fighting this emerging threat [of terrorism]. They have regularly denounced terrorist acts and those who carry them out. And they have provided critical assistance to law enforcement in helping to disrupt terrorist plots and combat radicalization."

These sentiments were echoed by Alejandro Beutel of the Muslim Public Affairs Council, when he made the following statement:

> "One of the most important benefits of trusted partnerships is the ability of community members to feel comfortable enough to step forward and provide critical information to prevent any crime, including terrorism."

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

In a background paper, released in May of 2010, Beutel documents 16 terrorist plots which have been disrupted in part with the assistance of the Muslim community, nine of which involved home-grown jihadist Muslim community within the larger society." (Critical Infrastructure Protection, 2010)

Findings regarding the Risks/Challenges of Community Engagement

While there are many benefits from engaging with communities, some experts warn of 'significant challenges in the development of programs that foster *substantive relationships* rather than token discussions or community relations events'. A study of policing in Arab-American communities sponsored by the National Institute of Justice, for example, highlighted four key obstacles hindering outreach between U.S. Arabs (Christian and Muslim) and law enforcement:

- "Distrust between Arab communities and law enforcement;
- Lack of cultural awareness among law enforcement officers;
- Language barriers; and
- Concerns about immigration status and fears of deportation."

Terrorism expert Marc Sageman cautions that engagement can be perceived as a government focus on Muslim communities and he suggests that 'an important role at the federal level is to lead efforts to combat discrimination against Muslim-Americans'.

Mohamed Elibiary, the President of the *Freedom and Justice Foundation*, a Muslim community group based in Carrollton, Texas has told Congress that "while the government has publicly claimed a desire for 'partnership' with the mainstream American Muslim community, law enforcement has only offered the community a conduit to 'inform' on community members of concern." He argues that 'this "securitization" of government interactions with Muslim-American communities would be counterproductive. Outreach may be most effective when U.S. Muslim communities initiate it and community government contact revolves around countering the extremist messages popular among home-grown violent jihadists.'

Marc Sageman suggests 'it would be more appropriate for local authorities, such as a mayor's office, to perform the engagement role because they know these communities better than federal officials. An important role at the federal level is to lead efforts to combat discrimination against Muslim-Americans, an activity in which the Civil Rights Division of the (US) Department of Justice is currently engaged (Critical Infrastructure Protection, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

10.7 Evaluations of Community Outreach initiatives in the United Kingdom

A major shift has occurred in the United Kingdom's approach to citizen engagement programs since this report was completed. As such, it is important to note that the information below reflects only a snapshot in time.

Prevent and the Pathfinder Fund

In 2008, the UK government Audit Commission released the findings of their review of the Prevent program, and the Pathfinder Fund. During their review, they visited 15 sites to evaluate the effectiveness of the program, in which four themes emerged (Audit Commission 2008, 4-6):

- A need for a more clearly-defined strategic approach;
- A need for greater information sharing;
- A need for visible and effective leadership; and
- A need for formal evaluations of the program.

Other criticisms of the program have been noted, including the following:

- The exclusive focus on Muslim communities is seen as biased and as a result, many choose not to apply;
- Some of the members of the Muslim community believe that the program is part of a political agenda aimed at changing Muslim communities;
- Many Muslim communities have found the criteria too rigid and some think that funding decisions are biased in favour of Muslim groups that are well-known in the community; and
- Many believe that receiving funding from Prevent might damage their credibility, as it is tied with local government, and as such there has been difficulty finding groups who are willing to apply for funding (The Change Institute 2008).

Evaluation of the Prevent Program by the UK House of Commons' Communities and Local Government Committee

Similar concerns were voiced in the UK House of Commons' Communities and Local Government Committee's inquiry into the *Prevent* program. The Committee found that the program, as it is currently organized, is "contentious" and the individuals toward whom the program is aimed will likely never fully be accepting of it (House of Commons Communities and Local Government Committee 2010). Other main issues raised by this investigation include the following:

- **The Committee questioned the lead role taken by the Department of Communities and Local Government in the program**. The Department of Communities and Local Government is mandated with promoting cohesiveness, however many of the witnesses believed that *Prevent* undermined cohesiveness in

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the communities (House of Commons Communities and Local Government Committee 2010). As such, the Committee suggested the Department for Communities and Local Government focus more on building stronger communities;

- **Allegations of spying and surveillance in Muslim communities.** The Committee suggested that the Government should conduct an independent investigation into these allegations and provide clear direction on the type of information needed for the program and how this information is not 'information gathering' of the type undertaken by the police or security services" (House of Commons Communities and Local Government Committee 2010, 63);
- **Overlap between the Prevent and Pursue:** Many of the witnesses testified that this overlap gives the impression that community work with Muslim groups is associated with counter-terrorism efforts (House of Commons Communities and Local Government Committee 2010);
- **Program's focused on al-Qaeda inspired terrorism has led to stigmatization and a sense of alienation among Muslim communities, and has led to resentment in non-Muslim communities** (House of Commons Communities and Local Government Committee 2010); and
- **Identified a lack of risk-based assessment and an understanding of actual risk**. This has led to the program's unfocused approach which in turn led to a lack of agreement among partners regarding the goals of Prevent. Similarly, the Committee stated that because the aims and objectives of the program are unclear, monitoring and evaluation of the program has suffered (House of Commons Communities and Local Government Committee 2010).

Recommendations Made by the UK House of Commons' Communities and Local Government Committee – Prevent Program

The report states that "the development of a proportionate risk-based approach to delivering Prevent, along with greater clarity as to what the programme aims to achieve, are needed before any useful performance measures can be agreed at national and local level" (House of Commons Communities and Local Government Committee 2010, 52). Other recommendations made by the Committee include:

- Allocating some of Prevent's funding towards "encouraging participation in democratic means of debate" (29);
- Ensuring that the Government continues to prioritize investment into alleviating socio-economic deprivation;
- That universities and prisons be included in risk assessments and that work with these institutions be better co-ordinated with the Prevent program;
- That the Government provide more opportunities for empowerment and civic engagement to strengthen the engagement of all excluded groups;
- That the Government seek the advice of independent academics in determining how programs should be developed, rather than relying

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

solely on local authorities to determine which organizations are the best fits in challenging the al-Qaeda narrative.

- Sharing between local partners be improved and that more training and support be provided to front-line workers, including police and teachers (House of Commons Communities and Local Government Committee 2010).

The Committee also felt there may be too much emphasis on the theological basis of extremism and more attention may need to be placed on other factors, such as politics, policy and socio-economics, which may play an even greater role in the process of radicalisation (House of Commons Communities and Local Government Committee 2010).

The Committee also suggested that the Government should take into account current research on the risk factors for radicalisation and update CONTEST to reflect the fact that there are other factors, beyond theological causes, that are associated with radicalisation. Finally, the Committee stated that the Muslim community should be involved in developing counter-narrative to extremist views (House of Commons Communities and Local Government Committee 2010).

10.8 Effectiveness of Information Sharing Strategies

'Recent terrorist activity, such as the attempted Time Square bombing underscores the need for terrorism-related information sharing' (Government Account Office, USA).

In the past, information flow between stakeholders has been restrained, or nonexistent, for at least three reasons: a natural bureaucratic reluctance to share information, technological difficulties associated with compatibility, and legal restraints to prevent the misuse of information for unintended purposes (Information Sharing: Federal Agencies are Helping Fusion Centers, 2010).

A variety of designations have been given to information the federal government wishes to control (critical infrastructure information [see below], homeland security information, terrorism information, sensitive security information). A catch-all term for these and other designations of controlled information is "*sensitive but unclassified.*" Since much of what is considered to be critical infrastructure is owned and operated by the private sector, critical infrastructure protection relies to a large extent on the ability of the private sector and the federal government to share information (Information Sharing: Federal Agencies are Helping Fusion Centers, 2010).

However, in the wake of September 11, many information strategies were drafted in order to mandate the sharing of information across government and with the general population. Fusion centers were set-up across the US to facilitate the exchange of this information but the question remains, how effective have these strategies been in achieving these goals?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

These information sharing arrangements were evaluated by the GAO and they came to the following conclusions:

- It is unclear how open the private sector and the government have been in sharing information;
- The private sector primarily wants from government information on specific threats which the government may want to protect in order not to compromise sources or investigations;
- Much of the threat assessment done by the federal government is considered classified. For its part, the government wants specific information on vulnerabilities and incidents which companies may want to protect to prevent adverse publicity or to keep confidential company practices; and
- The private sector, too, is concerned about whether providing this information might lead to future regulatory action or other liabilities.

Therefore, successful information sharing will depend on the ability of each side to demonstrate it can hold in confidence the information exchanged (Information Sharing: Federal Agencies are Helping Fusion Centers, 2010).

Sharing information between government and the private sector is made more complex by the question of how the information will be handled within the context of the *Freedom of Information Act (FOIA).* In particular, the private sector is reluctant to share the kind of information the government wants without it being exempt from public disclosure under the existing FOIA statute. The *Homeland Security Act* (P.L. 107-296, Sec. 214) exempts information defined as **critical infrastructure information** from FOIA (as well as providing other protections). Similar FOIA exemptions are offered in other legislation. For example, the *Public Health Security and Bioterrorism Preparedness Act* (P.L. 107-188, Sec. 401, see below) exempts certain security related information from FOIA. Even with these protections in statute, it is uncertain how much information on assets, vulnerabilities, incidents, etc. is being shared with DHS, or how useful it is (Information Sharing: Federal Agencies are Helping Fusion Centers, 2010).

The FOIA exemptions for critical infrastructure information (CII) and other types of sensitive but unclassified information is not without its critics. The non-government-organizations that actively oppose government secrecy are reluctant to expand the government's ability to hold more information as classified or sensitive. These critics, and others, feel that the protections offered to CII and other types of sensitive but unclassified information is too broad and believe that controls are stifling public debate and oversight, as well as impeding technological advances that could benefit both security and the economy (Information Sharing: Federal Agencies are Helping Fusion Centers, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Voluntary or Mandatory compliance of Private Sector companies

As a general statement of policy, owners and operators of critical infrastructure are to work with the federal government on a voluntary basis. Sharing information with the federal government about vulnerability assessments, risk assessments, and taking additional protective actions is meant to be voluntary.

However, the degree to which some of the activities are mandated varies across sectors. In some cases, sectors are quite regulated, for example, Nuclear power plants must meet very specific standards for assessing their vulnerabilities whereas, other sectors such as information and telecommunication, oil and gas, and commercial (i.e., malls and office buildings) are encouraged but not mandated (Information Sharing: Federal Agencies are Helping Fusion Centers, 2010).

10.9 Evaluations of HSIN's - Public Transit Security Information

The Transportation Security Administration (TSA) in the Department of Homeland Security (DHS) shares information with public transit agencies under the direction of the Public Transportation Information Sharing and Analysis Centre (PT-ISAC). This communication is done through the public transit sub-portal on the DHS' Homeland security Information Network (HSIN- PT). In order to evaluate the effectiveness of this system, the GAO surveyed public transit agencies to gain their perceptions of the effectiveness and utility of the HSIN. The findings of this survey were as follows:

- 75% of participants reported being generally satisfied with the security-information they received. However, some felt that federal efforts could be improved;
- Respondents were least satisfied with the information in terms of the 6 dimensions of quality i.e. *relevance, validity, timeliness, completeness, action-ability*, and *ease of use*; and
- Some respondents also reported the need to streamline the information received.

Through this evaluation, the GAO identified the potential overlap between the PT-ISAC, the HSIN_PT and the TS-ISAC which all communicate similar unclassified and security-related information for public transit agencies. Further, the GAO found that a greater proportion of those agencies who were previously unaware of the HSIN were form midsize agencies, non-rail industries and those areas without their own police department. As a result, Federal and industry officials formed a working group to assess the effectiveness of the information-sharing mechanisms, including developing options to streamline current mechanisms. The recommendations of this working group will be released when finalized (Public Transit Security Information, 2010).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

10.10 Best Practices in Emergency Planning:

FEMA's National Response Framework identified the following criteria for effective response and response planning, including:

a) Acceptability - meets the requirements of anticipated scenarios and is consistent with applicable laws;
b) Adequacy;
c) Completeness;
d) Consistency and standardization of products;
e) Feasibility;
f) Flexibility;
g) Interoperability; and
h) Collaboration.

In addition, FEMA has developed standards that call for validation, review, and testing of emergency operation plans because this offers the best way to determine if such plans are understood and work. Officials should use functional and full-scale emergency management exercises to evaluate plans. Also, regularly scheduled drills, exercises and follow-up activities are critical components of emergency planning (Disaster Response: Criteria for Developing and Validating Effectiveness, 2010)

10.11 Unifying the National Effort to Combat Home-grown Jihadist Terrorism

Many experts believe that combating violent extremism must include efforts to counter the extremist radicalization that fuels hatred and violence in an effort to "prevent young American Muslims from embracing extremist ideas in the first place." Asra Nomani, author of *Standing Alone in Mecca: An American Woman's Struggle for the Soul of Islam*, writes that "we have to fundamentally challenge the interpretations of Islam that are claiming our youth…if that's not part of our strategy, we are dead in the water…." Thus, such a strategy should include "efforts to contest the extremist narrative of radicalizers, empower and network mainstream voices countering extremism, promote diversity of ideas and means of expression, and challenge extremist voices and ideas in the public domain."

How should these activities be unified into a coherent national effort? Although many agencies at all levels of government are engaged in counterterrorism activities, there is currently no unified strategy, plan, or framework specifically focused on violent extremism as it manifests itself in home-grown jihadist terrorism in the US.

Governments may wish to consider legislatively creating a mandate a strategy, framework, or plan for this effort. The Government Accountability Office (GAO) has found that:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

'Achieving meaningful results in many national security–related interagency efforts requires coordinated efforts among various actors across federal agencies; foreign, state, and local governments; non-government organizations; and the private sector. Given the number of agencies involved in U.S. government national security efforts, it is important that there be mechanisms to coordinate across agencies…Strategies can help agencies develop mutually reinforcing plans and determine activities, resources, processes, and performance measures for implementing those strategies.

A clearly-articulated national strategy or framework can prioritize activities, assign responsibility for specific tasks among departments and agencies at the Federal level, and harmonize those efforts. A strategy that clearly articulates long-term objectives, priorities, and 'lanes in the road' can go a long way to managing tension' (Critical Infrastructure Protection, 2010)'.

000323

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

11.0 Conclusions

This paper has shown that the strategy of engaging citizens in national security has been implemented by all of the countries we examined to some degree. Common threads which have been identified between the countries which we have examined from the Western World include the following:

- A broader definition of the concept of 'national security' has been adopted;
- Sharing of information is essential in preventing attacks on critical infrastructure due to the fact that 85% of these companies are privately owned. Given their high rate of interdependence, an attack on one company could cause a chain reaction, having a much larger, even catastrophic effect if an attack were to occur;
- *National Information Strategies* have been created in order to facilitate the free exchange of information to the extent that this exchange does not compromise national security[2] ;
- Governments have engaged citizens in the protection of national security in order to prepare for and prevent attacks from occurring and also to mitigate the effects should an attack occur. They have achieved these goals in the following ways:

    - By collaborating with industry and academics to identify potential risks to critical infrastructure and the development and implementation of action plans to mitigate these risks;
    - By collaborating with industry experts particularly in the fields of cyberspace and defence technology to identify and mitigate risks from new technologies;
    - By collaborating with first responders at the regional level in order to identify risks at the regional level so that these can be addressed by a national action plans and strategies
    - By implementing outreach programs for members of marginalized communities in the hopes of identifying and de-radicalizing members of the community who are at risk of resorting to extremism;
    - By working with other countries on an international level to identify and mitigate risks which cross borders and require international collaboration; and finally,
    - By informing and outreaching to the general public in order to raise awareness of and identify potential threats as they emerge to avoid a terrorist act coming into fruition.

[2] An information sharing strategy could not be located for France at this time but this may simply be due to insufficient search terms being used due to language barrier.

000324

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

There are lessons to be learned from evaluations which have been conducted into existing programs, including the following:

- Proper evaluations of potential threats and vulnerabilities are necessary for preparedness planning;
- Tests of emergency systems should be conducted periodically to identify and address weaknesses;
- Information as to potential threats as well as the tools and information necessary to prevent attacks are a necessary component of a national security strategy in the 21st century and as such, governments, may need to consider drafting legislation to mandate compliance of businesses to recommended security measures and sharing of information in order to ensure the free exchange of information and that security measures are universally employed;
- Governments should consider drafting a national security strategy to combat extremist narratives; and
- Governments should continue to collaborate with minority groups, however it may be best if these initiatives are led by grassroots community organizations in order to avoid the perception of favouring or conversely scrutinizing a segment of the population.

It is in these ways that these governments have achieved and will continue to achieve, national security goals in the 21st century.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Appendix A: Abbreviations

General:

CERT – Computer Emergency Response Team
CIKA - Critical infrastructure and key assets
CII - Critical Infrastructure Information
ECI - European Critical Infrastructure
EUCIP – European Union Critical Infrastructure Protection
GWOT - Global War on Terrorism
MSE - medium-sized enterprises
MS - Member States
NCI - National Critical Infrastructures
PPRR - prevent, prepare, respond to and recover
SME - subject matter experts
WOT – War on Terrorism

United States:

Acts:

IRTPA - Intelligence Reform and Terrorism Prevention Act
FOIA - Freedom of Information Act
NDAA - National Defense Authorization Act
NSA - National Security Act of 1947

Departments/Organizations:

ASIS - American Society for Industrial Security
BJA - Justice Programs' Bureau of Justice Assistance
CBP- Customs and Border Protection
CRCL - Civil Rights and Civil Liberties (CRCL) Engagement Team (E-Team)
CRS – Congressional Research Service
DDR&E - Office of the Director, Defence Research and Engineering
DHS – Department of Homeland Security
DNI - Office of the Director of National Intelligence's
FDA – United States Food and Drug Administration
FEMA – Federal Emergency Management Agency
GAO – Government Accountability Office
HSC - Homeland Security Council
IACP - International Association of Chiefs of Police
IP – Department of Homeland Security Office of Infrastructure Protection
ISC- Information Sharing Council
INSS - Institute for National Strategic Studies
NIC - National Intelligence Council

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

NCSD - National Cyber Security Division
NCTC – National Counterterrorism Centre
OPS - Director of the Office of Operations Coordination and Planning
PT-ISAC - Public Transportation Information Sharing and Analysis Centre
TSA - Transportation Security Administration
USDOD – US Department of Defense
USDOJ – US Department of Justice

National Security Strategies:

MSP – Maritime Security Policy
NBPS – National Border Patrol Strategy
NCIS – National Counterintelligence Strategy
NDS – National Defence Strategy
NIS – National Intelligence Strategy
NMLS – National Money Laundering Strategy
NMS – National Military Strategy
NMSCO – National Military Strategy for Cyberspace Operations
NMS-CWMD – National Military Strategy to Combat Weapons of Mass Destruction
NMSP-WOT – National Military Strategic Plan for the War on Terrorism
NSAS – National Strategy for Aviation Security
NSCT - National Strategy to Combat Terrorism
NSCTT – National Strategy to Combat Terrorist Travel
NSCWMD – National Strategy to Combat Weapons of Mass Destruction
NSHS – National Strategy for Homeland Security
NSP – National Space Policy
NSPPCIKA – National Strategy for the Physical Protection of Critical Structures and Key Assets
NSS – National Security Strategy
NSSC – National Security to Secure Cyberspace
SHDCS – Strategy for Homeland Defence and Civil Support
SVNSS – Small Vessel National Security Strategy

Reviews:

BMDR – Ballistic Missile Defence Review
BUR – Bottom's Up Review
NSCBT – National Strategy for Countering Biological Threats
NPR - Nuclear Posture Review
QDR – Quadrennial Defense Review
QHSR - Quadrennial Homeland Security Review
SPR – Space Posture Review

National Information Sharing Strategies

CTISS - Common Terrorism Information Sharing Standards
DOD ISS – Department of Defence Information Sharing Strategy

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ICISS - Intelligence Community Information Sharing Strategy
ISE - Information Sharing Environment
ISEIP – Information Sharing Environment Implementation Plan
NIS – National Intelligence Strategy
NSIS – National Strategy for Information Sharing

Outreach program:

ACSI - Americas Counter Smuggling Initiative
ADSII – Air Domain Surveillance and Intelligence Integration Plan
APP- Auxiliary Police Program
BASC – Business Alliance for Secure Commerce
BGST – Board on Global Science and Technology
BTRP - Biological Threat Reduction Prevention
CAN – Citizen Action Network
CBR - Cooperative Biological Research
CIP- Carrier Initiative Program
CIRC – The National Critical Infrastructure Resiliences Committee
CISAC - Committee on International Security and Arms Control
CISPAC – Critical Infrastructure Sector Partnership Advisory Council
COI – Communities of Interest
CSTL - Committee on Science, Technology and Law
C-TPAT - Customs-Trade Partnership Against Terrorism
DSAC - Domestic Security Alliance Council
FAC - Federal Advisory Committees
GCC- Government Coordinating Councils
HSAC- Homeland Security Advisory Council
HSIN - Homeland Security Information Network
HSINAC – Homeland Security Information Network Advisory Committee
iCAV - Integrated Common Analytical Viewer
IPP – Industry Partnership Program
JCOC - Joint Civilian Orientation Conference
LBCIP – Land Border Carrier Initiative Program
NAS – National Academy of Sciences
NCFTA - National Cyber-Forensics & Training Alliance
NIPP – National Infrastructure Protection Plan
OSAC – Overseas Security Advisory Council
RRAP - Regional Resiliency Assessment Program
SAVs - Site Assistance Visits
SCC- Sector Coordinating Councils
SLTTGCC – State, Local, Tribal and Territorial Government Coordinating Council
STD - Science & Technology Directorate
TISP – The Infrastructure Security Partnership

000328

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Australia

Departments

AAG – Australian Attorney General
ACMA - Australian Communications and Media Authority
ADF – Australian Defence Force
ASIO- Australian Secret Intelligence Organization
AUDOD – Australian Department of Defence
BLU - Business Liaison Unit
COAG - Council of the Australian Governments
DCP - Defence Capability Plan
DIC - Department of Immigration and Citizenship
DIISR - Australian Department of Innovation, Industry, Science and Research
DIT - Department of Infrastructure and Transport
DMPD - Australian Department of the Prime Minister and Cabinet
DSTO - Defense Science and Technology Organization
EMA - Emergency Management Australia
NRIC - National Research Infrastructure Council
NSSID – National Security Science and Innovation Directory
NSSIS – National Security Science and Innovation Strategy
PMSEIC - Prime Minister's Science, Engineering and Innovation Council

Information Strategy

ICT – Defence Information and Communications Technology Strategy

Outreach Programs

AISI – Australian Internet Security Initiative
ASAF – Aviation Security Advisory Forum
BGMN – Business Government Ministerial Forum
BLU – ASIO Business Liaison Unit
CIAG – Critical Infrastructure Advisory Council
CIPMA – Critical Infrastructure Protection Modelling and Analysis Program
CNVA – Computer Network Vulnerability Assessment Program
CTD - Capability and Technology Demonstrator Program
DSAN – Defence Science Access Network
IAAG – Infrastructure Assurance Advisory Groups
IT SEAG – IT Security Expert Advisory Group
MCRG - Muslim Community Reference Group
NDRF -National Disaster Resilience Framework
NIRG – National Industry Reference Group on Chemical Security
NRIG – National Research Infrastructure Council
NSA- National Security Advisor
NSSIAB - National Security Science and Innovation Advisory Board

000329

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

PMSEIC – Prime Minister's Science, Engineering and Innovation Council
PPRR- Prevent, Prepare, Respond to and Recover
RICM – Regional Industry Consultative Meeting
RPDE – Rapid Prototyping, Development and Evaluation Program
TISN – The Trusted Information Sharing Network for Critical Infrastructure Protection

European Union

CIWN – Critical Infrastructure Warning Information Network
EPCIP – European Programme for Critical Infrastructure Protection

United Kingdom

Departments

CBRN – Chemical, Biological, Radiological and Nuclear Terrorism
CO - Cabinet office
CLG – Department of Communities and Local Government
CONTEST – Countering International Terrorism Strategy
NRA - National Risk Assessments
NRR - National Risk Register
NSID – Cabinet Committee on National Security, International Relations and Development
NSS – National Security Strategy
OSCT - Office for Security and Counter Terrorism
OPM – Office of Public Management
RICU - Research, Information and Communications Unit

Information Strategy

MODIS – Ministry of Defence Information Strategy

Outreach

CIRP - Critical Infrastructure Resilience Program
PCSOs – Police Community Safety Officers
RISC – The Security and Resilience Industry Suppliers Council
SNTs – Safe Neighbourhood Teams
TAB – Technical Advisory Board

000330

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The Netherlands (translated)

Departments

AIVD – General Intelligence and Security Service of the Netherlands
CTAS – Counter Terrorism Alert System
DTN – National Risk Assessment
IBB - Civil Aviation Security Inspectorate
MII – Minister for Integration and Immigration
MIKR – Ministry of the Interior and Kingdom Relations
MIVD - Military Intelligence and Security Service
NCTB– National Coordinator for Counterterrorism
WCIT – World Congress on Information Technology

Information Strategy

SIP – Safety Information Policy

France

VRP – Vigipirate Renforcé Plan

000331

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Appendix B: Definitions

Action research: Action research can be defined as 'learning by doing' and involves a cyclical process which includes identifying a problem, planning, taking action, reflecting on outcomes and amending action based on evolving understanding. The primary difference between action research and other research is that it deliberately seeks to engage stakeholders as active participants in the research and learning process. It also differs from traditional models of research due to its iterative orientation and because it is usually led internally by staff and stakeholders rather than by an external expert.
For action research to be effective, public officials need to sensitively engage with community members, either one-on-one or in groups, and build trusting relationships within which experiences and needs can be explored. Interviews, surveys, focus groups and informal meetings can be used to support the research process. There is a high emphasis on collecting and analysing qualitative, rather than quantitative data.
(http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Advisory committees: Advisory committees are generally made up of representatives from a particular profession, industry, peak-body, community or interest group who are appointed to provide technical or specific information on often complex or multi-faceted proposal(s) or issue(s). Establishing an advisory committee enables expert and ongoing input into planning and decision-making from a range of groups and agencies that have relevant skills or knowledge. Advisory committee members may meet throughout the duration of a specific project to provide input and advice. Other advisory committees or councils may have a mandate to provide ongoing, high level policy and planning advice to Ministers, departments and others. Membership and terms of reference of the committee, including committee and participant roles and responsibilities, time frames and decision-making processes, need to be clearly articulated and agreed prior to commencement. It is important to establish whether the committee members are representing a broader group or participating as individuals.
(http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Briefings: Briefings are a technique to provide key information to agency decision-makers, Members of Parliament, other agencies and key stakeholders at regular intervals to assist them to stay informed about the progress of an engagement activity. Often one-way in nature, by raising awareness amongst key stakeholders, briefings can lead to more effective two-way communication and the identification of issues or options not previously considered. It is particularly important to provide briefings if an engagement activity could have political implications, or if the stakeholders being briefed are likely to be impacted by decisions made as a result of the engagement activity.
(http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Charrettes: A charrette or 'inquiry by design' workshop is an intensive workshop where stakeholders come together to identify issues, deliberate about preferred outcomes and create plans for the future. A charrette can be held over several days or weekends and involves participants splitting into small groups to discuss and brainstorm issues and topics. Once these groups identify options they are collated and fed back to all participants for further comment with a view to developing more formal plans. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Citizen: According to Oxford's dictionary, a citizen is an individual who is: "a member of a state, an enfranchised in habitant of a country (as opposed to an alien)" (Oxford dictionary). In Canada a citizen is a "person who is Canadian by birth or who has applied for Canadian citizenship through Citizenship and Immigration Canada and has received a citizenship certificate. (http://canadaonline.about.com/od/citizenship/g/cdncitizen.htm).

Citizen Engagement: According the to Queensland government, citizen engagement can be defined as "the many ways in which government connects with citizens in the development and implementation of policies, programs and services". (www.onlinelearning.qld.gov.au/materials/ce/online/ce/info/learning/guide/t1s1.htm)

Citizens' panels: A citizens' panel can involve large numbers of people, often between 100 and 2000, who are selected to be representative of the population. Participants agree to take part in regular deliberations about a range of issues over a period of time. The panel members are surveyed on a regular basis on specific issues or processes to track changes in attitudes, knowledge and behaviour. Approximately one-third of the panel is replaced each year to ensure it remains representative. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Community meetings: Community public meetings are one of the most familiar methods of increasing awareness about an issue or proposal and can be suitable for small and large groups. Community meetings are generally called by the agency and have a specified time, date, venue, agenda and invitation list. Opportunities may also exist to provide information, or to create consultations at existing community meetings, at the invitation of other groups. Attending existing meetings makes good use of community infrastructure, and if negotiated in advance, is likely to minimise community frustration, demonstrate respect for community processes and to lead to more coordinated engagement. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Community reference groups: Community reference groups are made up of invited representatives from a particular community who have an interest in a given topic. Reference group members attend regular meetings, represent their group or community's views and provide input into the development, implementation and evaluation of strategies, plans, programs and services.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Community profiling: Community profiling involves reviewing a range of data sources to build a picture of the demographic makeup of a community and in the case of geographic communities; the land use mix, population trends, business and employment patterns and available infrastructure. Community profiles can be established to inform decision making for a specific engagement process. Organisations including local governments and community based organisations may have existing community profiles which could be useful. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Crowdsourcing: Crowdsourcing is the act of taking tasks traditionally performed by an employee or contractor, and outsourcing it to an undefined, generally large group of people or community in the form of an open call. Users--also known as the crowd--typically form into online communities, and the crowd submits solutions. The crowd also sorts through the solutions, finding the best ones. These best solutions are then owned by the entity that broadcast the problem. (http://ideascale.com/crowdsourcing.html)

Deliberative retreats: Deliberative retreats are framed around a specific decision or action that requires the attention of key stakeholders. The chief decision-makers need to attend, including those who may oppose proposed change. The major aim of a retreat is to achieve consensus about future actions. A skilled facilitator may be able to assist with designing and conducting the retreat.
(http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Design workshops: Design workshops are structured around specific, complex issues. The main objective of a design workshop is to give a number of stakeholders an opportunity to provide information and advice and plan for creative problem solving. It is strongly suggested that a detailed agenda is provided to each participant prior to the event. Membership of a workshop group is defined, often limited to eight people and each member is encouraged to participate in preparing possible potential solutions to the issue being considered prior to the meeting.
(http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Direct Democracy: Direct Democracy is a form of democracy for which all citizens have the opportunity to participate directly in the political decision-making process. This opportunity to participate is typically only in the legislative political arena, however, could include input into how executive decisions are made as well in some cases.
(http://en.wikipedia.org/wiki/)

Discussion boards and listserves: Discussion boards are places on the Internet that people can access to engage in conversations and discussions around issues. A listserve is an automated mailing list which allows the subscribers to the list to send email messages to all other members of the list.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

E-Democracy: The term 'e-democracy' was developed by combining the words 'electronic' and 'democracy' to refer to a form of direct democracy which uses the Internet to increase citizen or civic engagement. (http://en.wikipedia.org/wiki/E-democracy)

Focus groups: Focus groups are one example of an active participation methodology used to explore the opinions, knowledge, perceptions, and concerns of individuals in regard to a particular topic. A focus group typically involves six to ten people who have some knowledge of or experience with an issue. Group discussion is led by a moderator who guides participants through a series of open-ended questions. The information gathered can provide important clues to the participants' attitudes and values as they relate to an issue. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Hacktivism: Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a *hacktivist.*
(http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci552919,00.html)

IdeaScale is online, web-based idea management software which allows the sharing of ideas from the general public. IdeaScale enables Government or companies to build communities based web-site on the simple model of crowdsourcing. The term "Crowdsourcing" in simple terms is eliciting the advice of a "crowd" of people. (http://ideascale.com).

Internet-based forums: These can be limited to certain individuals (e.g. a core group of stakeholders) or open to anyone. They can be designed to allow citizens to respond to government proposals online, read and view the comments of all participants, and engage with other citizens in dialogue centred around proposals. Generally Internet-based forums take one of two forms – issue-based forum and policy-based forum.
(http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Learning circles: Learning circles provide an effective, practical and democratic opportunity for small groups of people (generally between five and 20) to come together to discuss and learn about issues which are important to them and their community. Learning circles have been used by community groups, trade unions, churches and social justice groups for many years to help explore social and political issues and provide a forum to make decisions and take action.
(http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Open days: Open days involve providing community members with access to an office/centre/project site that they would not normally access, for a limited period of time. They provide important learning opportunities for interested citizens as well providing a forum for people to raise concerns and issues and to celebrate progress. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Open Space Technology: Open Space Technology is a large group facilitation technique for up to 1000 participants which has been used in a wide variety of circumstances including peace-making between factional groups, strategic redirection of companies in crisis, innovation and visioning sessions, knowledge sharing and community development. Open Space Technology is based on the premise that people will take ownership of issues they feel strongly about. Participants, rather than organisers, set the agenda, decide the length of the event (generally between one to three days) and the outcomes. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Participatory editing: Participatory editing provides citizens with the opportunity to shape written reports and documents, without necessarily leaving their homes. Drafts are circulated to stakeholders in hard copy or electronically for comments and feedback. An editor goes through the submitted comments and produces a revised version of the report which is then returned to the participating stakeholders for their endorsement or amendment. The process may be repeated several times. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Prefect: 'A person appointed to any of various positions of command, authority, or superintendence, as a chief magistrate in ancient Rome or the chief administrative official of a department of France or Italy.' – (Source: Dictionary.com, accessed: July 28, 2010)

Policy action teams: Policy Action Teams are responsible for an intensive program of policy development around a particular issue e.g. anti-social behaviour in a disadvantaged neighbourhood. Teams are composed of 20 to 40 members representing a cross-section of government departments, as well as experts from the community, industry and tertiary education sectors. The teams bring together the expertise of those 'on the ground' with that of public officials who have been working on the relevant issue – often in isolation. While policy action teams are encouraged to engage in 'blue skies' thinking, all recommendations must be evidence-based. Where relevant, the team may work in the community affected by the policy issue to gain first-hand experience. Teams are often chaired by a senior public official and have a 'champion' Minister, who is assigned to take a proactive role in the work of the team. A lead agency provides a supporting secretariat and careful consideration is given to how the team can maximise the contribution of communities to the policy issue and what capacity building is required to support that contribution. Policy action teams are potentially best suited to addressing issues which are complex and cut across traditional departmental boundaries and which require innovative and new perspectives. Experiences from the United Kingdom suggest

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

that teams work best when tackling policy issues which need to involve stakeholders from across the social spectrum and when it is important to have stakeholders take ownership of issues at a local or service delivery level. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Polls: Polls generally involve posing a small number of closed questions to a range of people in order to identify community opinion. The answers sought are often "yes" or "no", or scaled responses, for example, "strongly supported", "supported", "not supported", "unsure". It has become increasingly affordable to conduct polls, and in particular telephone polls, in recent years. Polls are often a suitable adjunct to public participation activities. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Social networking sites: Social networking sites, sometimes referred to as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Stakeholder segmentation: Stakeholder segmentation is a way of clustering the community into groups. By identifying the nature and size of 'segments' within a community it is possible to design a community engagement Strategy which ensures balanced engagement with each of the identified groups. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Summits: A summit is a large scale, time limited event which brings together large numbers of diverse participants to consider information, engage in dialogue and to make recommendations for action. Summits are often used in the early phases of developing strategies to address particularly complex issues. They can be both a visioning and exploratory exercise. Intensive planning is required to organise a summit. Summits are interactive and can be tailored to suit a diverse group of interested community participants, key stakeholders and policy makers. (http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

References:

Australia:

Attorney General's Office. Australia. 2008. Attorney General's Portfolio Security Environment Update 2007-08. Retrieved February 22nd, 2010 from: http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/9EDD156E9DA7C75FCA25716F000C9401?OpenDocument"

Attorney General. Australia. 2008. Security Environment Update. Retrieved February 24th, 2010 from: http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/9EDD156E9DA7C75FCA25716F000C9401?OpenDocument"

Attorney General's Office. Australia. 2009. Cyber Security Strategy. Retrieved February 22nd, 2010 from http://www.ag.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases_2009_FourthQuarter_23November2009-AustralianCyberSecurityStrategyLaunched"

Attorney General's Office. Australia. 2009. Lexicon of Terrorism. Retrieved February 24th, 2010 from: http://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/CS2U6/upload_binary/cs2u60.pdf;fileType%3Dapplication%2Fpdf.

Attorney-General's Office. Australia.2010. Countering Violent Extremism in our Community. Retrieved May 12th, 2010 from: http://www.attorneygeneral.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases_2010_SecondQuarter_11May2010-CounteringViolentExtremisminourCommunity

Attorney-General's Office. Australia 2010. National Security Campaign. Retrieved March 25th, 2010 from: http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/D1197555B9B04E9FCA256FAB00168903?OpenDocument.

Attorney-General's Office. Australia. 2010. National Security Public Service Campaign. Retrieved March 25th, 2010 from: http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/D1197555B9B04E9FCA256FAB00168903?OpenDocument.

Attorney-General's Office. Australia. 2010. Protecting Our Community. Retrieved March 25th, 2010 from: "http://www.dpmc.gov.au/publications/counter_terrorism/docs/counter-terrorism_white_paper.pdf"; accessed: March 25th 2010

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Australian Communications and Media Authority. Australia. 2010. Australian Internet Security Initiative. Retrieved May 11th, 2010 from: http://www.acma.gov.au/WEB/STANDARD...PC/pc=PC_310317

Council of Australian Government. 2008. Chemicals of Security Concern. Retrieved April 24th, 2010 from: http://www.chemicalsecurity.gov.au/www/chemsec/chemsec.nsf/Page/Chemicals_of_security_concern

Council of Australian Government. 2008. Chemical Security Management Framework. Retrieved April 24th, 2010 from: http://www.chemicalsecurity.gov.au/www/chemsec/chemsec.nsf/Page/Framework

Council of Australian Government. 2008. National Industry Reference Group. Retrieved April 24th, 2010 from: http://www.chemicalsecurity.gov.au/www/chemsec/chemsec.nsf/Page/Industry#members

Critical Infrastructure Protection Branch. Australia.. 2010. Critical Infrastructure Protection Modelling and Analysis Program. Retrieved March 28th, 2010 from: http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection#c10)

Defence Science and Technology Organization. Australia.2010. Defence Science Access Network (DSAN). Retrieved April 15th, 2010 from: http://www.dsto.defence.gov.au/dsan/.

Department of Communities. Queensland Government. Engaging Queenslanders: A guide to Community Engagement Methods and techniques. Retrieved February 26th, 2010 from: http://www.getinvolved.qld.gov.au/assets/pdfs/engaging-queenslanders-methods-and-techniques.pdf

Department of Defence. Australia. 1997. Capability and Technology Demonstrator Program. Retrieved April 15th, 2010 from: http://www.dsto.defence.gov.au/collaboration/3743/page/3687

Department of Defence. Australia.1998. Defence and Industry Strategic Policy Statement. Retrieved May 12th, 2010 from: http://www.dsto.defence.gov.au/attachments/Defence%20and%20Industry%20Strategy%20Policy%20Statement%201998.pdf

Department of Defence. Australia.2000. Defence 2000: Our Future Defence Force. Retrieved February 23rd, 2010 from: http://merln.ndu.edu/whitepapers/Australia-2000.pdf

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Defence. Australia.2003. Australian National Security Strategy: A Defence Update 2003 Retrieved February 23rd, 2010 from: http://www.defence.gov.au/ans2003/index.htm

Department of Defence. Australia.2005. Australia's National Security Strategy: Update 2005. Retrieved February 23rd, 2010 from: http://www.defence.gov.au/update2005/docs.cfm

Department of Defence. Australia.2007. Defence and Industry Policy Statement. http://www.dsto.defence.gov.au/attachments/Def_Ind_Strat_policy_2007.pdf

Department of Defence. Australia.2007. Australia's National Security Update. Retrieved February 24th, 2010 from: http://www.defence.gov.au/ans/2007/pdf/Defence_update.pdf

Department of Defence. Australia.2009. Defence Capability Plan: Public Version. Retrieved February 24th, 2010 from: http://www.defence.gov.au/dmo/id/dcp/dcp.cfm.

Department of Defence. Australia.2009. Information Strategy of Australia. Retrieved: http://www.defence.gov.au/publications/DefenceICTStrategy2009.pdf; accessed: May 12th, 2010

Department of Defence. Australia.2009. The 2009 Defence White Paper-Defending Australia in the Asia Pacific Century: Force 2030. Retrieved February 22, 2010 from: http://www.defence.gov.au/whitepaper/docs/defence_white_paper_2009.pdf

Department of Defence. Australia. 2009. The Strategic Reform Program: Delivering Force 2030. Retrieved February 28th, 2010 from: http://www.defence.gov.au/publications/reformBooklet.pdf.

Department of Defence. Australia. 2009. The Strategic Reform Program Delivering Force 2030. Retrieved April 15th, 2010 from: http://www.defence.gov.au/publications/reformBooklet.pdf.

Department of Immigration and Citizenship. Australia. 2007. Muslim Youth Summits. Retrieved May 11th, 2010 from: http://www.immi.gov.au/living-in-australia/a-diverse-australia/muslim-youth-summit.pdf.

Department of Infrastructure, Transport, Regional Development and Local Government. Australia. 2010. Aviation Security Advisory Forum. Retrieved April 25th, 2010 from: www.infrastructure.gov.au/transport/security/aviation/.

Department of Infrastructure, Transport, Regional Development and Local Government. Australia. 2009. The National Aviation Policy Statement. Retrieved April 6th, 2010 from: http://www.infrastructure.gov.au/aviation/nap/.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Infrastructure, Transport, Regional Development and Local Government. Australia. 2010. Transport Security Programs for Aviation. Retrieved April 25th, 2010 from: www.infrastructure.gov.au/transport/security/aviation/.

Department of Innovation, Industry, Science and Research. Australia. 2009. National Research Infrastructure Council. Retrieved April 22nd, 2010 from: http://www.innovation.gov.au/Section/science/Pages/nric.aspx.

Department of Innovation, Industry, Science and Research. Australia. 2010. The Prime Minister's Science and Innovation Council. Retrieved April 25th, 2010 from: http://www.innovation.gov.au/section/pmseic/pages/default.aspx.

Department of the Prime Minister and Cabinet. Australia.. http://cip.gmu.edu/archive/Australia_ProtectAUTerrorism_2006.pdf.

Department of the Prime Minister and Cabinet. Australia. 2009. The National Security Science and Innovation Strategy. Retrieved March 28th, 2010 from: http://www.dpmc.gov.au/nsst/docs/NSSIS_directory.pdf.

Department of the Prime Minister and Cabinet. Australia. 2009. The National Security Science and Innovation Directory. Retrieved March 28th, 2010 from: http://www.dpmc.gov.au/nsst/docs/NSSIS_directory.pdf.

Emergency Alert. Australia. 2009. Emergency Alert. Retrieved April 24th, 2010 from: http://www.emergencyalert.gov.au/frequently-asked-questions/what-is-emergency-alert.html.

Emergency Management Australia. 2008. Working Together To Manage Emergencies. Retrieved May 5th, 2010 from: http://www.ema.gov.au/www/emaweb/emaweb.nsf/Page/Emergency_ManagementVolunteersWorking_Together_to_Manage_Emergencies.

Food Industry Working Group. Australia. 2010. Pantry List. Retrieved May 15th, 2010 from: http://www.pantrylist.com.au/pantry/links/be-prepared/index.php.

Muslim Community Reference Group. Australia. 2006. Building on Social Cohesion, Harmony and Security: An Action Plan. Retrieved May 11th, 2010 from: http://www.immi.gov.au/living-in-australia/a-diverse-australia/mcrg_report.pdf.

Office of the Prime Minister and Cabinet. Australia. 2009. National Security Science and Technology Branch. Retrieved May 2nd, 2010 from: www.pmc.gov.au/nsst.

Office of Prime Minister and Cabinet. Australia. 2010. Counter Terrorism White Paper: Securing Australia, Protecting our Society. Retrieved February 22, 2010 from: http://www.dpmc.gov.au/publications/counter_terrorism/index.cfm.

000341

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Office of the Prime Minister and Cabinet. Australia. 2010. National Security Adviser. Retrieved May 2nd, 2010 from: http://www.dpmc.gov.au/national_security/index.cfm.

Prime Minister of Australia. 2008. Australia's First National Security Statement. Retrieved February 24th, 2010 from: http://www.pm.gov.au/node/5424.

Queensland Government. 2008. Community engagement – an overview. Retrieve March 25th, 2010 from: www.onlinelearning.qld.gov.au/materials/ce/online/ce/info/learning/guide/t1s1.htm.

RPDE. Australia. 2009. RPDE Program. Retrieved May 11th, 2010 from: □ http://www.rpde.org.au/.

Security Intelligence Organization. Australia. Business Liaison Unit. 2005. Retrieved May 3rd, 2010 from: http://www.blu.asio.gov.au/.

Trusted Information Network. Australia. 2004. Critical Infrastructure Protection National Strategy. Retrieved March 25th, 2010 from: http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(427A90835BD17F8C477D6585272A27DB)~Critical_Infrastructure_Protection_National_Strategy.pdf/$file/Critical_Infrastructure_Protection_National_Strategy.pdf.

Trusted Information Network. Australia. 2008. Good Security – Good Business. Retrieved March 25th, 2010 from: http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(99292794923AE8E7CBABC6FB71541EE1)~Good+Security+Business+final+6+November+2008.pdf/$file/Good+Security+Business+final+6+November+2008.pdf.

Trusted Information Network. Australia. 2010. CIRNEWS: For Owners and Operators of Critical Infrastructure. Vol. 7. No1. Retrieved March 28th, 2010 from: http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(966BB47E522E848021A38A20280E2386)~CIR+Newsletter+March+2010.PDF/$file/CIR+Newsletter+March+2010.PDF

Trusted Information Network. Australia. 2010. TISN web-site. February 28th, 2010 from: http://www.tisn.gov.au" http://www.tisn.gov.au.

Trusted Information Network. Australia. 2010. Publications List. Retrieved March 28th, 2010 from: http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/PublicationsA_-_Z.

Trusted Information Network. Australia. 2010. Infrastructure Assurance Advisory Groups. Retrieved March 28th, 2010 from: Networkhttp://www.tisn.gov.au/www/tisn/tisn.nsf/Page/About_the_TISNInfrastructure_Assurance_Advisory_Groups.

Trusted Information Network. Australia. 2010. Critical Infrastructure Advisory Council. Retrieved March 28th, 2010 from:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/AbouttheTISN_CriticalInfrastructureAdvisoryCouncil_CriticalInfrastructureAdvisoryCouncil.

Trusted Information Network. Australia. 2010. Critical Network Vulnerability Assessment Program. Retrieved March 14th, 2010 from: http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_ComputerNetworkVulnerabilityAssessment(CNVA)Program.

European Union:

Commission of the European Communities. European Union. 2004. Declaration on Combating Terrorism. Retrieved May 15th, 2010 from: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/79637.pdf.

Commission of the European Communities. European Union. 2004. EU Plan of Action on Combating Terrorism. Retrieved May 18th, 2010 from: http://www.consilium.europa.eu/uedocs/cmsUpload/EUplan16090.pdf.

Commission of the European Communities. European Union. 2005. Green Paper: On a European Programme for Critical Infrastructure Protection. Retrieved April 24th, 2010 from: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.

Committee on Prevention of Proliferation of Biological Weapons, Office for Central Europe and Eurasia, National Research Council. European Union. 2007. The Biological Threat Reduction Program of the Department of Defence: From Foreign Assistance to Sustainable Partnerships. Retrieved May 3rd, 2010 from: http://www.nap.edu/catalog.php?record_id=12005.

Commission of the European Communities. European Union. 2008. Proposal for a Council Decision on creating a Critical Infrastructure Warning System. Retrieved May 25th, 2010 from: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/sec/2008/2701/COM_SEC(2008)2701_EN.pdf.

European Ministers of Justice. European Union. 2009. European action plan to prevent attacks and accidents involving chemical, biological, radiological or nuclear materials. Retrieved May 16th, 2010 from: http://english.nctb.nl/current_topics/press_releases/2009/press_release_091201.aspx?cp=92&cs=25472.

European Union Committee. European Union. 2010. Protecting Europe Against Large-Scale Attacks. Retrieved May 5th, 2010 from: http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6802.htm.

000343

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

France:

France. Department of Defence. 2008. La coopération civilo-militaire sur le territoire. Retrieved July 14, 2010 from: http://213.139.102.176/livre_blanc/les_reperes/les_grandes_fonctions_strategiques/la_cooperation_civilo_militaire_sur_le_territoire.

France. Department of Defence. Le livre blanc – 1972. Retrieved July 16th, 2010 from : http://translate.google.ca/translate?hl=en&sl=fr&u=http://www.vie-publique.fr/documents-vp/livre_blanc_1972.shtml&ei=GhFPTNfBJoXSsAPf5p3PBw&sa=X&oi=translate&ct=result&resnum=2&ved=0CB4Q7gEwAQ&prev=/search%3Fq%3DLe%2Blivre%2Bblanc%2Bsur%2Bla%2Bdefense%2Bnationale%2Bof%2B1972%26hl%3Den.

France. Department of Defence. 1994. Le livre blanc – 1994 – Partie I. Retrieved July 12th, 2010 from: http://merln.ndu.edu/whitepapers/France1994part1.pdf.

France. Department of Defence. 1994. Le livre blanc – 1994 – Partie II. Retrieved July 12th, 2010 from: Retrieved July 12th, 2010 from: http://merln.ndu.edu/whitepapers/France1994part2.pdf.

France. Department of Defence. 2003. 2003 – 2008 Military Programme Bill of Law. Retrieved July 12th, 2010 from: http://merln.ndu.edu/whitepapers/France_English.pdf.

France. Department of Health. 2006. Biotox Plan. Retrieved July 22nd, 2010 from: □ http://www.sante.gouv.fr/htm/dossiers/biotox/.

France. Department of the Interior. 2003. Réunion des préfets. Retrieved July 19th, 2010: http://www.interieur.gouv.fr/sections/le_ministre/interventions/archives-nicolas-sarkozy/20-03-2003-reunion-prefets/view.

France. Office of the President of the French Republic. 2008. The French White Paper on Defence and National Security (Press Kit). Retrieved July 12th, 2010 from: http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf.

France. Office of the President of the French Republic. 2008. The French White Paper on Defence and National Security. Retrieved July 12th, 2010 from: http://merln.ndu.edu/whitepapers/France_English2008.pdf.

Santoro, David. 2010. France's Non-Proliferation Policy. Retrieved July 28th, 2010 from: http://www.ligi.ubc.ca/sites/liu/files/Publications/2010_May3_Santoro.pdf.

Van de Linde, Erik and Kevin O'Brien et al. Rand Europe. 2002. Quick scan of post 9/11 national counter-terrorism policymaking and implementation in selected European countries. Retrieved July 23rd, 2010 from: http://www.rand.org/pubs/monograph_reports/2005/MR1590.pdf.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Wikipedia. 2010. Vigipirate. Retrieved July 19th, 2010 from: tp://en.wikipedia.org/wiki/Vigipirate.

The Netherlands:

AIVD. 2004. The Netherlands. Animal Rights Activism in the Netherlands - between peaceful and burning protest. Retrieved May 15th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@48309/animal-rights_0)

AIVD. 2007. The Netherlands. Animal Rights Activism in the Netherlands -Springboard for Europe. Retrieved May 15th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@108282/animal-rights.

AIVD. 2009. The Netherlands. Animal rights extremism in the Netherlands, fragmented but growing. Retrieved May 14th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@123867/animal-rights_1.

AIVD. 2004. The Netherlands. Annual Reports of the AIVD. Retrieved April 28th, 2010 from: https://www.aivd.nl/english/publications/aivd-publications?Zoe=&ZoeWay=&index_year=&index_month=&Van=&pager_page=1.

AIVD. 2004. The Netherlands. Background of jihad recruits in the Netherlands. May 15th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@119090/background-of-jihad.

AIVD. 2004. The Netherlands. Espionage and security risks - invisible, but still existing. Retrieved May 15th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@12761/espionage-and.

AIVD. 2004. The Netherlands. From dawa to jihad - the various threats from radical Islam to the democratic legal order. Retrieved May 15th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@52983/from-dawa-to-jihad.

AIVD. 2007. The Netherlands. Resilience and Resistance. Retrieved May 14th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@126280/resilience-and.

AIVD. 2004. The Netherlands. Saudi influences in the Netherlands. Retrieved May 15th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@13421/saudi-influences-in.

AIVD. 2007. The Netherlands. The Radical Dawa in Transition, The Rise of Islamic Neoradicalism in The Netherlands. Retrieved May 15th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@108809/the-radical-dawa-in.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

AIVD. The Netherlands. Three publications on espionage from AIVD and MIVD. Retrieved May 14th, 2010 from: https://www.aivd.nl//english/publications/aivd-publications/@126059/three-publications.

AIVD. 2006. The Netherlands. Violent Jihad in the Netherlands. Retrieved May 15th, 2010 from: https://www.aivd.nl/english/publications/aivd-publications?Zoe=&ZoeWay=&index_year=&index_month=&Van=&pager_page=1.

Asser Institute. The Netherlands. 2010. New Institute for Anti terrorism in The Hague, Retrieved May 14th, 2010 from: http://www.asser.nl/Default.aspx?site_id=1&level1=13689&level2=14631&textid=37696.

Directorate-General for Public Safety and Security. The Netherlands. 2004. Performing together for public safety and security – an introduction. 2004. Retrieved May 16th, 2010 from: http://www.minbzk.nl//english/subjects/public-safety/publications/@12653/directorate_general.

Ministry of Foreign Affairs. The Netherlands. 2009. Speech at Global Initiative to Combat Nuclear Terrorism. Retrieved May 14th, 2010 from: http://www.minbuza.nl/en/News/Speeches_and_Articles/2009/June/Speech_at_Global_Initiative_to_Combat_Nuclear_Terrorism.

Ministry of the Interior and Kingdom Relations. The Netherlands. 1999. Disaster Control and Crisis Management in the Netherlands. Retrieved May 13th, 2010 from: □ http://www.minbzk.nl//english/subjects/public-safety/publications/@4710/disaster_control)

Ministry of the Interior and Kingdom Relations. The Netherlands. 2001. Citizens and Government in the information society. Retrieved May 18th, 2010 from: http://www.minbzk.nl/english/general/advanced-search?Zoe=Psychosocial%20effects%20of%20threat%20and%20protection%20–%20March%202008&ZoeWay=or&ZoeOrd=date&ZoeSitIdt=103&pager_page=10.

Ministry of the Interior and Kingdom Relations. The Netherlands. 2002. Progress Report Countering NBC attacks by terrorists. Retrieved May 13th, 2010 from: http://www.minbzk.nl//english/subjects/public-safety/publications/@3534/progress_report.

Ministry of the Interior and Kingdom Relations. The Netherlands. 2003. Critical Infrastructure Protection in the Netherlands – Part 1, Retrieved February 24th, 2010 from: http://www.minbzk.nl//english/subjects/public-safety/publications/@5241/critical.)

Ministry of Interior and Kingdom Relations. The Netherlands. 2003. Counter-terrorism in the Netherlands. Retrieved May 5th, 2010 from http://www.minbzk.nl/english/general/advanced-

000346

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

search?Zoe=Psychosocial%20effects%20of%20threat%20and%20protection%20–%20March%202008&ZoeWay=or&ZoeOrd=date&ZoeSitIdt=103&pager_page=10.

Ministry of Interior and Kingdom Relations. The Netherlands. 2004. Critical Infrastructure Protection in the Netherlands. Retrieved April 28th, 2010 from: http://www.minbzk.nl//english/subjects/public-safety/publications/@10447/critical_0.

Ministry of the Interior and Kingdom Relations. The Netherlands. 2007. National Security: Strategy and work programme 2007-2008. Retrieved May 14th, 2010 from: http://www.minbzk.nl/bzk2006uk/subjects/public-safety/publications/106955/national-security.

Ministry of the Interior and Kingdom Relations. The Netherlands. 2007. Polarization and Radicalization Action Plan 2007-2011. Retrieved May 14th, 2010 fromhttp://www.minbzk.nl//english/subjects/public-safety/national-security/publications/@115647/national-risk

Ministry of the Interior and Kingdom Relations. The Netherlands. 2007. Scenario Planning for Critical Infrastructure Protection. Retrieved May 14th, 2010 from: http://www.minbzk.nl//english/subjects/public-safety/publications/@114598/scenario-planning.

Ministry of Interior and Kingdom Relations. The Netherlands. 2008. Factsheet: Advisory Report on Large-Scale Evacuation. Retrieved April 29th, 2010 from: http://www.minbzk.nl/english/subjects/public-safety/national-security/@114277/factsheet-advisory_0.

Ministry of Interior and Kingdom Relations. The Netherlands. 2008. Final Report: National Safety & Security. Responding to risks to citizens, communities and the nation. Retrieved April 29th, 2010 from: http://www.minbzk.nl//english/subjects/public-safety/national-security/publications/@115984/final-report.

Ministry of Interior and Kingdom Relations. The Netherlands. 2008. National Risk Assessment Method Guide. Retrieved April 28th, 2010 from: http://www.minbzk.nl//english/subjects/public-safety/national-security/publications/@114278/factsheet-national_0.

Ministry of the Interior and Kingdom Relations. The Netherlands. 2009. Guidance Methodology National Safety and Security Strategy. Retrieved May 14th, 2010 from: http://www.minbzk.nl//english/subjects/public-safety/national-security/publications/@125930/guidance-methodology.

Ministry of the Interior and Kingdom Relations. The Netherlands. 2010. Factsheet: National Safety and Security Strategy. Retrieved May 14th, 2010 from:

000347

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

http://www.minbzk.nl//english/subjects/public-safety/national-security/publications/@114278/factsheet-national_0.

Ministry of the Interior and Kingdom Relations. The Netherlands. 2009. Second Report on Critical Infrastructure Protection. Retrieved May 14th, 2010 from: http://www.minbzk.nl//english/subjects/public-safety/publications/@118681/second-report-on.

Ministry of Interior and Kingdom Relations. The Netherlands. The Safety Information Policy: Connections in the field of Safety. Retrieved April 29th, 2010 from: http://english.minbzk.nl/subjects/public-safety/safety-information.

National Coordinator for Counterterrorism. The Netherlands. 2002. Recruitment for the jihad in the Netherlands. Retrieved May 14th, 2010 from: http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=3.

National Coordinator for Counterterrorism. The Netherlands. 2004. Combating Terrorism. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?simpleSearch=The+Strategy+and+work+programme+2007-2008&zoekknop=Search.

National Coordinator for Counterterrorism. The Netherlands. 2004. Counterterrorism Policy. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?simpleSearch=The+Strategy+and+work+programme+2007-2008&zoekknop=Search.

National Coordinator for Counterterrorism. The Netherlands. 2004. From Dawa to Jihad. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=3.

National Coordinator for Counterterrorism. The Netherlands. 2005. Memorandum on Society's Resilience and Integration policy. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?simpleSearch=radicalisation+broader.

National Coordinator for Counterterrorism. The Netherlands. 2005. Radicalism and Radicalization. Retrieved May 15th, 2010 from http://english.nctb.nl/search.aspx?simpleSearch=radicalisation+broader□+

National Coordinator for Counterterrorism. The Netherlands. 2006. First Inventory of Policy on Counterterrorism: Germany, France, Italy, Spain the United Kingdom and the United States. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=2.

000348

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

National Coordinator for Counterterrorism. The Netherlands. 2006. Guide Counterterrorism for companies. Retrieved May 15th, 2010 from http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=3.

National Coordinator for Counterterrorism. The Netherlands. 2006. Guide to Counter Terrorism at the Local Level. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?simpleSearch=radicalisation+broader.

National Coordinator for Counterterrorism. The Netherlands. 2006. Progress report: Policies on integration and prevention of radicalisations in the Netherlands. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?simpleSearch=radicalisation+broader+

National Coordinator for Counterterrorism. The Netherlands. 2006. Violent Jihad in the Netherlands. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?simpleSearch=radicalisation+broader+

National Coordinator for Counterterrorism. The Netherlands. 2007. Jihadists and the Internet Retrieved May 15th, 2010 from http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=3.

National Coordinator for Counterterrorism. The Netherlands. 2007. Netherlands against Terrorism campaign aims to beat radicalism at its roots. Retrieved May 14th, 2010 from: http://english.nctb.nl/current_topics/press_releases/2007/press_release_20071119.aspx?cp=92&cs=25472&action=0.

National Coordinator for Counterterrorism. The Netherlands. 2007. Radicalization in broader perspective. Retrieved May 15th, 2010 fromhttp://english.nctb.nl/search.aspx?simpleSearch=radicalisation+broader+

National Coordinator for Counterterrorism. The Netherlands. 2008. Decline and Disengagement - An analysis of processes of deradicalisation. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=2.

National Coordinator for Counterterrorism. The Netherlands. 2008. High Tech Crime, Different Types of Crime and Perpetrators. Retrieved May 15th, 2010 from http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=3.

National Coordinator for Counterterrorism. The Netherlands. 2008. Psychological Effects of Threat Protection. Retrieved May 18th, 2010 from:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

http://english.nctb.nl/search.aspx?simpleSearch=Prof.+B.P.R.+Gersons+&zoekknop=Search.

National Coordinator for Counterterrorism. The Netherlands. 2008. Salafism in the Netherlands. Retrieved May 15th, 2010 from http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=3.

National Coordinator for Counterterrorism. The Netherlands. 2008. Summary DTN. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=2.

National Coordinator for Counterterrorism. The Netherlands. 2010. Countering Violent Extremist Narratives. Retrieved May 15th, 2010 fromhttp://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=3.

National Coordinator for Counterterrorism. The Netherlands. 2010. Ideology and Strategy of Jihadism. Retrieved May 15th, 2010 http://english.nctb.nl/search.aspx?r=10&s=true&p1=radicalisation%20broader%20&select=3.

National Coordinator for Counterterrorism. The Netherlands. 2010. Islamic and Extreme Right Radicalism. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?simpleSearch=radicalisation+broader+

National Coordinator for Counterterrorism. The Netherlands. 2010. Jihadist Terrorism in the Netherlands. Retrieved May 15th, 2010 from: http://english.nctb.nl/search.aspx?simpleSearch=radicalisation+broader+

National Coordinator for Counterterrorism. The Netherlands. Civil Aviation Security Inspectorate (IBB) Retrieved May 15th, 2010 from: http://english.nctb.nl/organisation/who_is_nctb/the_organisation/IBB.aspx.

National Coordinator for Counterterrorism. The Netherlands. Counterterrorism Alert System. Retrieved May 14th, 2010 from: http://english.nctb.nl/themes/Counterterrorism_Alert_System/index.aspx.

The Hague. The Netherlands. 2006. The Hague Against Terrorism. Retrieved May 14th, 2010 from: http://www.denhaag.nl/en/expats-and-students/to/The-Hague-against-Terrorism.htm.

000350

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

United Kingdom:

Audit Commission. United Kingdom. 2008. Preventing Violent Extremism: Learning and development exercise. Report to the Home Office and Communities and Local Government. London, UK: Her Majesty's Inspectors of Constabulary. Retrieved February 3, 2010 from http://www.auditcommission.gov.uk/SiteCollectionDocuments/AuditCommissionReports/NationalStudies/20081110preventingviolentextremism.pdf

Cabinet Office. United Kingdom. 2008. Security in an Interdependent World. Retrieved February 25th, 2010 from: http://interactive.cabinetoffice.gov.uk/documents/security/national_security_Strategy.pdf

Cabinet Office. United Kingdom. 2009. Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space. Retrieved, March 25th, 2010 from: http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf.

Cabinet Office. United Kingdom. 2010. A National Information Assurance Strategy. Retrieved April 5th, 2010 from: http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/nia_Strategy.pdf.

Cabinet Office. United Kingdom. 2010. National Risk Register. Retrieved April 5th, 2010 fromhttp://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/national_risk_register/national_risk_register.pdf.

Cabinet Office. United Kingdom. 2010. Sector Resilience Plan for Critical Infrastructure 2010. Retrieved May 13th, 2010 from: http://www.cabinetoffice.gov.uk/media/349100/sector-resilience-plan.pdf.

Cabinet Office. United Kingdom. 2010. Strategic Framework and Policy Statement. Retrieved April 5th, 2010 from: http://www.cabinetoffice.gov.uk/media/349103/strategic-framework.pdf.

Cabinet Office. United Kingdom. 2009. The Road to 2010. Retrieved March 3rd, 2010 http://www.acronym.org.uk/docs/0907/roadto2010.pdf.

CERT. UK-CERT. United Kingdom. 2010 Retrieved March 22nd, 2010 from: http://www.ukcert.org.uk/.

Communities and Local Government. United Kingdom. 2007a. 'What works' in Community Cohesion. Retrieved April 16th, 2010 from: http://www.communities.gov.uk/publications/communities/whatworks.

000351

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Communities and Local Government. United Kingdom. 2004. Firm Foundations: The Government's Framework for Community Capacity Building. Retrieved April 16th, 2010 from: http://www.communities.gov.uk/publications/communities/firmfoundations.

Communities and Local Government. United Kingdom. 2007b. Preventing violent extremism: Community Leadership Fund. Retrieved February 12, 2010 from http://www.communities.gov.uk/documents/corporate/pdf/430934.pdf

Department for Children, Schools and Families. United Kingdom. 2010. Learning Together to be Safe: A Toolkit to Help Schools in the Prevention of Violent Extremism. Retrieved April 28th, 2010 from: http://www.dcsf.gov.uk/violentextremism/toolkitforschools/.

Department for International Development. United Kingdom. 2009. White Paper: Building our Common Future. Retrieved March 25th, 2010 from : http://webarchive.nationalarchives.gov.uk/+/http://www.dfid.gov.uk/about-dfid/quick-guide-to-dfid/how-we-do-it/building-our-common-future/.

Home Office. United Kingdom. 2009. The National Security Strategy of the United Kingdom: Update 2009 Security for the Next Generation. Retrieved February 23rd, 2010 from: http://www.cabinetoffice.gov.uk/media/216734/nss2009v2.pdf.

Home Office. United Kingdom. 2010. Delivering the Prevent Strategy: An Updated Guide for Local Partners. Retrieved February 22nd, 2010 from: http://www.dcsf.gov.uk/violentextremism/preventStrategy/downloads/2009%20Updated%20guide%20to%20local%20partners.pdf.

Home Office. United Kingdom. 2010. The Prevent Strategy: A Guide for Local Partners in England. Retrieved February 22nd, 2010 from: http://www.dcsf.gov.uk/violentextremism/downloads/Prevent%20Strategy%20A%20Guide%20for%20Local%20Partners%203%20June%202008.pdf.

Home Office. United Kingdom. 2010. Technical Advisory Board. Retrieved March 27th, 2010 from: http://www.homeoffice.gov.uk/counter-terrorism/technical-advisory-board/.

House of Commons Communities and Local Government Committee. 2010. Communities and Local Government Committee - Sixth Report Preventing Violent Extremism. Retrieved October 20th, 2010 from: http://www.publications.parliament.uk/pa/cm200910/cmselect/cmcomloc/65/6502.htm

Ministry of Defence. United Kingdom. 2009. MOD Information Strategy. Retrieved May 5th, 2010 from: http://www.mod.uk/NR/rdonlyres/530403AF-FC89-41E0-852F-4D2934C15001/0/2009_MODIS.pdf.

Office for Security and Counter Terrorism. United Kingdom. 2009. Countering International Terrorism: CONTEST Annual Report. Retrieved April 16th, 2010 from:

000352

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

http://webarchive.nationalarchives.gov.uk/20100418065544/http://security.homeoffice.gov.uk/news-publications/publication-search/contest/CONTEST-annual-report-2010.

Office for Security and Counter Terrorism. United Kingdom. 2010. Channel: Supporting Individuals Vulnerable to Recruitment by Violent Extremists. Retrieved May 16th, 2010 from: http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/.

Office for Security and Counter Terrorism. United Kingdom. 2010. Government Response to Lord Carlisle's 5th Annual Report on Prevention of Terrorism Act 2005. Retrieved May 16th, 2010 from: http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/.

Office for Security and Counter Terrorism. United Kingdom. 2010. Prevent: A Communications Guide. Retrieved April 16th, 2010 from: http://webarchive.nationalarchives.gov.uk/20100418065544/http://security.homeoffice.gov.uk/news-publications/publication-search/prevent/prevent-communications-guide?view=Standard&pubID=700721.

Office for Security and Counter Terrorism. United Kingdom. 2010. Social Behavioural Science Booklet. Retrieved May 6th, 2010 from: http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/news-publications/publication-search/science-technology/social-behavioural-science.

Office for Security and Counter Terrorism. United Kingdom. 2010. Strategy for Countering the Use of CBRN by Terrorists. Retrieved May 6th, 2010 from: http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/news-publications/publication-search/cbrn-guidance/strat-countering-use-of-CBRN.

Office for Security and Counter Terrorism. United Kingdom. 2010. Using Science to Counter the Threat. Retrieved April 16th, 2010 from: http://webarchive.nationalarchives.gov.uk/20100418065544/http://security.homeoffice.gov.uk/science-and-technology/.

Parliament of the United Kingdom. 2010. Publications: Joint Committee on Human Rights. Retrieved May 15th, 2010 from: http://www.publications.parliament.uk/pa/jt/jtrights.htm.

The Change Institute. 2008. Study on the best practice in cooperation between authorities and civil society with a view to the prevention and response to violent radicalisation. London, UK: The Change Institute. Retrieved February 4, 2010 from http://www.communities.gov.uk/documents/corporate/pdf/430934.pdf

United Kingdom Security and Resilience Industry Suppliers' Community. United Kingdom. 2010. RISC. Retrieved May 16th, 2010 from: http://www.riscuk.org/.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

United States:

9/11 Commission. 2004. 9/11 Commission Report. Retrieved April 18th, 2010 from: http://www.9-11commission.gov/report/911Report.pdf.

Bureau of Justice Assistance Office of Justice Programs. US Department of Justice. 1999. Operation Cooperation Partnership Profiles. Retrieved February 17th, 2010 from: http://www.ilj.org/publications/docs/Partnership_Profiles.pdf

Bureau of Justice Assistance, Office of Justice Programs. US Department of Justice. 2000. Operation Cooperation: Guidelines for Partnerships between Law Enforcement and Private Security Organizations. 2000. Retrieved February 17th, 2010 from: http://www.ilj.org/publications/docs/Operation_Cooperation.pdf

Bureau of Justice Assistance, Office of Justice Programs, US Department of Justice. 2005. Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships. New Realities in Law Enforcement in the Post 911 Era. Retrieved February 17th, 2010 from: http://www.ncjrs.gov/pdffiles1/bja/210678.pdf.

Central Intelligence Agency. United States. 2005. The National Intelligence Strategy. Retrieved February 19th, 2010 from: http://www.fas.org/irp/offdocs/nis.pdf.

Central Intelligence Agency. United States. 2007. 500 day plan: Integration and Collaboration. Retrieved April 27th, from: http://www.dni.gov/500-day-plan.pdf.

Central Intelligence Agency. United States. 2008. Intelligence Community Information Sharing Strategy. Retrieved April 23rd, 2010 from: http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf

Central Intelligence Agency. United States. 2009. The National Intelligence Strategy. Retrieved February 19th, 2010 from: http://www.dni.gov/reports/2009_NIS.pdf.

Coast Guard. United States. 2010. America's Waterway Watch. Retrieved February 22md, 2010 from: http://www.americaswaterwaywatch.us/.

Coast Guard. United States. 2010. Citizen Action Network. Retrieved February 22md, 2010 from: http://www.uscg.mil/d13/can/.

Central Intelligence Agency. United States. 2010. The CAESAR, POLO, and ESAU Papers. Retrieved April 28th, 2010 from: http://www.foia.cia.gov/cpe.asp.

Computer Emergency Readiness Team. United States. US-CERT. Retrieved May 14th, 2010 from: http://www.us-cert.gov/.

Congressional Research Service. 2005. Port and Maritime Security: Background and Issues for Congress. Retrieved: November 7th, 2010, from: www.opencrs.com.

000354

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Congressional Research Service. 2010. Critical Infrastructures: Background, Policy, and Implementation. Retrieved: November 7th, 2010, from: www.opencrs.com.

Customs and Border Protection. United States. 2004. The National Border Patrol Strategy. Retrieved April 18, 2010, from: http://www.cbp.gov/linkhandler/cgov/border_security/border_patrol/border_patrol_ohs/national_bp_Strategy.ctt/national_bp_Strategy.pdf.

Customs and Border Protection. United States. 2010. Industry Partnership Programs. Retrieved April 8th, 2010 from: http://www.cbp.gov/xp/cgov/trade/cargo_security/carriers/ipp.xml.

Dale, Catherine. National Security Strategy: Legislative Mandates, Execution to Date and Considerations for Congress, 2008. Congressional Research Service, May 28, 2008 Retrieved February 15th, 2010 from: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA485603&Location=U2&doc=GetTRDoc.pdf.

Department of Defence. United States. 2004 (unclassified version). National Military Strategy. Retrieved February 15, 2010 from: http://www.defense.gov/news/Mar2005/d20050318nms.pdf.

Department of Defence. United States. 2005. National Defence Strategy. Retrieved February 15, 2010 from: http://www.globalsecurity.org/military/library/policy/dod/nds-usa_mar2005.htm.

Department of Defence. United States. 2005. National Defence Strategy and Civil Support. Retrieved February 16, 2010 from: http://www.fas.org/irp/agency/dod/homeland.pdf.

Department of Defence. United States. 2006. National Military Strategy for Cyberspace Operations. Retrieved February 16, 2010 from: http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf

Department of Defence. United States. 2006. National Military Strategic Plan for the War on Terrorism. Retrieved February 18, 2010 from: http://www.cfr.org/publication/9795/national_military_strategic_plan_for_the_war_on_terrorism.html.

Department of Defence. United States. 2006. National Military Strategy to Combat Weapons of Mass Destruction. Retrieved February 25th, 2010 from: http://www.cfr.org/publication/10234/.

Department of Defence. United States. 2007. National Defence Strategy and Civil Support. Retrieved February 16, 2010 from: http://www.dtic.mil/futurejointwarfare/concepts/joc_hld_v20.pdf.

000355

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Defence. United States. 2007. The United States Department of Defence Information Strategy. Retrieved April 23rd, 2010 from: http://cio-nii.defense.gov/docs/InfoSharingStrategy.pdf.

Department of Defence. United States. 2008. National Defence Strategy. Retrieved February 15, 2010 from: http://www.defense.gov/news/2008%20National%20Defense%20Strategy.pdf.

Department of Defence. United States. 2009. Defence Solutions Web-site. Retrieved March 22nd, 2010 from: http://www.defensesolutions.gov/.

Department of Defence. United States. 2010. DoDTechipedia. Retrieved February My 7th, 2010 from: http://www.dtic.mil/dtic/announcements/DoDtechipedia.html.

Department of Defence. United States. 2010. Quadrennial Defence Review. Retrieved February 25th, 2010 from: http://www.defense.gov/QDR/QDR%20as%20of%2029JAN10%201600.pdf.

Department of Homeland Security. United States. 2002. National Security Strategy for Homeland Security. Retrieved, February 15, 2010 from: http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf.

Department of Homeland Security. United States. 2005, National Strategy for Maritime Security. Retrieved February 17, 2010 from: http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf.

Department of Homeland Security. United States. 2005. Maritime Transportation System Security Recommendations. Retrieved February 19th, 2010 from: http://www.dhs.gov/files/programs/editorial_0752.shtm.

Department of Homeland Security. United States. 2006. 9/11: Five Years Later: Successes and Challenges Retrieved February 16th, 2010 from: http://georgewbush-whitehouse.archives.gov/nsc/waronterror/2006/.

Department of Homeland Security. United States. 2006. Cyber Storm: Securing Cyber Space. Retrieved May 2nd, 2010 from: http://www.dhs.gov/files/training/gc_1204738275985.shtm.

Department of Homeland Security. United States. 2006. National Security Strategy to Combat Terrorist Travel. Retrieved April 20th, 2010 from: http://www.fas.org/irp/threat/travel.pdf.

Department of Homeland Security. United States. 2007. Domestic Outreach Plan: Supporting Plan to the National Strategy for Aviation and Security. Retrieved February 15ht, 2010 from: http://www.dhs.gov/xlibrary/assets/hspd16_domoutreachplan.pdf

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department Homeland Security. United States. 2007. National Security Strategy for Homeland Security. Retrieved, February 15, 2010 from: http://www.dhs.gov/xabout/history/gc_1193938363680.shtm.

Department Homeland Security. United States. 2007. National Strategy for Aviation and Security. Retrieved March 22, 2010 from: http://www.fas.org/irp/offdocs/nspd/nspd-47.pdf.

Department of Homeland Security. United States. 2008. One Team, One Mission, Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008-2013, Retrieved February 15, 2010 from: http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread .pdf

Department of Homeland Security. United States. 2008. Small Vessel National Security Strategy. Retrieved March 22nd, 2010 from: http://pacnwest.org/docs/DHSSVSS.pdf.

Department of Homeland Security. United States. 2008. United States Department of Homeland Security Charter of the Charter of the Critical Infrastructure Partnership Advisory Council. Retrieved, February 15, 2010 from: http://www.dhs.gov/xlibrary/assets/cipac/cipac_charter.pdf.

Department of Homeland Security. United States. 2009. "DHS' Strategy and Plans to Counter Small Vessel Threats Need Improvement. Retrieved February 24th, 2010 from: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_09-100_Sep09.pdf.

Department of Homeland Security. United States. 2009 National Infrastructure Advisory Council Charter. Retrieved February 24th, 2010 from: http://www.dhs.gov/xlibrary/assets/niac/niac_charter_10-13-09.pdf.

Department of Homeland Security. United States. 2009. National Infrastructure Project: Partnering to enhance protection and resiliency. Retrieved February 24th, 2010 from: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Department of Homeland Security. United States. 2009. National Infrastructure Protection Plan. Retrieved, February 15, 2010 from: http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf.

Department of Homeland Security. United States. 2009. Sector Specific Plans. Retrieved February 25th, 2010 from: http://www.dhs.gov/files/programs/editorial_0827.shtm#0.

Department of Homeland Security. United States. 2010. Critical Infrastructure Partnerships. Retrieved February 19th, 2010 from: http://www.dhs.gov/files/partnerships/editorial_0206.shtm.

000357

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Homeland Security. United States. 2010. Homeland Security Advisory Council. Retrieved February 19th, 2010 from: http://www.dhs.gov/files/committees/editorial_0331.shtm.

Department of Homeland Security. United States. 2010. National Infrastructure Advisory Council Fact Sheet. Retrieved February 24th, from: http://www.dhs.gov/xlibrary/assets/niac/niac_brochure.pdf.

Department of Homeland Security. United States. 2010. National Cyber Awareness Campaign. Retrieved April 28th, 2010 from: http://www.dhs.gov/files/cyber-awareness-campaign.shtm.

Department of Homeland Security. United States. 2010. National Security Dialogues. Retrieved April 16th, 2010 from: http://www.homelandsecuritydialogue.org.

Department of Homeland Security. United States. 2010. Quadrennial Homeland Security Review. Retrieved February 25, 2010 from: http://www.dhs.gov/xabout/gc_1208534155450.shtm.

Department of Homeland Security. United States. 2010. Science and Technology Directorate. Retrieved February 17th, 2010 from: http://www.dhs.gov/xabout/structure/editorial_0530.shtm.

Department of Justice. United States. 2006. Outreach: Civil Rights Division. Retrieved May 7th, 2010 from: http://www.justice.gov/crt/religdisc/report/part3.pdf.

Department of Justice. United States. 2009. National Security Division. Statistics on Unsealed International Terrorism and Terrorism Related Convictions. Retrieved April 25th, 2010 from: http://www.justice.gov/cjs/docs/terrorism-convictions-statistics.pdf.

Federal Bureau of Investigation. United States. 2010. FBI's Community Outreach Program. Retrieved May 11th, 2010 from: http://www.fbi.gov/congress/congress10/hovington031710.htm.

Government Accountability Office. 2010. Transportation Security: Additional Actions Could Strengthen the Security of Intermodal Transportation Facilities. Retrieved November 5th, 2010 from: www.gao.gov.

Government Accountability Office. 2010. Aviation Security: Progress Made but Actions Needed to Address Challenges in Meeting the Air Cargo Screening Mandate. Retrieved November 5th, 2010 from: www.gao.gov.

Government Accountability Office. 2010. Information Management: Challenges In Federal Agencies' Use of Web 2.0 Technologies. Retrieved November 5th, 2010 from: www.gao.gov.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Government Accountability Office. 2010. Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened. Retrieved November 5th, 2010 from: www.gao.gov.

Government Accountability Office. 2010. Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results. Retrieved November 5th, 2010 from: www.gao.gov.

Government Accountability Office. 2010. Public Transit Security Information Sharing; DHS Could Improve Information Sharing through Streamlining and Increased Outreach Retrieved November 5th, 2010 from: www.gao.gov.

General Services Administration. United States. Federal Advisory Committee Act Management Overview. Retrieved April 28th, 2010 from http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=9673.

Homeland Security Newswire. 2009. DHS' Cyber Storm III to test U.S. national cyber response plan. Retrieved April 28th, 2010 from: http://homelandsecuritynewswire.com/dhs-cyber-storm-iii-test-us-national-cyber-response-plan.

Infragard. 2010. Infragard. Retrieved November 8th, 2010 from: www.infragard.net.

Infrastructure Security Partnership. 2006. Critical Infrastructure Resilience Committee. Retrieved April 15th, 2010 from: http://www.tisp.org/index.cfm?pid=11845.

Infrastructure Security Partnership. 2006. Regional Disaster Resilience: A Guide for Developing an Action Plan. Retrieved April 15th, 2010 from http://www.tisp.org/index.cfm?cdid=10962&pid=10261.

National Academy of Sciences. 2010. Committee on International Security and Arms Control Retrieved May 4th, 2010 from: http://sites.nationalacademies.org/PGA/cisac/PGA_048467.

National Academy of Sciences. United States. 2010. Board on Global Science and Technology. Retrieved April 28th, 2010 from: http://sites.nationalacademies.org/PGA/bgst/index.htm.

National Academy of Sciences. United States. Committee on Science, Technology and Law. Retrieved April 28th, 2010 from: http://sites.nationalacademies.org/pga/stl/index.htm.

National Academy of Sciences. United States. 2006. Policy and Global Affairs Brochure. Retrieved April 30th, 2010 from: http://sites.nationalacademies.org/PGA/PGA_041186.

000359

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

National Intelligence Council. United States. 2010. Global Trends 2010. Retrieved May 6th, 2010 from: http://www.dni.gov/nic/special_globaltrends2010.html.

National Strategy for Information Sharing. 2007. Successes and Challenges in Improving Terrorism-Related Information Sharing. Retrieved February 2, 2011 from: http://www.fas.org/sgp/library/infoshare.pdf

Office of the Assistant Secretary of Defence for Public Affairs. United States. 2010. Joint Civilian Orientation Conference. Retrieved April 28th, 2010 from: http://jcoc.dod.mil/.

Overseas Security Advisory Council. United States. 2010. Overseas Security Advisory Council. Retrieved March 24th, 2010 from: https://www.osac.gov/About/index.cfm.

Program Manager, Information Sharing Environment. United States. 2006. Information Sharing Environment Implementation Plan. Retrieved April 23rd, 2010 from: http://www.ise.gov/docs/ISE-impplan-200611.pdf.

Secret Service. United States. 2010. Insider Threat Study. Retrieved May 2nd, 2010 from: http://www.secretservice.gov/ntac_its.shtml.

The White House. 2003. National Strategy for Combating Terrorism, Retrieved February 15th, 2010 from: https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

The White House. 2002. National Security Strategy. Retrieved, February 15, 2010 from: http://www.comw.org/qdr/fulltext/nss2002.pdf□

The White House. 2002. National Strategy to Combat Weapons of Mass Destruction, Retrieved February 15, 2010 from: http://www.state.gov/documents/organization/16092.pdf.

The White House. 2003. National Strategy for the Protection of Critical Infrastructure and Key Assets. Retrieved April 18, 2010, from: http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

The White House. 2003. National Strategy to Secure Cyberspace. Retrieved April 18, 2010, from: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

The White House. 2005. The National Counter-Intelligence Strategy. Retrieved April 18th, 2010 from: http://www.ncix.gov/publications/policy/FinalCIStrategyforWebMarch21.pdf.

The White House. 2006. National Strategy for Combating Terrorism, Retrieved February 15th, 2010 from: http://www.cfr.org/publication/11389/www.cfr.org/content/publications/attachments/NSCT0906.pdf.

000360

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The White House. 2006. National Security Strategy. Retrieved, February 15, 2010 from: http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/.

The White House. 2006. The National Space Policy. Retrieved April 20th, 2010 from: □ http://www.fas.org/irp/offdocs/nspd/space.pdf.

The White House. 2006. National Strategy to Combat Weapons of Mass Destruction, Retrieved February 15, 2010 from: http://www.cbsnews.com/htdocs/pdf/NSCT0906.pdf.

The White House. 2007. National Strategy for Information Sharing: Successes and Challenges to Improving Terrorism-Related Information Sharing. Retrieved April 22nd, 2010 from: http://georgewbush-whitehouse.archives.gov/nsc/infosharing/NSIS_book.pdf.

The White House. 2009. Cyberspace Policy Review: Assuring a Trusted and Resilient Information Communications Infrastructure. Retrieved March 23rd, 2010 from: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

The White House. 2009. Data.gov web-site. Retrieved February 26th, 2010 from: http://www.data.gov/.

The White House. 2009. Open Government Blog. Retrieved February 26th, 2010 from: □ http://www.whitehouse.gov/open/blog.

The White House. 2009. Open Government Dashboard. Retrieved February 26th, 2010 from: http://www.whitehouse.gov/open/around.

The White House. 2009. Open Government Directive. Retrieved February 26th, 2010 from: http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf.

The White House. 2009. National Strategy for Countering Biological Threats. Retrieved April 27th, 2010 from: http://www.whitehouse.gov/sites/default/files/National_Strategy_for_Countering_BioThreats.pdf.

The White House. 2010. National Security Strategy. Retrieved, July 18th, 2010 from: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_Strategy.pdf

Treasury Board. United States. 2002. National Money Laundering Strategy. Retrieved April 19th, 2001 from: http://www.ustreas.gov/press/releases/docs/monlaund.pdf.

Treasury Board. United States. 2007. National Money Laundering Strategy. Retrieved April 19th, 2001 from: http://www.ustreas.gov/press/releases/docs/nmls.pdf.

Wu, Tzeyoung Max. 2009. DoDTechipedia. A Way to Collaborate. IACNewsletter. Volume 12, Number 2, Summer 2009. Retrieved February 25th, 2010 from: http://iac.dtic.mil/iatac/download/Vol12_No2.pdf

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Other Sources:

Canadian Association of Chiefs of Police. 2008. Building Community Resilience to Violent Ideologies. Retrieved February 15th, 2010 from: https://www.cacp.ca/media/committees/efiles/16/422/RadicalizationEng.pdf

Canada On-Line. Definition of Citizen. Retrieved February 23rd, 2010 from: http://canadaonline.about.com/od/citizenship/g/cdncitizen.htm.

Fife Council. 2010. An Introduction to Consultation Methods. Retrieved November 8th, 2010 from: www.fife.gov.uk.

Ideascale. Idealscale web-site. Retrieved April 10th, 2010 from: http://ideascale.com.

Klaus, Hans. 2009. A New Post Cold War Definition of Security: Defining Security in the 21st century. Retrieved May 13th, 2010 from: http://knol.google.com/k/a-new-post-cold-war-definition-of-security.

Kreis, Steven. 2009. The Athenian Origins of Direct Democracy. Retrieved February 23rd, 2010 from: www.historyguide.org/ancient/lecture6b.html.

OECD. Engaging Citizens in Policy Making: Information, Consultation and Public Participation. 2001. Retrieved February 16th, 2010 from: http://www.oecd.org/dataoecd/24/34/2384040.pdf.

Search Security.com. 2007. Definition of Hacktivism. Retrieved May 3rd, 2010 from: www.SearchSecurity.com.

Wikipedia. Definitions of Direct Democracy and E-Democracy. Retrieved February 23rd, 2010 from http://en.wikipedia.org/.

000362

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

A COMPARISON OF ANTI-TERRORISM OFFENCES AND RELATED POLICE POWERS: CANADA, the UNITED STATES, the UNITED KINGDOM, AUSTRALIA, NEW ZEALAND, and FRANCE

Comprehensive Chart/Spreadsheet of Anti-Terrorism Legislation Currently Enacted or Proposed (As of 1 February 2011)

Prepared by Mélanie DESHAIES, as part of the Services Contract N°4500102198
With the Research and Statistics Division of the Department of Justice of Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada

18 APRIL 2011

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

TABLE OF CONTENTS

Sections *Pages*

TITLE (a) – Current DEFINITION of TERRORISM or TERRORIST ACTIVITY Used in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011) 4
Chart a.1 – Defining Terrorism (Summary of legal framework and approach) 4
Chart a.2 – Definition of "Terrorism" or "Terrorist activity" (Definition of notions) 7

TITLE (b) – Current ANTI-TERRORISM OFFENCES Created by the Anti-Terrorism Legislation in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011) 12
Chart b.1 – Anti-Terrorism Offences (Summary of legal framework) 12
Chart b.2 – Anti-Terrorism Offences (Definitions) 15
Chart b.3 – Proscribed Organizations (Grounds of proscription and List of organizations) 70

TITLE (c) – Current POLICE POWERS Specifically Created to Investigate Terrorism Offences in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011) 75
Chart c.1 – Police Powers and Other Investigative Tools (Summary of legal framework and approach) 75
Chart c.2 – Police Powers and Other Investigative Tools (Definitions) 77

TITLE (d) – Current SPECIAL PROCEDURES Used to Prevent the Commission of Terrorism in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011) 109
Chart d.1 – Special Procedures (Presentation and definitions) 109

TITLE (e) – Relevant GOVERNMENT PROPOSALS NOT YET ENACTED for Changes to the Current Anti-Terrorism Legislation in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011) 139
Chart e.1 – Anti-Terrorism Legislation Adopted After 1 February 2011 (Legislation and reference) 139
Chart e.2 – Government Proposals As of 1 February 2011 (Summary of relevant anti-terrorism legislation not yet enacted) 139
Chart e.3 – Government Proposals Introduced Between 1 February 2011 and 18 March 2011 (Legislation and reference) 141

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(a) Current DEFINITION of TERRORISM or TERRORIST ACTIVITY Used in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011)[1]

Since there is no universally agreed-upon definition of "terrorism" in international law, countries surveyed have enacted definitions that greatly vary in language and scope. While some national legislation provide for a direct definition of "terrorism" (United States, United Kingdom), other national legislation favour an approach that reflects the actual method of international law, which consist in defining "terrorist activity" (Canada) or "terrorist act" (Australia, New Zealand, France). This Title of the research presents the definitions of "terrorism" and "terrorist act" currently in use in Canada, the United States (US), the United Kingdom (UK), Australia, New Zealand (NZ), or France.

a.1 – Defining Terrorism	
Country	**Summary of legal framework and approach**
Canada	Canada has two definitions of terrorism: one outlined in legislation and used in criminal matters, and the other developed by case law and used in immigration matters. With regard to the later definition, please refer for instance to: *Suresh v. Canada*, 2002 SCC 1. **The present research focuses primarily on the statutory definition provided under the Canadian *Criminal Code***. In contrast to the situation in other countries, such as France or the US, no definition of "terrorist activity" existed in Canada's *Criminal Code* before the *Anti-terrorism Act* came into force in response to the events of 11 September 2001. Canada's definition of "terrorist activity" is a two parts definition. In the first part (subparagraph 83.01(1)(a) of the *Criminal Code*), terrorist activity is defined as acts or omissions in relation to certain offences found in various subsections to section 7 of the *Criminal Code*. In the second part of the definition (subparagraph 83.01(1)(b) of the *Code*), other acts or omissions are described more generally and require specific intent and motive elements to constitute terrorist activity. The first part of the Canadian definition resembles some of the definitions of "terrorism" found in US law and the *Code pénal français* (French Penal Code). However, the definition found in Canada's *Criminal Code* is more complex than the definitions existing in those countries, because it merely refers to the relevant offences by subsection numbers instead of actually describing the types of activities that constitute terrorism under Canadian criminal law. The second part of the definition of terrorist activity in the Canadian *Criminal Code* has more in common with the UK and Australian definitions, although it is both broader and narrower than the UK and Australia definitions in some respect. Characteristics that make the second part of the Canadian definition broader than the UK and Australian definition include the fact that the second part of the Canadian definition comprises acts, omissions, attempts, threats and counselled actions to be terrorism, as well as the fact that it makes explicit reference to intimidating the public or a segment of it in relation to economic security. Characteristics that make the second part of the Canadian definition narrower that the UK and Australian definitions include the fact that Canada's definition states that acts or omissions that constitute terrorism (the harms, dangers or risks to persons, damage to property or interference or disruption of essential services, facilities or systems) must be committed intentionally (in other words, a person must have intended to cause death, endanger a person's life, and so on, before their actions will constitute terrorism), as well as the fact that the second part of the Canadian definition creates a specific exception for international armed conflict undertaken in accordance with international law. The UK and Australian definitions both lack these features. With respect to the motive requirement, the second part of the Canadian definition, as well as the UK and Australian definitions, all require the act to be undertaken for a political, religious or ideological purpose or cause. Neither the US definitions nor the French definition contain such a requirement. It is to be noticed that Canada is the only country that has a provision in its *Criminal Code* clarifying that mere expression of religious, political or ideological thought, in and of itself, is not terrorism. For a detailed comparative analysis of the characteristics of the Canadian definition under the *Criminal Code*, please refer to: Jennifer BIRD, *Definitions of Terrorism in Canada, the United Kingdom, the United States, Australia and France: A Comparative Analysis*, Prepared for the Standing Senate Committee on Legal and Constitutional Affairs, Parliamentary Information and Research Service, 25 March 2008. **It is to be noticed that for its analytical component under this current Title, as well as under Title (b) *infra*, the research relies heavily, but not exclusively on Ms. Bird's analysis.**
United States	Unlike Canada and the UK, there is more than one definition of terrorism in US legislation. There are actually multiple definitions of terrorism available into either US federal law or individual states law.[2] The definitions are generally tailored to the requirements of various subject matters, such as criminal law or immigration law. As a result, in order to understand which definition applies, one must know the subject matter one is dealing with. For instance, the definitions of terrorism that are used for deciding whether or not one has committed a terrorist offence under US federal law are found in the *United States Code*, Title 18, sections 2331(1) and (5), and 2332B(g)(5). The definition of terrorism used to decide whether one has been involved in

[1] **NOTE: As a matter of greater clarity, the information identified as subparagraphs "(a)" and "(b)" respectively in the Statement of Work (namely the "Anti-terrorism offences" and the "Definition of terrorism" respectively) are presented in reverse order in the present research.**

[2] Please refer for instance to section 490.25 of the *New York Penal Code*:
http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$PEN490.25$$@TXPEN0490.25+&LIST=LAW+&BROWSER=BROWSER+&TOKEN=35912168+&TARGET=VIEW

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	terrorism according to US immigration law is found in the *United States Code*, Title 8, section 1182(3)(B)(iii). It is to be noticed that criminal law is primarily a state responsibility in the US. Accordingly, criminal laws dealing with terrorism will necessary vary from state to state. With respect to federal laws related to terrorism, all federal legislations in the US, once enacted, become integrated into the *United States Code* (*US Code*), which is a codification by subject matters of the general and permanent federal laws of the US. **The present research focuses primarily on US federal law**, and the chart below presents four (4) statutory definitions currently provided under the *US Code*. It is worth noting that the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorist Act* (also known as the *USA Patriot Act*), which was passed into law after the events of 11 September 2001, has added the definition of "domestic terrorism" and broadened what constitutes the "federal crime of terrorism" in accordance with the *US Code*. The definition of the "federal crime of terrorism" is the one that resembles most the definition provided in the Canadian *Criminal Code*, in that all the activities considered "federal crimes of terrorism" are specifically enumerated and can be found in the *US Code*. In addition, while there are many activities enumerated in the definition of the "federal crime of terrorism", the types of activities enumerated are mostly ones that are generally associated with terrorism, such as hijacking, providing material support to terrorists, and so on. Just as the type of activities that will constitute terrorism under US federal law vary depending on which part of the *US Code* one is dealing with, so do the types and levels of intent required. With respect to the definition of the "federal crime of terrorism", an act will only be considered a federal crime of terrorism if it is calculated to influence or affect the conduct of a government by intimidation or coercion, or to retaliate against government conduct (clause 2332b(g)(5)(A) of the *US Code*). In contrast to the situation in Canada and the UK, there is no specific motive requirement in any of the US definitions of terrorism. **The US special legislation governing the detention and trial of individuals initially referred to as "unlawful enemy combatants" at the US military base at Guantanamo Bay, Cuba, does not form part of the present research**.
United Kingdom	The UK has enacted the *Terrorism Act 2000* prior to the events of 11 September 2001. This *Act* superseded and replaced two other statutes that the UK Parliament had previously enacted to deal with paramilitary violence emanating from Northern Ireland, namely the *Prevention of Terrorism (Temporary Powers) Act 1989* and the *Northern Ireland (Emergency Provisions) Act 1996*. The definition of "terrorism" currently in use in the UK is found in section 1 of the *Terrorism Act 2000*. By contrast to the situation in Canada and the US, the UK appears to have only one definition of terrorism, which is used in all contexts. The definition of "terrorism" found in section 1 of the *Terrorism Act 2000* has been incorporated by reference into specific terrorism offences contained not only in the *Terrorism Act 2000*, but also in statutes that have been enacted after 11 September 2001, such as the *Anti-Terrorism, Crime & Security Act 2001*, the *Prevention of Terrorism Act 2005* and the *Terrorism Act 2006*. Terrorism, as defined in section 1 of the *Terrorism Act 2000*, encompasses not only actions that have been committed, but also threats of action. The definition does not, however, specifically include omissions. In all cases, the action or threat of action must be serious before it will qualify as "terrorism". The action or threat of action is not limited to violence or threat of violence against persons, but also includes actions or threats of actions that damage property or interfere with or disrupt electronic systems, as long as the acts or threats are serious. Under UK law, such action or threatened action will be considered "terrorism" no matter where in the world they occur (in other words, terrorism is not limited to acts or threats of action perpetrated in the UK). It is worth noting that the term "intent" is not specifically used in the definition of "terrorism" found in the *Terrorism Act 2000*. However, the requirement for intent does exist in the specific offences created in the *Terrorism Act 2000* and other related statutes. Moreover, in order for an act or threat of action to be considered "terrorism" in accordance with UK law, it must, in general, be designed to influence a government, the public, or a section of the public, wherever situated (subparagraph 1(1)(b) of the *Terrorism Act 2000*). Interestingly, this intent requirement is removed if firearms are used in the action or threat of action (subparagraph 1(3) of the *Terrorism Act 2000*). This feature makes the UK definition broader in scope than the Canadian definition of "terrorist activity", which always requires intent before an act or omission will be considered "terrorist activity" (subparagraph 83.01(1)(b) of Canada's *Criminal Code*). With respect to the motive element, before an act or threatened act will be considered "terrorism" according to UK law, it must have been undertaken in order to advance a political, religious or ideological cause (subparagraph 1(1)(c) of the *Terrorism Act 2000*).
Australia	Prior to 11 September 2001, Australia had no laws dealing specifically with terrorism, other than measures enacted by the Northern Territory. Since 11 September 2001, Australia has enacted close to 40 pieces of anti-terrorism legislation, mostly influenced by the UN Security Council resolutions and the UK anti-terrorism laws.[3] Australia's definition of "terrorist act" is found in subsection 100.1(1) of the *Criminal Code Act 1995*, as modified by the *Security Legislation Amendment (Terrorism) Act 2002*. The Australian approach in criminal matters mirrors Canada and NZ approaches, in that the definition of "terrorist act" is incorporated by reference into the specific terrorism offences provisions contained in the *Criminal Code Act 1995*. Under Australian law, an act is considered to be a "terrorist act" if it causes serious physical harm or death to a person, endangers a person's life (other than the life of the person taking the action), cause a serious risk to the health and safety of the public or a segment of it, or seriously interferes with, disrupts or destroys an electronic system, which is defined broadly in subparagraph 100.1(2) of the *Criminal Code Act 1995*. These acts are very similar to the acts that constitute "terrorist activity" under paragraph 83.01(1)(b) of the Canadian *Criminal Code*. As is the case with the UK definition of "terrorism", no specific mention is made of "omission" in the Australian definition. However, threats of actions as well as the actions themselves are "terrorist acts" under the *Criminal Code Act 1995*. Like the Canadian definition of "terrorist activity", the Australian definition of "terrorist act" specifies that advocacy, protest, dissent or industrial action that is not intended to cause death or serious physical harm, endanger the life of a person, or create a serious risk to the health and safety of the public or a segment of it, does not constitute a "terrorist act" (subparagraph 100.1(3) of the *Criminal Code Act 1995*). However, unlike the second part of the Canadian definition, the Australian definition does not create a specific exception for acts related to armed conflict under international law. Under Australian law, an act will be considered a "terrorist act" regardless of whether it occurs inside or

[3] For a partial list of Australia anti-terrorism laws, please see for instance: http://www.ema.gov.au/agd/www/nationalsecurity.nsf/AllDocs/826190776D49EA90CA256FAB001BA5EA?OpenDocument

000367

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	outside Australia, and regardless of whether the damage or harm is done inside or outside Australia. With respect to intent, Australia's definition of "terrorist act" requires the act to be done or the threat made with the intention of coercing or influencing by intimidation an Australian or foreign government or with the intention of intimidating the public or a segment of the public (clause 100.1(1)(c) of the *Criminal Code Act 1995*). With respect to the motive requirement, before an act or threat will be considered a "terrorist act" in accordance with Australian law, it must have been committed or made with the intention of advancing a political, religious or ideological cause (clause 100.1(1)(b) of the *Criminal Code Act 1995*). Finally, it is to be noticed that the Australian definition is simpler than the Canadian definition, because its lack an equivalent to the first part of Canada's definition under subparagraph 83.01(1)(a) of the *Criminal Code*. In addition, the Australian definition makes no specific reference to offences under UN conventions.
New Zealand	Prior to the events of 11 September 2001, NZ had no law dealing specifically with "terrorism". Measures akin to anti-terrorism legislation can, however, be traced back to the *Public Safety Conservation Act 1932*. Since 11 September 2001, NZ has enacted specific anti-terrorism statutes and special legislations for transnational offences, which include jurisdiction for offences that may be terrorist acts. It is worth noting that the anti-terrorism laws enacted by NZ are not, as far-reaching as the anti-terrorism legislation passed in the US, the UK or Australia for instance. The definition of "terrorist act" currently in use in NZ law is found in section 5 of the *Terrorism Suppression Act 2002*. Under this *Act*, an action requires three fundamental elements to constitute a "terrorist act". First, the act must be carried out for the purpose of advancing an ideological, political, or religious cause (subparagraph 5(2) of the *Terrorism Suppression Act 2002*). Second, the act must be done with the intent to induce terror in a civilian population, or to unduly compel or to force a government or an international organisation to do or abstain from doing any act (clause 5(2)(a) or (b) of the *Terrorism Suppression Act 2002*). Finally, the act must be intended to cause, inside or outside NZ, at least one of the outcomes enumerated under subparagraphs 5(3)(a) to (e) of the *Terrorism Suppression Act 2002*. Like the second part of Canada's definition of "terrorist activity" found in subparagraph 83.01(1)(b) of the *Criminal Code,* the scope of NZ definition of "terrorist act" excludes activities related to armed conflicts under international law, as well as participation in any protest, advocacy, or dissent, or in any strike, lockout, or other industrial action (subparagraphs 5(4) and (5) of the *Terrorism Suppression Act 2002*). In addition, like the first part of the Canadian definition found in subparagraph 83.01(1)(a) of the *Criminal Code*, the Australian definition of "terrorist act" encompasses acts that violate UN conventions specifically referred to in Schedule 3 of the *Terrorism Suppression Act 2002* (subsections 4(1) and (5)(1)(b) of the *Terrorism Suppression Act 2002*). It is to be noticed that detailed information and comprehensive analysis on the NZ anti-terrorism legislation are currently lacking. At present, the key informative source on NZ anti-terrorism laws is John E. SMITH, *New Zealand's Anti-Terrorism Campaign: Balancing Civil Liberties, National Security, And International Responsibilities*, with funding from the Ian Axford Fellowship in Public Policy (http://www.fulbright.org.nz/voices/axford/smithj.html). Mr. Smith study focuses only on the *Terrorism Suppression Act 2002* and does not covers the changes introduced after the *Counter-Terrorism Bill* was passed into six (6) separate laws by the NZ Parliament in 2003.
France	The French anti-terrorism legislation dates from 1986 and has been further developed in 1996, 2001 and 2006 over France's various experiences with terrorism. Accordingly, France already had a sophisticated anti-terrorism framework in place when the events of 11 September 2001 occurred. The last piece of French anti-terrorism law has been adopted on 14 April 2011. The definition of "acts of terrorism" ("*actes de terrorisme*") currently in use in France is provided in sections 421-1 and 421-2 of the *Code pénal* (French Penal Code). Terrorism in not defined under these provisions that list certain offences, which, in combination with a subjective element, are subject to special procedural and sentencing rules under French criminal law. The approach taken by France is similar to the one taken by the US with the definition of the "federal crime of terrorism", in that the French definition links a certain type of intent to a given list of crimes. Thus, under French law, a variety of acts already falling within the ambit of criminal law become terrorist acts when committed in a specific context with a specific intent. According to section 421-1 of the French Penal Code, before any of the acts listed in section 421-1 can be considered as an "act of terrorism", it must have been committed intentionally in connection with an individual or collective undertaking, the purpose of which is seriously to disturb the public order through intimidation or terror. The intent part of the French definition of "acts of terrorism" is very similar to the intent part of the definition of "terrorist activity" or "terrorist act" or "terrorism" found in Canada, the UK, the US, and Australia. However, the French definition may somewhat be broader than the other definitions, in that all that is required under section 421-1 of the French Penal Code is an "intention to disturb the public order through intimidation or terror" (rather than an intention to influence the government or compel it to act or refrain from acting and/or an intention to intimidate the public or a segment of it). As is the case with the various US definitions of terrorism, and in contrast to the UK definition, the Australian definition and the second part of the Canadian definition, the French definition contains no political, religious or ideological motive requirement. As a general matter, the French definition of "acts of terrorism" is easier to understand than the Canadian definition of "terrorist activity" under the *Criminal Code*, because it provides specific examples of the types of prohibited activities contained in the offences it incorporates by reference into the definition.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

a.2 – Definition of "Terrorism" or "Terrorist Activity"	
Country	**Definition of notions**
Canada "*Terrorist activity*"	***Criminal Code***[4]**:** **Sec. 83.01(1) Definitions** (1) The following definitions apply in this Part. […] "terrorist activity" means (a) an act or omission that is committed in or outside Canada and that, if committed in Canada, is one of the following offences: (i) the offences referred to in subsection 7(2) that implement the Convention for the Suppression of Unlawful Seizure of Aircraft, signed at The Hague on December 16, 1970, (ii) the offences referred to in subsection 7(2) that implement the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on September 23, 1971, (iii) the offences referred to in subsection 7(3) that implement the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on December 14, 1973, (iv) the offences referred to in subsection 7(3.1) that implement the International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on December 17, 1979, (v) the offences referred to in subsection 7(3.4) or (3.6) that implement the Convention on the Physical Protection of Nuclear Material, done at Vienna and New York on March 3, 1980, (vi) the offences referred to in subsection 7(2) that implement the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on February 24, 1988, (vii) the offences referred to in subsection 7(2.1) that implement the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on March 10, 1988, (viii) the offences referred to in subsection 7(2.1) or (2.2) that implement the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on March 10, 1988, (ix) the offences referred to in subsection 7(3.72) that implement the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on December 15, 1997, and (x) the offences referred to in subsection 7(3.73) that implement the International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on December 9, 1999, or (b) an act or omission, in or outside Canada, (i) that is committed (A) in whole or in part for a political, religious or ideological purpose, objective or cause, and (B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and (ii) that intentionally (A) causes death or serious bodily harm to a person by the use of violence, (B) endangers a person's life, (C) causes a serious risk to the health or safety of the public or any segment of the public, (D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or (E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C), and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counselling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law. […]
United States "*International terrorism*"	***United States Code***[5]**:** **Sec. 2331(1) Definitions** As used in this chapter –

[4] Canadian *Criminal Code*: http://laws-lois.justice.gc.ca/fra/lois/C-46/
[5] *United States Code*: http://www.law.cornell.edu/uscode/ See also: http://uscode.house.gov/download/ascii.shtml

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Domestic terrorism*"	(1) the term "international terrorism" means activities that – (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum; […] **Sec. 2331(5) Definitions** […] (5) the term "domestic terrorism" means activities that – (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States. […]
"*Federal crime of terrorism*"	**Sec. 2332b(g)(5) Acts of terrorism transcending national boundaries** […] (5) the term "Federal crime of terrorism" means an offense that – (A) is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and (B) is a violation of – (i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 175c (relating to variola virus), 229 (relating to chemical weapons), subsection (a), (b), (c), or (d) of section 351 (relating to congressional, cabinet, and Supreme Court assassination and kidnapping), 831 (relating to nuclear materials), 832 (relating to participation in nuclear and weapons of mass destruction threats to the United States), 842(m) or (n) (relating to plastic explosives), 844(f)(2) or (3) (relating to arson and bombing of Government property risking or causing death), 844(i) (relating to arson and bombing of property used in interstate commerce), 930(c) (relating to killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (relating to conspiracy to murder, kidnap, or maim persons abroad), 1030(a)(1) (relating to protection of computers),1030(a)(5)(A) resulting in damage as defined in 1030(c)(4)(A)(i)(II) through (VI) (relating to protection of computers), 1114 (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1361 (relating to government property or contracts), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751(a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1992 (relating to terrorist attacks and other acts of violence against railroad carriers and against mass transportation systems on land, on water, or through the air), 2155 (relating to destruction of national defense materials, premises, or utilities), 2156 (relating to national defense material, premises, or utilities), 2280 (relating to violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2332f (relating to bombing of public places and facilities), 2332g (relating to missile systems designed to destroy aircraft), 2332h (relating to radiological dispersal devices), 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), 2339C (relating to financing of terrorism), 2339D (relating to military-type training from a foreign terrorist organization), or 2340A (relating to torture) of this title; (ii) sections 92 (relating to prohibitions governing atomic weapons) or 236 (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2122 or 2284); (iii) section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with a dangerous weapon), section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life by means of weapons, on aircraft), section 46506 if homicide or attempted homicide is involved (relating to application of certain criminal laws to acts on aircraft), or section 60123(b) (relating to destruction of interstate gas or hazardous liquid pipeline facility) of title 49; or (iv) section 1010A of the Controlled Substances Import and Export Act (relating to narco-terrorism).
"*Terrorist activities*" (For the purpose of	**Sec. 1182(3)(B)(iii) Terrorist activities** […] (iii) "Terrorist activity" defined As used in this chapter, the term "terrorist activity" means any activity which is unlawful under the laws of the place where it is committed (or which, if it had been committed in the United States,

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

immigration law only)	would be unlawful under the laws of the United States or any State) and which involves any of the following: (I) The highjacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle). (II) The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained. (III) A violent attack upon an internationally protected person (as defined in section 1116(b)(4) of title 18) or upon the liberty of such a person. (IV) An assassination. (V) The use of any – (a) biological agent, chemical agent, or nuclear weapon or device, or (b) explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property. (VI) A threat, attempt, or conspiracy to do any of the foregoing.
United Kingdom "*Terrorism*" "*Terrorist*"	***Terrorism Act 2000***[6]**:** **Sec. 1 Terrorism: interpretation** (1) In this Act "terrorism" means the use or threat of action where— (a) the action falls within subsection (2), (b) the use or threat is designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public, and (c) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause. (2) Action falls within this subsection if it— (a) involves serious violence against a person, (b) involves serious damage to property, (c) endangers a person's life, other than that of the person committing the action, (d) creates a serious risk to the health or safety of the public or a section of the public, or (e) is designed seriously to interfere with or seriously to disrupt an electronic system. (3) The use or threat of action falling within subsection (2) which involves the use of firearms or explosives is terrorism whether or not subsection (1)(b) is satisfied. (4) In this section— (a) "action" includes action outside the United Kingdom, (b) a reference to any person or to property is a reference to any person, or to property, wherever situated, (c) a reference to the public includes a reference to the public of a country other than the United Kingdom, and (d) "the government" means the government of the United Kingdom, of a Part of the United Kingdom or of a country other than the United Kingdom. (5) In this Act a reference to action taken for the purposes of terrorism includes a reference to action taken for the benefit of a proscribed organisation. **Sec. 40 Terrorist: interpretation** (1) In this Part "terrorist" means a person who— (a) has committed an offence under any of sections 11, 12, 15 to 18, 54 and 56 to 63, or (b) is or has been concerned in the commission, preparation or instigation of acts of terrorism. (2) The reference in subsection (1)(b) to a person who has been concerned in the commission, preparation or instigation of acts of terrorism includes a reference to a person who has been, whether before or after the passing of this Act, concerned in the commission, preparation or instigation of acts of terrorism within the meaning given by section 1.
Australia "*Terrorist act*"	***Criminal Code Act 1995***[7]**:** **Sec. 100.1 Definitions** (1) In this Part: […] *terrorist act* means an action or threat of action where: (a) the action falls within subsection (2) and does not fall within subsection (3); and

[6] UK *Terrorism Act 2000*: http://www.legislation.gov.uk/ukpga/2000/11/contents
[7] Australian *Criminal Code Act 1995*: http://www.comlaw.gov.au/Details/C2011C00123

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(b) the action is done or the threat is made with the intention of advancing a political, religious or ideological cause; and (c) the action is done or the threat is made with the intention of: (i) coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or of part of a State, Territory or foreign country; or (ii) intimidating the public or a section of the public. [...] (2) Action falls within this subsection if it: (a) causes serious harm that is physical harm to a person; or (b) causes serious damage to property; or (c) causes a person's death; or (d) endangers a person's life, other than the life of the person taking the action; or (e) creates a serious risk to the health or safety of the public or a section of the public; or (f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to: (i) an information system; or (ii) a telecommunications system; or (iii) a financial system; or (iv) a system used for the delivery of essential government services; or (v) a system used for, or by, an essential public utility; or (vi) a system used for, or by, a transport system. (3) Action falls within this subsection if it: (a) is advocacy, protest, dissent or industrial action; and (b) is not intended: (i) to cause serious harm that is physical harm to a person; or (ii) to cause a person's death; or (iii) to endanger the life of a person, other than the person taking the action; or (iv) to create a serious risk to the health or safety of the public or a section of the public. (4) In this Division: (a) a reference to any person or property is a reference to any person or property wherever situated, within or outside Australia; and (b) a reference to the public includes a reference to the public of a country other than Australia.
New Zealand "*Terrorist act*"	***Terrorism Suppression Act 2002***[8]**:** **Sec. 5 Terrorist act defined** (1) An act is a terrorist act for the purposes of this Act if— (a) the act falls within subsection (2); or (b) the act is an act against a specified terrorism convention (as defined in section 4(1)); or (c) the act is a terrorist act in armed conflict (as defined in section 4(1)). (2) An act falls within this subsection if it is intended to cause, in any 1 or more countries, 1 or more of the outcomes specified in subsection (3), and is carried out for the purpose of advancing an ideological, political, or religious cause, and with the following intention: (a) to induce terror in a civilian population; or (b) to unduly compel or to force a government or an international organisation to do or abstain from doing any act. (3) The outcomes referred to in subsection (2) are— (a) the death of, or other serious bodily injury to, 1 or more persons (other than a person carrying out the act): (b) a serious risk to the health or safety of a population: (c) destruction of, or serious damage to, property of great value or importance, or major economic loss, or major environmental damage, if likely to result in 1 or more outcomes specified in paragraphs (a), (b), and (d): (d) serious interference with, or serious disruption to, an infrastructure facility, if likely to endanger human life: (e) introduction or release of a disease-bearing organism, if likely to devastate the national economy of a country.

[8] NZ *Terrorism Suppression Act 2002*: http://www.legislation.govt.nz/act/public/2002/0034/latest/DLM151491.html

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(4) However, an act does not fall within subsection (2) if it occurs in a situation of armed conflict and is, at the time and in the place that it occurs, in accordance with rules of international law applicable to the conflict. (5) To avoid doubt, the fact that a person engages in any protest, advocacy, or dissent, or engages in any strike, lockout, or other industrial action, is not, by itself, a sufficient basis for inferring that the person— (a) is carrying out an act for a purpose, or with an intention, specified in subsection (2); or (b) intends to cause an outcome specified in subsection (3). THIS PROVISION IS TO BE READ IN CONJUNCTION WITH: **Sec. 4 Interpretation** (1) In this Act, unless the context otherwise requires,— […] *specified terrorism convention* means any treaty specified in Schedule 3 […] *terrorist act in armed conflict* means an act— (a) that occurs in a situation of armed conflict; and (b) the purpose of which, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or abstain from doing any act; and (c) that is intended to cause death or serious bodily injury to a civilian or other person not taking an active part in the hostilities in that situation; and (d) that is not excluded from the application of the Financing Convention by article 3 of that Convention […]
France "*Acts of terrorism*"	***Code pénal* (French Penal Code)[9]:** **Article 421-1** Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes : 1° Les atteintes volontaires à la vie, les atteintes volontaires à l'intégrité de la personne, l'enlèvement et la séquestration ainsi que le détournement d'aéronef, de navire ou de tout autre moyen de transport, définis par le livre II du présent code ; 2° Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le I ivre III du présent code ; 3° Les infractions en matière de groupes de combat et de mouvements dissous définies par les articles 431-13 à 431- 17 et les infractions définies par les articles 434-6 et 441-2 à 441-5 ; 4° Les infractions en matière d'armes, de produits explosifs ou de matières nucléaires définies par le I de l'article L. 1333-9, les articles L. 1333-11 et L. 1333-13-2, le II des articles L. 1333-13- 3 et L. 1333-13-4, les articles L. 1333- 13-6, L. 2339-2, L. 2339-5, L. 2339-8 et L. 2339-9 à l'exception des armes de la 6e catégorie, L. 2339-14, L. 2339-16, L. 2341-1, L. 2341-4, L. 2341-5, L. 2342- 57 à L. 2342-62, L. 2353-4, le 1° de l'article L. 2353-5 et l' article L. 2353-13 du code de la défense ; 5° Le recel du produit de l'une des infractions prévues aux 1° à 4° ci- dessus ; 6° Les infractions de blanchiment prévues au chapitre IV du titre II du livre III du présent code ; 7° Les délits d'initié prévus à l'article L. 465-1 du code monétaire et financier. **Article 421-2** Constitue également un acte de terrorisme, lorsqu'il est intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, le fait d'introduire dans l'atmosphère, sur le sol, dans le sous-sol, dans les aliments ou les composants alimentaires ou dans les eaux, y compris celles de la mer territoriale, une substance de nature à mettre en péril la santé de l'homme ou des animaux ou le milieu naturel.

[9] *Code pénal français* (French Penal Code): http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719&dateTexte=20110416 (in French).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(b) Current ANTI-TERRORISM OFFENCES Created by the Anti-Terrorism Legislation in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011)

Since the events of 11 September 2001, the threat of international terrorism prompted governments to strengthen their respective anti-terrorism framework. In doing so, most countries surveyed have been guided by the UN resolutions and conventions, but all governments have approached the process in different ways, based on their own legal tradition and political system. As highlighted with the information provided under Title (a) of the research (*supra*), nearly all governments have either implemented for the first time or significantly expanded definition(s) of terrorism into their national law. The same applies with respect to anti-terrorism offences specifically created to respond to or cover the threat of current international terrorism. While some countries surveyed already had a significant history of law-making designed to counter certain forms of terrorism or related activities, all countries have reviewed and improved the adequacy of their anti-terrorism legislation in light of the events of 11 September 2001 (as well as other events such as the terrorist attacks in Madrid, London, and Bali). This current Title of the research deals with legislative changes related to new anti-terrorism or terrorism-related offences created during and after the year 2001 in Canada, the United States (US), the United Kingdom (UK), Australia, New Zealand (NZ), and France.

b.1 – Anti-Terrorism Offences	
Country	**Summary of legal framework**
Canada	As stated previously, the definition of "terrorist activity" currently in use in Canada is found in subsection 83.01(1) of the *Criminal Code* (as modified by the *Anti-Terrorism Act*). As regard to how this definition is used when it comes to anti-terrorism offences, the Canadian approach has been to incorporate the definition of "terrorist activity", as well as the definition of "terrorist group" found in the same subsection of the *Code*, by reference into specific *Criminal Code* offence provisions, in order to make certain defined acts in relation to terrorist activities or terrorist groups illegal. Canada's definition of terrorist activity reveals an attempt to classify a broad array of actions or failures to act as terrorist activities. As detailed previously, in the first part of the definition (subparagraph 83.01(1)(a) of the *Code*), "terrorist activity" is defined to include any act or omission committed, threatened, attempted or counselled, inside or outside Canada, with respect to terrorist offences referred to in ten (10) anti-terrorism international treaties entered into by Canada. The terrorist offences referred to in the first part of the definition can be found in various subsections of section 7 of the *Criminal Code*. Section 7 of the *Code* is a complex provision, because its various subsections make reference to numerous other sections of the *Criminal Code*. As a result, a great deal of effort is required for one to understand whether an act or omission constitutes a terrorist offence according to subsection 83.01(1) of Canada's *Criminal Code*. The Canadian definition of terrorist activity is not limited to actions or omissions that are offences under certain subsections of section 7. The second part of the definition (subparagraph 83.01(1)(b) of the *Code*) additionally defines terrorist activity to include a variety of other acts or omissions committed, threatened, attempted or counselled with a specific intent and motive. In all cases, the act or omission must be serious before it will be considered terrorist activity. The acts or omissions are not limited to violence against persons, and also include acts or omission that cause substantial property damage, whether to public or private property that is likely to cause serious harm, danger or risk to persons, as well as acts or omissions that cause serious interference with or serious disruption of an essential service, facility or system. An act or omission will be considered "terrorist activity" regardless of whether or not it occurs inside or outside Canada. As noted previously, the scope of Canada's definition of terrorist activity excludes activities related to armed conflicts under international law, as well as serious interferences with or disruptions of essential services, facilities and systems as a result of advocacy, protest, dissent or work stoppage. It is to be noticed that the *Anti-terrorism Act* of 2001 has also introduced several new offences specifically designed to capture the activities of terrorists or terrorist groups into the *Criminal Code* (see sections 83.02 and sq.). Because these new offences incorporate the definition of "terrorist activity" or "terrorist group" set out in section 83.01(1) of the *Criminal Code*, they have an ambit as extensive as the definition they incorporate. The Chart b.2 below presents a general overview of the terrorism offences provided in the Canadian *Criminal Code*.
United States	As stated previously, the US has several statutory definitions of terrorism within the *United States Code* (*US Code*) alone. By creating many different definitions of terrorism, legislative bodies in the US have been able to tailor each definition to fit the relevant subject matter. The disadvantage of this approach is that there are so many different definitions of terrorism that it is difficult, especially for a layperson, to know exactly which activities are considered to be terrorism offences under US law. The information provided under this current Title of the research focuses on US federal law and more precisely on offences that constitute "federal crimes of terrorism" under section 2332b(g)(5) of the *US Code*. The definitions of "international terrorism" and "domestic terrorism" provided in other sections of the *US Code* are extremely complex, in that they require one to have knowledge of all the acts involving violence and/or acts that are dangerous to human life in US federal and individual state law, in order to determine whether a specific act constitutes a terrorism offence. The definition of "federal crime of terrorism" is a bit less complex, because all the offences considered by this definition can be found in the definition itself and in the *US Code* (in other words, there is no need to have recourse to individual states laws in order to know whether or not a specific offences or activity is a federal crime of terrorism). The US definition of "federal crime of terrorism" couples a list of so-called regular criminal offences, like homicide, attempted homicide or bombing, with a specific intent. It is the specific intent that causes a regular offence to become a terrorist offence. Thus, according to

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	clause 2332b(g)(5)(A) of the *US Code*, an act will only be considered a "federal crime of terrorism" if it is calculated to influence or affect the conduct of a government by intimidation or coercion, or to retaliate against government conduct. The enumeration of activities provided under clause 2332b(g)(5)(B) of the *US Code* makes it relatively easy to determine whether or not a specific act would be considered a "federal crime of terrorism" under US law. By contrast, the second part of the Canadian's definition of "terrorist activity" is more general in nature. Under subparagraph 83.01(1)(b) of Canada's *Criminal Code*, some types of activities are described, but no specific *Criminal Code* offences are mentioned. This approach makes the Canadian definition of "terrorist activity" arguably broader than the definition of the "federal crime of terrorism" found in the *US Code*. With respect to a motive element, it is to be recalled that none of the various definitions of terrorism found in the *US Code*, including that of "federal crime of terrorism", contain a motive requirement.
United Kingdom	There are currently six (6) main pieces of legislation in force in the UK dealing with terrorism. While the UK anti-terrorism laws enacted prior to 2000 provided mainly for offences addressing paramilitary violence emanating from Northern Ireland, the legislative changes introduced as of the year 2000 are more specifically adapted to respond to international terrorism. The new offences that have been created by the UK Parliament are found in three Acts, namely the *Terrorism Act 2000*, the *Anti-Terrorism, Crime & Security Act 2001*, and the *Terrorism Act 2006*. These Acts provide for "terrorist offences" such as those related to the funding of and support of terrorist groups or activities. Except for these specific terrorist offences, most suspected terrorists in the UK are prosecuted under general criminal law offences, such as murder or other crimes against the person, criminal damage, hostage taking and their associate inchoate offences. Other offences committed by terrorists are for instance causing explosion[10], bomb making[11], and the illegal possession of firearms or explosives.[12] The Chart b.2 below provides an overview of the most important terrorist offences introduced in UK law through the three abovementioned Acts enacted as of the year 2000. As stated previously, the general definition of "terrorism" currently in use in the UK is found in section 1 of the *Terrorism Act 2000*. This definition has been incorporated by reference into specific terrorism offences contained in the *Terrorism Act 2000*, as well as in the *Anti-Terrorism, Crime & Security Act 2001* and the *Terrorism Act 2006*. As indicated in the Charts under Title (a) of the research (*supra*), the word "intent" is not specifically referred to in the definition of terrorism under section 1 of the *Terrorism Act 2000*. The requirement for intent is, however, provided in specific offences created in the *Terrorism Act 2000* and the other related statutes, which incorporate the definition of terrorism by reference. As detailed previously, for an act or threat of action to constitute "terrorism" in accordance with UK law, it must be designed to influence a government, the public, or a section of the public, wherever situated (subparagraph 1(1)(b) of the *Terrorism Act 2000*). However, if a firearm is involved in the action or threat, the requirement that the act be designed to influence a government, the public and so on, becomes irrelevant (subparagraph 1(3) of the *Terrorist Act 2000*). With respect to the motive requirement, an act or threatened act must have been undertaken to advance a political, religious or ideological cause in order to be considered "terrorism" under UK law (subparagraph 1(1)(c) of the *Terrorism Act 2000*). It is interesting to note that unlike the Canadian definition of "terrorist activity", the UK definition of "terrorism" does not refer to UN conventions. Acts that violate UN conventions are instead prohibited as separate offences in UK statutes (see, for instance, subsection 20(2) of the *Terrorism Act 2006*, and the list of offences that constitute "conventions offences" in Schedule 1 of that *Act*[13]).
Australia	Australia has now passed close to 40 pieces of anti-terrorism legislation. As highlighted under the Title (a) of the research (*supra*), this country had no laws dealing specifically with terrorism prior to the events of 11 September 2001. Measures analogous to anti-terrorism legislation can, however, be traced back to the *Crimes Act 1914*. The new anti-terrorism or terrorism-related offences created by the Australian Parliament are found in Part 5.3 and 2.4[14] of the *Criminal Code Act 1995*, which contains the main terrorism legislation enacted since September 2001. The *Crimes Act 1914* and the *Criminal Code Act 1995* have undergone several changes implemented through a series of anti-terrorism laws, the key pieces of which, with respect to new offences, being the *Security Legislation Amendment (Terrorism) Act 2002*, the *Suppression of the Financing of Terrorism Act 2002*, the *Criminal Code Amendment (Suppression of Terrorist Bombings) Acts 2002*, the *Criminal Code Amendment (Anti-Hoax and Other Measures) Act 2002*, the *Criminal Code Amendment (Offences Against Australians) Act 2002*, and the *Anti-Terrorism Act (No. 2) 2004*. These Acts provide for criminal offences typically associated with terrorism, such as those related to the funding and support of, and membership in terrorist organisations, as well as the use of bombs or lethal devices in prohibited places. The Chart b.2 below provides an overview of the anti-terrorism offences introduced in Australian law in the aftermath of 11 September 2001. As stated previously, the general definition of "terrorist act" currently in use in Australia is found in subsection 100.1(1) of the *Criminal Code Act 1995* (as modified by the *Security Legislation Amendment (Terrorism) Act 2002*). This definition is incorporated by reference into the specific terrorism offences contained in other provisions of the *Criminal Code Act 1995*. As detailed previously, under Australian law, an act is considered to be a "terrorist act" if it causes serious physical harm or death to a person, endangers a person's life (other than the life of the person taking the action), cause a serious risk to the health and safety of the public or a segment of it, or seriously interferes with, disrupts or destroys an electronic system. The action and threat of action are both considered terrorist acts under the *Criminal Code Act 1995*. With respect to intent, the Australian definition requires the act to be done or the threat made with the intention of coercing or influencing by intimidation an Australian or foreign government or with the intention of intimidating the public or a segment of the

[10] See section 29 of the UK *Offences Against the Person Act 1861*: http://www.legislation.gov.uk/ukpga/Vict/24-25/100 and section 2 of the UK *Explosive Substance Act 1883*: http://www.legislation.gov.uk/ukpga/Vict/46-47/3
[11] See sections 5 and 16 of the UK *Firearms Act 1968*: http://www.legislation.gov.uk/ukpga/1968/27
[12] See sections 3 and 4 of the UK *Explosive Substances Act 1883*: http://www.legislation.gov.uk/ukpga/Vict/46-47/3
[13] For Schedule 1 (Convention Offences) of the UK *Terrorism Act 2006*, please refer to: http://www.legislation.gov.uk/ukpga/2006/11/schedule/1
[14] On the extension of criminal responsibility (attempt, conspiracy, incitment, etc.) under Part 2.4 of the Australian *Criminal Code Act 1995*, please refer to: http://www.comlaw.gov.au/Details/C2011C00261

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	public. Before an act or threat will be considered a terrorist act, it must also have been committed or made with the intention of advancing a political, religious or ideological cause. Under Australian law, an act will be considered a terrorist act no matter where in the world it occurs, and regardless of whether the damage or harm is done inside or outside Australia.
New Zealand	The NZ government had introduced the *Terrorism (Bombings and Financing) Bill* in April 2000, which aimed at criminalising terrorist acts using explosive devices and the direct or indirect financing of terrorist acts. After the events of 11 September 2001, the NZ government undertaken to review and expand this *Bill*, which was finally renamed and adopted as the *Terrorism Suppression Act 2002*. Shortly thereafter, the NZ government introduced the *Counter-Terrorism Bill* (*Bill 27-2*) in order to complement the *Terrorism Suppression Act 2002* by providing new terrorism-related offences and a range of investigative measures designed to combat terrorism. After a third reading in the NZ Parliament, the *Bill 27-2* was divided and finally passed into six (6) separate laws, one for each statute that the law would amend.[15] The new offences that have been created by the NZ Parliament are found in two Acts, namely the *Terrorism Suppression Act 2002* (as amended by the *Terrorism Suppression Amendment Act 2003 No. 106*), and the *Crimes Act 1961* (as modified by the *Crimes Amendment Act (No. 2) 2003 No. 105*). These Acts provide for new criminal offences, which are not all terrorism-specific, but have been deemed necessary to ensure that NZ criminal law can capture the whole range of offences likely to be committed by terrorists. The new offences include for instance: terrorist bombing, terrorist financing, participation in terrorist groups, causing disease and sickness in animals, contamination of food, crops, water or other products intended for human consumption, threats of harm to people or property. Terrorist acts have also become an aggravating factor for sentencing purposes pursuant to subsection 9(1)(ha) of the *Sentencing Act 2002* (as amended by the *Sentencing Amendment Act 2003 No. 109*).[16] Except for these specific terrorism-related offences, persons suspected of terrorist acts in NZ can also be prosecuted for general criminal law offences under the *Crimes Act 1961*[17], as well as for offences provided under specialised legislations, such as the *Aviation Crimes Act 1972*[18], the *Crimes (Internationally Protected Persons, United Nations and associated Personnel and Hostage) Act 1980*[19], and the *Maritime Crimes Act 1999*[20]. The chart below presents an overview of the terrorism-related offences introduced into NZ law as of the year 2002. As stated previously, the general definition of "terrorist act" currently in use in NZ is provided in section 5 of the *Terrorism Suppression Act 2002*. This definition has been incorporated by reference into other NZ statutes, such as the *Crimes Act 1961* and the *New Zealand Security Intelligence Service Act 1969* (as modified by the *New Zealand Security Intelligence Service Amendment Act 2003*).
France	France is a target of international terrorism since the 1980s. The French Parliament has responded to different "terrorist waves" by progressively enacting anti-terrorism laws, the keystone being the *Law no. 86-1020 of 9 September 1986*, which has been updated at regular intervals. Since the events of 11 September 2001, France has adopted a series of laws that have reinforced the basic legislation and procedural regulations related to terrorism. The French anti-terrorism legislations is not emergency law, but special law containing derogations of the kind already current in the law on economic and financial crimes, or the law on organized crime, of which anti-terrorism law now forms part. Like Canada's *Anti-terrorism Act* of 2001, the *Law no. 86-1020 of 9 September 1986* and other terrorism-related laws, such as the *Law no. 96-647 of 22 July 1996*, the *Law no. 2001-1062 of 15 November 2001* and the *Law no. 2006-64 of 23 January 2006*, have made a number of changes to the existing legislation, especially to the *Code pénal* (French Penal Code). Criminal law is the primary tool used against terrorism in France, but the French anti-terrorism framework also draws on civil and administrative law to prevent the commission of acts of terrorism (through, for instance, refusal of admission or asylum, refusal of naturalization, deprivation of rights, expulsion, removal, supervision of associations, etc.). As highlighted with the information provided under Title (a) of the research (*supra*), France's definition of "acts of terrorism" ("*actes de terrorisme*") is provided in the French Penal Code. The anti-terrorism offences created by anti-terrorism laws since 1986 are enumerated in sections 421-1 and sq. of that Code. Section 421-1 gives a list of ordinary offences that become "acts of terrorism" when committed with the necessary intent (i.e. acts committed "intentionally in connection with an individual or collective undertaking, the purpose of which is seriously to disturb the public order through intimidation or terror"). That activity portion of the French definition of "acts of terrorism" resembles the first part of the Canadian definition of "terrorist activity" (subparagraph 83.01(1)(a) of the *Criminal Code*), in that it links acts of terrorism to specific offences under the French Penal Code or other French codes or statutes. However, the French definition is easier to understand than the first part of the Canadian definition, because it provides examples of the types of prohibited activities contained in the offences it incorporates by references into the definition. It is to be noticed that a series of laws passed by the French Parliament since 15 November 2001 has gradually expanded the list of terrorism offences under sections 421-1 and sq. of the French Penal Code. Also punished under the current French Penal Code are for instance participation in any group formed or association established, and other preliminary acts committed, with a view to prepare an "act of terrorism". The Chart b.2 below provides an overview of indictable anti-terrorism offences under French criminal law.

[15] The six (6) new laws are: the *Terrorism Suppression Amendment Act 2003 No. 106*, the *New Zealand Security Intelligence Service Amendment Act 2003*, the *Crimes Amendment Act (No. 2) 2003 No. 105*, the *Sentencing Amendment Act 2003 No. 109*, the *Misuse of Drugs Amendment Act (No. 2) 2003 No. 107*, and the *Summary Proceedings Amendment Act 2003 No. 110*.
[16] For the NZ *Sentencing Act 2002*, please see: http://legislation.govt.nz/act/public/2002/0009/latest/whole.html?search=qs_act_entertainment_resel#dlm135342
[17] NZ *Crimes Act 1961*: http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM327382.html
[18] NZ *Aviation Crimes Act 1972*: http://www.legislation.govt.nz/act/public/1972/0137/latest/DLM409117.html
[19] NZ *Crimes (Internationally Protected Persons, United Nations and associated Personnel and Hostage) Act 1980*: http://www.legislation.govt.nz/act/public/1980/0044/latest/DLM36282.html
[20] NZ *Maritime Crimes Act 1999*: http://www.legislation.govt.nz/act/public/1999/0056/latest/whole.html#dlm28238

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

b.2 – Anti-Terrorism Offences

Country	Definitions
Canada	DEFINITION OF "TERRORIST ACTIVITY" UNDER THE *CRIMINAL CODE*: As stated above, the definition of "terrorist activity" found in subsection 83.01(1) of the *Criminal Code* is a two parts definition. In the FIRST PART of the definition (subparagraph 83.01(1)(a)), "terrorist activity" is defined to include any act or omission committed, threatened, attempted or counselled, inside or outside Canada, as defined in various subsections of section 7 of the *Criminal Code*. No specific degree of intent is provided and no specific motive is required for an act or omission to constitute a terrorist activity under subparagraph 83.01(1)(a) of the *Code*. By contrast, in the SECOND PART of the definition (subparagraph 83.01(1)(b)), "terrorist activity" is defined to include a variety of other acts or omissions committed, threatened, attempted or counselled. Under this second part of the definition, an act will not constitute terrorist activity unless it intentionally causes a specifically defined injury or damage (clause 83.01(1)(b)(ii)), and is committed with the intent of intimidating the public or a segment of it with respect to security, economic or otherwise, or to compel a person, government, domestic or international organization, wherever located, to do something or refrain from doing something (clause 83.01(1)(b)(i)(B)). With respect to the motive, an act or omission will not constitute a terrorist activity under the second part of the definition unless it has been committed, in whole or in part, for a political, religious or ideological purpose, objective or cause (clause 83.01(1)(b)(i)(A)). Subsection 83.01(1) of the ***Criminal Code***[21] reads as follows:
"*Terrorist activity*"	**Sec. 83.01(1) Definitions** (1) The following definitions apply in this Part. […] "terrorist activity" means
First part of the definition:	(a) an act or omission that is committed in or outside Canada and that, if committed in Canada, is one of the following offences: (i) the offences referred to in subsection 7(2) that implement the Convention for the Suppression of Unlawful Seizure of Aircraft, signed at The Hague on December 16, 1970, (ii) the offences referred to in subsection 7(2) that implement the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on September 23, 1971, (iii) the offences referred to in subsection 7(3) that implement the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on December 14, 1973, (iv) the offences referred to in subsection 7(3.1) that implement the International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on December 17, 1979, (v) the offences referred to in subsection 7(3.4) or (3.6) that implement the Convention on the Physical Protection of Nuclear Material, done at Vienna and New York on March 3, 1980, (vi) the offences referred to in subsection 7(2) that implement the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on February 24, 1988, (vii) the offences referred to in subsection 7(2.1) that implement the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on March 10, 1988, (viii) the offences referred to in subsection 7(2.1) or (2.2) that implement the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on March 10, 1988, (ix) the offences referred to in subsection 7(3.72) that implement the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on December 15, 1997, and (x) the offences referred to in subsection 7(3.73) that implement the International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on December 9, 1999, or
Second part of the definition:	(b) an act or omission, in or outside Canada, (i) that is committed (A) in whole or in part for a political, religious or ideological purpose, objective or cause, and (B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and (ii) that intentionally (A) causes death or serious bodily harm to a person by the use of violence, (B) endangers a person's life, (C) causes a serious risk to the health or safety of the public or any segment of the public, (D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or (E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C), and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counselling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or

[21] Canadian *Criminal Code*: http://laws-lois.justice.gc.ca/fra/lois/C-46/

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law. […]
For greater certainty:	For greater certainty (1.1) For greater certainty, the expression of a political, religious or ideological thought, belief or opinion does not come within paragraph (b) of the definition "terrorist activity" in subsection (1) unless it constitutes an act or omission that satisfies the criteria of that paragraph. Facilitation (2) For the purposes of this Part, facilitation shall be construed in accordance with subsection 83.19(2).
"*Offences committed on aircraft*"	SUBPARAGRAPH 83.01(1)(a) SPECIFICALLY REFERS TO: **Sec. 7(2) Offences committed on aircraft** […] (2) Notwithstanding this Act or any other Act, every one who (a) on an aircraft, while the aircraft is in flight, commits an act or omission outside Canada that if committed in Canada or on an aircraft registered in Canada under regulations made under the Aeronautics Act would be an offence against section 76 or paragraph 77(a), (b) in relation to an aircraft in service, commits an act or omission outside Canada that if committed in Canada would be an offence against any of paragraphs 77(b), (c) or (e), (c) in relation to an air navigation facility used in international air navigation, commits an act or omission outside Canada that if committed in Canada would be an offence against paragraph 77(d), (d) at or in relation to an airport serving international civil aviation, commits an act or omission outside Canada that if committed in Canada would be an offence against paragraph 77(b) or (f), or (e) commits an act or omission outside Canada that if committed in Canada would constitute a conspiracy or an attempt to commit an offence referred to in this subsection, or being an accessory after the fact or counselling in relation to such an offence, shall be deemed to have committed that act or omission in Canada if the person is, after the commission thereof, present in Canada. […]
"*Offences against fixed platforms or international maritime navigation*"	**Sec. 7(2.1) Offences against fixed platforms or international maritime navigation** […] (2.1) Notwithstanding anything in this Act or any other Act, every one who commits an act or omission outside Canada against or on board a fixed platform attached to the continental shelf of any state or against or on board a ship navigating or scheduled to navigate beyond the territorial sea of any state, that if committed in Canada would constitute an offence against, a conspiracy or an attempt to commit an offence against, or being an accessory after the fact or counselling in relation to an offence against, section 78.1, shall be deemed to commit that act or omission in Canada if it is committed (a) against or on board a fixed platform attached to the continental shelf of Canada; (b) against or on board a ship registered or licensed, or for which an identification number has been issued, pursuant to any Act of Parliament; (c) by a Canadian citizen; (d) by a person who is not a citizen of any state and who ordinarily resides in Canada; (e) by a person who is, after the commission of the offence, present in Canada; (f) in such a way as to seize, injure or kill, or threaten to injure or kill, a Canadian citizen; or (g) in an attempt to compel the Government of Canada to do or refrain from doing any act. […]
"*Offences against fixed platforms or navigation in the internal waters or territorial sea of another state*"	**Sec. 7(2.2) Offences against fixed platforms or navigation in the internal waters or territorial sea of another state** […] (2.2) Notwithstanding anything in this Act or any other Act, every one who commits an act or omission outside Canada against or on board a fixed platform not attached to the continental shelf of any state or against or on board a ship not navigating or scheduled to navigate beyond the territorial sea of any state, that if committed in Canada would constitute an offence against, a conspiracy or an attempt to commit an offence against, or being an accessory after the fact or counselling in relation to an offence against, section 78.1, shall be deemed to commit that act or omission in Canada (a) if it is committed as described in any of paragraphs (2.1)(b) to (g); and (b) if the offender is found in the territory of a state, other than the state in which the act or omission was committed, that is (i) a party to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on March 10, 1988, in respect of an offence committed against or on board a ship, or (ii) a party to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on March 10, 1988, in respect of an offence committed against or on board a fixed platform. […]
"*Offence against*	**Sec. 7(3) Offence against internationally protected person** […]

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

internationally protected person"	(3) Notwithstanding anything in this Act or any other Act, every one who, outside Canada, commits an act or omission against the person of an internationally protected person or against any property referred to in section 431 used by that person that, if committed in Canada, would be an offence against any of sections 235, 236, 266, 267, 268, 269, 269.1, 271, 272, 273, 279, 279.1, 280 to 283, 424 and 431 is deemed to commit that act or omission in Canada if (a) the act or omission is committed on a ship that is registered or licensed, or for which an identification number has been issued, pursuant to any Act of Parliament; (b) the act or omission is committed on an aircraft (i) registered in Canada under regulations made under the Aeronautics Act, or (ii) leased without crew and operated by a person who is qualified under regulations made under the Aeronautics Act to be registered as owner of an aircraft in Canada under those regulations; (c) the person who commits the act or omission is a Canadian citizen or is, after the act or omission has been committed, present in Canada; or (d) the act or omission is against (i) a person who enjoys the status of an internationally protected person by virtue of the functions that person performs on behalf of Canada, or (ii) a member of the family of a person described in subparagraph (i) who qualifies under paragraph (b) or (d) of the definition "internationally protected person" in section 2. […]
"*Offence of hostage taking*"	**Sec. 7(3.1) Offence of hostage taking** […] (3.1) Notwithstanding anything in this Act or any other Act, every one who, outside Canada, commits an act or omission that if committed in Canada would be an offence against section 279.1 shall be deemed to commit that act or omission in Canada if (a) the act or omission is committed on a ship that is registered or licensed, or for which an identification number has been issued, pursuant to any Act of Parliament; (b) the act or omission is committed on an aircraft (i) registered in Canada under regulations made under the Aeronautics Act, or (ii) leased without crew and operated by a person who is qualified under regulations made under the Aeronautics Act to be registered as owner of an aircraft in Canada under such regulations; (c) the person who commits the act or omission (i) is a Canadian citizen, or (ii) is not a citizen of any state and ordinarily resides in Canada; (d) the act or omission is committed with intent to induce Her Majesty in right of Canada or of a province to commit or cause to be committed any act or omission; (e) a person taken hostage by the act or omission is a Canadian citizen; or (f) the person who commits the act or omission is, after the commission thereof, present in Canada. […]
"*Offences involving nuclear material*"	**Sec. 7(3.4) Offences involving nuclear material** […] (3.4) Notwithstanding anything in this Act or any other Act, every one who, outside Canada, commits an act or omission that if committed in Canada would constitute an offence against, a conspiracy or an attempt to commit or being an accessory after the fact in relation to an offence against, or any counselling in relation to an offence against, (a) section 334, 341, 344 or 380 or paragraph 362(1)(a) in relation to nuclear material, (b) section 346 in respect of a threat to commit an offence against section 334 or 344 in relation to nuclear material, (c) section 423 in relation to a demand for nuclear material, or (d) paragraph 264.1(1)(a) or (b) in respect of a threat to use nuclear material shall be deemed to commit that act or omission in Canada if paragraph (3.5)(a), (b) or (c) applies in respect of the act or omission. […] **Sec. 7(3.6) Definition of "nuclear material"** […] (3.6) For the purposes of this section, "nuclear material" means (a) plutonium, except plutonium with an isotopic concentration of plutonium-238 exceeding eighty per cent, (b) uranium-233, (c) uranium containing uranium-233 or uranium-235 or both in such an amount that the abundance ratio of the sum of those isotopes to the isotope uranium-238 is greater than 0.72 per cent, (d) uranium with an isotopic concentration equal to that occurring in nature, and (e) any substance containing anything described in paragraphs (a) to (d), but does not include uranium in the form of ore or ore-residue. […]
"*Offence involving explosive or other device*"	**Sec. 7(3.72) Offence involving explosive or other lethal device** […] (3.72) Notwithstanding anything in this Act or any other Act, every one who, outside Canada, commits an act or omission that, if committed in Canada, would constitute an offence against, a conspiracy or an attempt to commit an offence against, or being an accessory after the fact or counselling in relation to an offence against, section 431.2 is deemed to commit that act or omission

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Offence relating to financing of terrorism*"	in Canada if (a) the act or omission is committed on a ship that is registered or licensed, or for which an identification number has been issued, under any Act of Parliament; (b) the act or omission is committed on an aircraft (i) registered in Canada under regulations made under the Aeronautics Act, (ii) leased without crew and operated by a person who is qualified under regulations made under the Aeronautics Act to be registered as owner of an aircraft in Canada under those regulations, or (iii) operated for or on behalf of the Government of Canada; (c) the person who commits the act or omission (i) is a Canadian citizen, or (ii) is not a citizen of any state and ordinarily resides in Canada; (d) the person who commits the act or omission is, after the commission of the act or omission, present in Canada; (e) the act or omission is committed against a Canadian citizen; (f) the act or omission is committed with intent to compel the Government of Canada or of a province to do or refrain from doing any act; or (g) the act or omission is committed against a Canadian government or public facility located outside Canada. […] **Sec. 7(3.73) Offence relating to financing of terrorism** […] (3.73) Notwithstanding anything in this Act or any other Act, every one who, outside Canada, commits an act or omission that, if committed in Canada, would constitute an offence against, a conspiracy or an attempt to commit an offence against, or being an accessory after the fact or counselling in relation to an offence against, section 83.02 is deemed to commit the act or omission in Canada if (a) the act or omission is committed on a ship that is registered or licensed, or for which an identification number has been issued, under an Act of Parliament; (b) the act or omission is committed on an aircraft (i) registered in Canada under regulations made under the Aeronautics Act, or (ii) leased without crew and operated by a person who is qualified under regulations made under the Aeronautics Act to be registered as the owner of an aircraft in Canada under those regulations; (c) the person who commits the act or omission (i) is a Canadian citizen, or (ii) is not a citizen of any state and ordinarily resides in Canada; (d) the person who commits the act or omission is, after its commission, present in Canada; (e) the act or omission is committed for the purpose of committing an act or omission referred to in paragraph 83.02(a) or (b) in order to compel the Government of Canada or of a province to do or refrain from doing any act; (f) the act or omission is committed for the purpose of committing an act or omission referred to in paragraph 83.02(a) or (b) against a Canadian government or public facility located outside Canada; or (g) the act or omission is committed for the purpose of committing an act or omission referred to in paragraph 83.02(a) or (b) in Canada or against a Canadian citizen. […]
"*Providing or collecting property for certain activities*" "*Providing property or services for terrorist purposes*"	IN ADDITION TO OFFENCES LISTED IN SUBPARAGRAPH 83.01(1)(a) ABOVE, THE *CRIMINAL CODE* ALSO PROVIDES FOR THE FOLLOWING OFFENCES: **Sec. 83.02 Providing or collecting property for certain activities** Every one who, directly or indirectly, wilfully and without lawful justification or excuse, provides or collects property intending that it be used or knowing that it will be used, in whole or in part, in order to carry out (a) an act or omission that constitutes an offence referred to in subparagraphs (a)(i) to (ix) of the definition of "terrorist activity" in subsection 83.01(1), or (b) any other act or omission intended to cause death or serious bodily harm to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, if the purpose of that act or omission, by its nature or context, is to intimidate the public, or to compel a government or an international organization to do or refrain from doing any act, is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years. **Sec. 83.03 Providing, making available, etc., property or services for terrorist purposes** Every one who, directly or indirectly, collects property, provides or invites a person to provide, or makes available property or financial or other related services (a) intending that they be used, or knowing that they will be used, in whole or in part, for the purpose of facilitating or carrying out any terrorist activity, or for the purpose of benefiting any person who is facilitating or carrying out such an activity, or (b) knowing that, in whole or part, they will be used by or will benefit a terrorist group, is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years. Using or possessing property for terrorist purposes 83.04 Every one who

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(a) uses property, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity, or (b) possesses property intending that it be used or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity, is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years.
"*Offences related to disclosure*"	**Sec. 83.12 Offences — freezing of property, disclosure or audit** (1) Every one who contravenes any of sections 83.08, 83.1 and 83.11 is guilty of an offence and liable (a) on summary conviction, to a fine of not more than $100,000 or to imprisonment for a term of not more than one year, or to both; or (b) on conviction on indictment, to imprisonment for a term of not more than 10 years. No contravention (2) No person contravenes section 83.1 if they make the disclosure referred to in that section only to the Commissioner of the Royal Canadian Mounted Police or the Director of the Canadian Security Intelligence Service.
"*Participation in activity of terrorist group*"	**Sec. 83.18 Participation in activity of terrorist group** (1) Every one who knowingly participates in or contributes to, directly or indirectly, any activity of a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out a terrorist activity is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years. *Prosecution* (2) An offence may be committed under subsection (1) whether or not (a) a terrorist group actually facilitates or carries out a terrorist activity; (b) the participation or contribution of the accused actually enhances the ability of a terrorist group to facilitate or carry out a terrorist activity; or (c) the accused knows the specific nature of any terrorist activity that may be facilitated or carried out by a terrorist group. *Meaning of participating or contributing* (3) Participating in or contributing to an activity of a terrorist group includes (a) providing, receiving or recruiting a person to receive training; (b) providing or offering to provide a skill or an expertise for the benefit of, at the direction of or in association with a terrorist group; (c) recruiting a person in order to facilitate or commit (i) a terrorism offence, or (ii) an act or omission outside Canada that, if committed in Canada, would be a terrorism offence; (d) entering or remaining in any country for the benefit of, at the direction of or in association with a terrorist group; and (e) making oneself, in response to instructions from any of the persons who constitute a terrorist group, available to facilitate or commit (i) a terrorism offence, or (ii) an act or omission outside Canada that, if committed in Canada, would be a terrorism offence. *Factors* (4) In determining whether an accused participates in or contributes to any activity of a terrorist group, the court may consider, among other factors, whether the accused (a) uses a name, word, symbol or other representation that identifies, or is associated with, the terrorist group; (b) frequently associates with any of the persons who constitute the terrorist group; (c) receives any benefit from the terrorist group; or (d) repeatedly engages in activities at the instruction of any of the persons who constitute the terrorist group.
"*Facilitating terrorist activity*"	**Sec. 83.19 Facilitating terrorist activity** (1) Every one who knowingly facilitates a terrorist activity is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years. Facilitation (2) For the purposes of this Part, a terrorist activity is facilitated whether or not (a) the facilitator knows that a particular terrorist activity is facilitated; (b) any particular terrorist activity was foreseen or planned at the time it was facilitated; or (c) any terrorist activity was actually carried out.
"*Commission of offence for terrorist group*"	**Sec. 83.2 Commission of offence for terrorist group** Every one who commits an indictable offence under this or any other Act of Parliament for the benefit of, at the direction of or in association with a terrorist group is guilty of an indictable offence and liable to imprisonment for life.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Instructing to carry out activity for terrorist group*"	**Sec. 83.21 Instructing to carry out activity for terrorist group** (1) Every person who knowingly instructs, directly or indirectly, any person to carry out any activity for the benefit of, at the direction of or in association with a terrorist group, for the purpose of enhancing the ability of any terrorist group to facilitate or carry out a terrorist activity, is guilty of an indictable offence and liable to imprisonment for life. Prosecution (2) An offence may be committed under subsection (1) whether or not (a) the activity that the accused instructs to be carried out is actually carried out; (b) the accused instructs a particular person to carry out the activity referred to in paragraph (a); (c) the accused knows the identity of the person whom the accused instructs to carry out the activity referred to in paragraph (a); (d) the person whom the accused instructs to carry out the activity referred to in paragraph (a) knows that it is to be carried out for the benefit of, at the direction of or in association with a terrorist group; (e) a terrorist group actually facilitates or carries out a terrorist activity; (f) the activity referred to in paragraph (a) actually enhances the ability of a terrorist group to facilitate or carry out a terrorist activity; or (g) the accused knows the specific nature of any terrorist activity that may be facilitated or carried out by a terrorist group.
"*Instructing to carry out terrorist activity*"	**Sec. 83.22 Instructing to carry out terrorist activity** (1) Every person who knowingly instructs, directly or indirectly, any person to carry out a terrorist activity is guilty of an indictable offence and liable to imprisonment for life. Prosecution (2) An offence may be committed under subsection (1) whether or not (a) the terrorist activity is actually carried out; (b) the accused instructs a particular person to carry out the terrorist activity; (c) the accused knows the identity of the person whom the accused instructs to carry out the terrorist activity; or (d) the person whom the accused instructs to carry out the terrorist activity knows that it is a terrorist activity.
"*Harbouring or concealing*"	**Sec. 83.23 Harbouring or concealing** Every one who knowingly harbours or conceals any person whom he or she knows to be a person who has carried out or is likely to carry out a terrorist activity, for the purpose of enabling the person to facilitate or carry out any terrorist activity, is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years.
"*Hoax – terrorist activity*"	**Sec. 83.231 Hoax — terrorist activity** (1) Every one commits an offence who, without lawful excuse and with intent to cause any person to fear death, bodily harm, substantial damage to property or serious interference with the lawful use or operation of property, (a) conveys or causes or procures to be conveyed information that, in all the circumstances, is likely to cause a reasonable apprehension that terrorist activity is occurring or will occur, without believing the information to be true; or (b) commits an act that, in all the circumstances, is likely to cause a reasonable apprehension that terrorist activity is occurring or will occur, without believing that such activity is occurring or will occur. *Punishment* (2) Every one who commits an offence under subsection (1) is guilty of (a) an indictable offence and liable to imprisonment for a term not exceeding five years; or (b) an offence punishable on summary conviction. Causing bodily harm (3) Every one who commits an offence under subsection (1) and thereby causes bodily harm to any other person is guilty of (a) an indictable offence and liable to imprisonment for a term not exceeding ten years; or (b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months. *Causing death* (4) Every one who commits an offence under subsection (1) and thereby causes the death of any other person is guilty of an indictable offence and liable to imprisonment for life.
United States	***United States Code*[22]:**

[22] *United States Code*: http://www.law.cornell.edu/uscode/ See also: http://uscode.house.gov/download/ascii.shtml

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Acts of terrorism*"	**Sec. 2332b Acts of terrorism transcending national boundaries** (a) Prohibited Acts.— (1) Offenses.— Whoever, involving conduct transcending national boundaries and in a circumstance described in subsection (b)— (A) kills, kidnaps, maims, commits an assault resulting in serious bodily injury, or assaults with a dangerous weapon any person within the United States; or (B) creates a substantial risk of serious bodily injury to any other person by destroying or damaging any structure, conveyance, or other real or personal property within the United States or by attempting or conspiring to destroy or damage any structure, conveyance, or other real or personal property within the United States; in violation of the laws of any State, or the United States, shall be punished as prescribed in subsection (c). (2) Treatment of threats, attempts and conspiracies.— Whoever threatens to commit an offense under paragraph (1), or attempts or conspires to do so, shall be punished under subsection (c). (b) Jurisdictional Bases.— (1) Circumstances.— The circumstances referred to in subsection (a) are— (A) the mail or any facility of interstate or foreign commerce is used in furtherance of the offense; (B) the offense obstructs, delays, or affects interstate or foreign commerce, or would have so obstructed, delayed, or affected interstate or foreign commerce if the offense had been consummated; (C) the victim, or intended victim, is the United States Government, a member of the uniformed services, or any official, officer, employee, or agent of the legislative, executive, or judicial branches, or of any department or agency, of the United States; (D) the structure, conveyance, or other real or personal property is, in whole or in part, owned, possessed, or leased to the United States, or any department or agency of the United States; (E) the offense is committed in the territorial sea (including the airspace above and the seabed and subsoil below, and artificial islands and fixed structures erected thereon) of the United States; or (F) the offense is committed within the special maritime and territorial jurisdiction of the United States. (2) Co-conspirators and accessories after the fact.— Jurisdiction shall exist over all principals and co-conspirators of an offense under this section, and accessories after the fact to any offense under this section, if at least one of the circumstances described in subparagraphs (A) through (F) of paragraph (1) is applicable to at least one offender. (c) Penalties.— […] (g) Definitions.— As used in this section— (1) the term "conduct transcending national boundaries" means conduct occurring outside of the United States in addition to the conduct occurring in the United States; (2) the term "facility of interstate or foreign commerce" has the meaning given that term in section 1958 (b)(2); (3) the term "serious bodily injury" has the meaning given that term in section 1365 (g)(3); [1] (4) the term "territorial sea of the United States" means all waters extending seaward to 12 nautical miles from the baselines of the United States, determined in accordance with international law; and (5) the term "Federal crime of terrorism" means an offense that— (A) is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and (B) is a violation of – (5) the term "Federal crime of terrorism" means an offense that – (A) is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and (B) is a violation of – (i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 175c (relating to variola virus), 229 (relating to chemical weapons), subsection (a), (b), (c), or (d) of section 351 (relating to congressional, cabinet, and Supreme Court assassination and kidnapping), 831 (relating to nuclear materials), 832 (relating to participation in nuclear and weapons of mass destruction threats to the United States), 842(m) or (n) (relating to plastic explosives), 844(f)(2) or (3) (relating to arson and bombing of Government property risking or causing death), 844(i) (relating to arson and bombing of property used in interstate commerce), 930(c) (relating to killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (relating to conspiracy to murder, kidnap, or maim persons abroad), 1030(a)(1) (relating to protection of computers),1030(a)(5)(A) resulting in damage as defined in 1030(c)(4)(A)(i)(II) through (VI) (relating to protection of computers), 1114 (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1361 (relating to government property or contracts), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751(a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1992 (relating to terrorist attacks and other acts of violence against railroad carriers and against mass transportation systems on land, on water, or through the air), 2155 (relating to destruction of national defense materials, premises, or utilities), 2156 (relating to national defense material, premises, or utilities), 2280 (relating to violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2332f (relating to bombing of public places and facilities), 2332g (relating to missile systems designed to destroy aircraft), 2332h (relating to radiological dispersal devices), 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), 2339C (relating to financing of terrorism), 2339D (relating to military-type training from a foreign terrorist organization), or 2340A (relating to torture) of this title; (ii) sections 92 (relating to prohibitions governing atomic weapons) or 236 (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2122 or 2284); (iii) section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with a dangerous weapon), section 46505(b)(3) or (c) (relating to explosive

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Destruction of aircraft or aircraft facilities*"	or incendiary devices, or endangerment of human life by means of weapons, on aircraft), section 46506 if homicide or attempted homicide is involved (relating to application of certain criminal laws to acts on aircraft), or section 60123(b) (relating to destruction of interstate gas or hazardous liquid pipeline facility) of title 49; or (iv) section 1010A of the Controlled Substances Import and Export Act (relating to narco-terrorism). SUBSECTION 2332b(5)(B)(i) SPECIFICALLY REFERS TO: **Sec. 32. Destruction of aircraft or aircraft facilities** (a) Whoever willfully— (1) sets fire to, damages, destroys, disables, or wrecks any aircraft in the special aircraft jurisdiction of the United States or any civil aircraft used, operated, or employed in interstate, overseas, or foreign air commerce; (2) places or causes to be placed a destructive device or substance in, upon, or in proximity to, or otherwise makes or causes to be made unworkable or unusable or hazardous to work or use, any such aircraft, or any part or other materials used or intended to be used in connection with the operation of such aircraft, if such placing or causing to be placed or such making or causing to be made is likely to endanger the safety of any such aircraft; (3) sets fire to, damages, destroys, or disables any air navigation facility, or interferes by force or violence with the operation of such facility, if such fire, damaging, destroying, disabling, or interfering is likely to endanger the safety of any such aircraft in flight; (4) with the intent to damage, destroy, or disable any such aircraft, sets fire to, damages, destroys, or disables or places a destructive device or substance in, upon, or in proximity to, any appliance or structure, ramp, landing area, property, machine, or apparatus, or any facility or other material used, or intended to be used, in connection with the operation, maintenance, loading, unloading or storage of any such aircraft or any cargo carried or intended to be carried on any such aircraft; (5) interferes with or disables, with intent to endanger the safety of any person or with a reckless disregard for the safety of human life, anyone engaged in the authorized operation of such aircraft or any air navigation facility aiding in the navigation of any such aircraft; (6) performs an act of violence against or incapacitates any individual on any such aircraft, if such act of violence or incapacitation is likely to endanger the safety of such aircraft; (7) communicates information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safety of any such aircraft in flight; or (8) attempts or conspires to do anything prohibited under paragraphs (1) through (7) of this subsection; shall be fined under this title or imprisoned not more than twenty years or both. (b) Whoever willfully— (1) performs an act of violence against any individual on board any civil aircraft registered in a country other than the United States while such aircraft is in flight, if such act is likely to endanger the safety of that aircraft; (2) destroys a civil aircraft registered in a country other than the United States while such aircraft is in service or causes damage to such an aircraft which renders that aircraft incapable of flight or which is likely to endanger that aircraft's safety in flight; (3) places or causes to be placed on a civil aircraft registered in a country other than the United States while such aircraft is in service, a device or substance which is likely to destroy that aircraft, or to cause damage to that aircraft which renders that aircraft incapable of flight or which is likely to endanger that aircraft's safety in flight; or (4) attempts or conspires to commit an offense described in paragraphs (1) through (3) of this subsection; shall be fined under this title or imprisoned not more than twenty years, or both. There is jurisdiction over an offense under this subsection if a national of the United States was on board, or would have been on board, the aircraft; an offender is a national of the United States; or an offender is afterwards found in the United States. For purposes of this subsection, the term "national of the United States" has the meaning prescribed in section 101(a)(22) of the Immigration and Nationality Act. (c) Whoever willfully imparts or conveys any threat to do an act which would violate any of paragraphs (1) through (6) of subsection (a) or any of paragraphs (1) through (3) of subsection (b) of this section, with an apparent determination and will to carry the threat into execution shall be fined under this title or imprisoned not more than five years, or both.
"*Violence at international airports*"	**Sec. 37. Violence at international airports** (a) Offense.— A person who unlawfully and intentionally, using any device, substance, or weapon— (1) performs an act of violence against a person at an airport serving international civil aviation that causes or is likely to cause serious bodily injury (as defined in section 1365 of this title) or death; or (2) destroys or seriously damages the facilities of an airport serving international civil aviation or a civil aircraft not in service located thereon or disrupts the services of the airport, if such an act endangers or is likely to endanger safety at that airport, or attempts or conspires to do such an act, shall be fined under this title, imprisoned not more than 20 years, or both; and if the death of any person results from conduct prohibited by this subsection, shall be punished by death or imprisoned for any term of years or for life. (b) Jurisdiction.— There is jurisdiction over the prohibited activity in subsection (a) if— (1) the prohibited activity takes place in the United States; or (2) the prohibited activity takes place outside the United States and (A) the offender is later found in the United States; or (B) an offender or a victim is a national of the United States (as defined in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22))).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(c) Bar to Prosecution.— It is a bar to Federal prosecution under subsection (a) for conduct that occurred within the United States that the conduct involved was during or in relation to a labor dispute, and such conduct is prohibited as a felony under the law of the State in which it was committed. For purposes of this section, the term "labor dispute" has the meaning set forth in section 2(c) [1] of the Norris-LaGuardia Act, as amended (29 U.S.C. 113 (c)), and the term "State" means a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.
"*Arson within special maritime and territorial jurisdiction*"	**Sec. 81. Arson within special maritime and territorial – Jurisdiction** Whoever, within the special maritime and territorial jurisdiction of the United States, willfully and maliciously sets fire to or burns any building, structure or vessel, any machinery or building materials or supplies, military or naval stores, munitions of war, or any structural aids or appliances for navigation or shipping, or attempts or conspires to do such an act, shall be imprisoned for not more than 25 years, fined the greater of the fine under this title or the cost of repairing or replacing any property that is damaged or destroyed, or both. If the building be a dwelling or if the life of any person be placed in jeopardy, he shall be fined under this title or imprisoned for any term of years or for life, or both.
"*Prohibitions related to biological weapons*"	**Sec. 175. Prohibitions with respect to biological weapons** (a) In General.— Whoever knowingly develops, produces, stockpiles, transfers, acquires, retains, or possesses any biological agent, toxin, or delivery system for use as a weapon, or knowingly assists a foreign state or any organization to do so, or attempts, threatens, or conspires to do the same, shall be fined under this title or imprisoned for life or any term of years, or both. There is extraterritorial Federal jurisdiction over an offense under this section committed by or against a national of the United States. (b) Additional Offense.— Whoever knowingly possesses any biological agent, toxin, or delivery system of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose, shall be fined under this title, imprisoned not more than 10 years, or both. In this subsection, the terms "biological agent" and "toxin" do not encompass any biological agent or toxin that is in its naturally occurring environment, if the biological agent or toxin has not been cultivated, collected, or otherwise extracted from its natural source. (c) Definition.— For purposes of this section, the term "for use as a weapon" includes the development, production, transfer, acquisition, retention, or possession of any biological agent, toxin, or delivery system for other than prophylactic, protective, bona fide research, or other peaceful purposes.
"*Prohibition of possession of biological agent pr toxin*"	**Sec. 175b. Possession by restricted persons** (a) (1) No restricted person shall ship or transport in or affecting interstate or foreign commerce, or possess in or affecting interstate or foreign commerce, any biological agent or toxin, or receive any biological agent or toxin that has been shipped or transported in interstate or foreign commerce, if the biological agent or toxin is listed as a non-overlap or overlap select biological agent or toxin in sections 73.4 and 73.5 of title 42, Code of Federal Regulations, pursuant to section 351A of the Public Health Service Act, and is not excluded under sections 73.4 and 73.5 or exempted under section 73.6 of title 42, Code of Federal Regulations. (2) Whoever knowingly violates this section shall be fined as provided in this title, imprisoned not more than 10 years, or both, but the prohibition contained in this section shall not apply with respect to any duly authorized United States governmental activity. (b) Transfer to Unregistered Person.— (1) Select agents.— Whoever transfers a select agent to a person who the transferor knows or has reasonable cause to believe is not registered as required by regulations under subsection (b) or (c) of section 351A of the Public Health Service Act shall be fined under this title, or imprisoned for not more than 5 years, or both. (2) Certain other biological agents and toxins.— Whoever transfers a biological agent or toxin listed pursuant to section 212(a)(1) of the Agricultural Bioterrorism Protection Act of 2002 to a person who the transferor knows or has reasonable cause to believe is not registered as required by regulations under subsection (b) or (c) of section 212 of such Act shall be fined under this title, or imprisoned for not more than 5 years, or both. (c) Unregistered for Possession.— (1) Select agents.— Whoever knowingly possesses a biological agent or toxin where such agent or toxin is a select agent for which such person has not obtained a registration required by regulations under section 351A(c) of the Public Health Service Act shall be fined under this title, or imprisoned for not more than 5 years, or both. (2) Certain other biological agents and toxins.— Whoever knowingly possesses a biological agent or toxin where such agent or toxin is a biological agent or toxin listed pursuant to section 212(a)(1) of the Agricultural Bioterrorism Protection Act of 2002 for which such person has not obtained a registration required by regulations under section 212(c) of such Act shall be fined under this title, or imprisoned for not more than 5 years, or both. (d) In this section: (1) The term "select agent" means a biological agent or toxin to which subsection (a) applies. Such term (including for purposes of subsection (a)) does not include any such biological agent or toxin that is in its naturally-occurring environment, if the biological agent or toxin has not been cultivated, collected, or otherwise extracted from its natural source. (2) The term "restricted person" means an individual who— (A) is under indictment for a crime punishable by imprisonment for a term exceeding 1 year; (B) has been convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year; (C) is a fugitive from justice; (D) is an unlawful user of any controlled substance (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802)); (E) is an alien illegally or unlawfully in the United States;

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(F) has been adjudicated as a mental defective or has been committed to any mental institution; (G) (i) is an alien (other than an alien lawfully admitted for permanent residence) who is a national of a country as to which the Secretary of State, pursuant to section 6(j) of the Export Administration Act of 1979 (50 App. U.S.C. 2405 (j)), section 620A of chapter 1 of part M of the Foreign Assistance Act of 1961 (22 U.S.C. 2371), or section 40 (d) of chapter 3 of the Arms Export Control Act (22 U.S.C. 2780 (d)), has made a determination (that remains in effect) that such country has repeatedly provided support for acts of international terrorism, or (ii) acts for or on behalf of, or operates subject to the direction or control of, a government or official of a country described in this subparagraph; (H) has been discharged from the Armed Services of the United States under dishonorable conditions; or (I) is a member of, acts for or on behalf of, or operates subject to the direction or control of, a terrorist organization as defined in section 212(a)(3)(B)(vi) of the Immigration and Nationality Act (8 U.S.C. 1182 (a)(3)(B)(vi)). (3) The term "alien" has the same meaning as in section 101(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(3)).
	(4) The term "lawfully admitted for permanent residence" has the same meaning as in section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(20)).
"*Variola virus*"	**Sec. 175c. Variola virus** (a) Unlawful Conduct.— (1) In general.— Except as provided in paragraph (2), it shall be unlawful for any person to knowingly produce, engineer, synthesize, acquire, transfer directly or indirectly, receive, possess, import, export, or use, or possess and threaten to use, variola virus. (2) Exception.— This subsection does not apply to conduct by, or under the authority of, the Secretary of Health and Human Services. (b) Jurisdiction.— Conduct prohibited by subsection (a) is within the jurisdiction of the United States if— (1) the offense occurs in or affects interstate or foreign commerce; (2) the offense occurs outside of the United States and is committed by a national of the United States; (3) the offense is committed against a national of the United States while the national is outside the United States; (4) the offense is committed against any property that is owned, leased, or used by the United States or by any department or agency of the United States, whether the property is within or outside the United States; or (5) an offender aids or abets any person over whom jurisdiction exists under this subsection in committing an offense under this section or conspires with any person over whom jurisdiction exists under this subsection to commit an offense under this section. (c) Criminal Penalties.— (1) In general.— Any person who violates, or attempts or conspires to violate, subsection (a) shall be fined not more than $2,000,000 and shall be sentenced to a term of imprisonment not less than 25 years or to imprisonment for life. (2) Other circumstances.— Any person who, in the course of a violation of subsection (a), uses, attempts or conspires to use, or possesses and threatens to use, any item or items described in subsection (a), shall be fined not more than $2,000,000 and imprisoned for not less than 30 years or imprisoned for life. (3) Special circumstances.— If the death of another results from a person's violation of subsection (a), the person shall be fined not more than $2,000,000 and punished by imprisonment for life. (d) Definition.— As used in this section, the term "variola virus" means a virus that can cause human smallpox or any derivative of the variola major virus that contains more than 85 percent of the gene sequence of the variola major virus or the variola minor virus.
"*Chemical weapons*"	**Sec. 229. Prohibited activities** (a) Unlawful Conduct.— Except as provided in subsection (b), it shall be unlawful for any person knowingly— (1) to develop, produce, otherwise acquire, transfer directly or indirectly, receive, stockpile, retain, own, possess, or use, or threaten to use, any chemical weapon; or (2) to assist or induce, in any way, any person to violate paragraph (1), or to attempt or conspire to violate paragraph (1). (b) Exempted Agencies and Persons.— (1) In general.— Subsection (a) does not apply to the retention, ownership, possession, transfer, or receipt of a chemical weapon by a department, agency, or other entity of the United States, or by a person described in paragraph (2), pending destruction of the weapon. (2) Exempted persons.— A person referred to in paragraph (1) is— (A) any person, including a member of the Armed Forces of the United States, who is authorized by law or by an appropriate officer of the United States to retain, own, possess, transfer, or receive the chemical weapon; or (B) in an emergency situation, any otherwise nonculpable person if the person is attempting to destroy or seize the weapon. (c) Jurisdiction.— Conduct prohibited by subsection (a) is within the jurisdiction of the United States if the prohibited conduct— (1) takes place in the United States; (2) takes place outside of the United States and is committed by a national of the United States; (3) is committed against a national of the United States while the national is outside the United States; or (4) is committed against any property that is owned, leased, or used by the United States or by any department or agency of the United States, whether the property is within or outside the United States.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Congressional, Cabinet and Supreme Court assassination, kidnapping and assault*"	**Sec. 351. Congressional, Cabinet, and Supreme Court assassination, kidnapping, and assault; penalties** (a) Whoever kills any individual who is a Member of Congress or a Member-of-Congress-elect, a member of the executive branch of the Government who is the head, or a person nominated to be head during the pendency of such nomination, of a department listed in section 101 of title 5 or the second ranking official in such department, the Director (or a person nominated to be Director during the pendency of such nomination) or Deputy Director of Central Intelligence, a major Presidential or Vice Presidential candidate (as defined in section 3056 of this title), or a Justice of the United States, as defined in section 451 of title 28, or a person nominated to be a Justice of the United States, during the pendency of such nomination, shall be punished as provided by sections 1111 and 1112 of this title. (b) Whoever kidnaps any individual designated in subsection (a) of this section shall be punished (1) by imprisonment for any term of years or for life, or (2) by death or imprisonment for any term of years or for life, if death results to such individual. (c) Whoever attempts to kill or kidnap any individual designated in subsection (a) of this section shall be punished by imprisonment for any term of years or for life. (d) If two or more persons conspire to kill or kidnap any individual designated in subsection (a) of this section and one or more of such persons do any act to effect the object of the conspiracy, each shall be punished (1) by imprisonment for any term of years or for life, or (2) by death or imprisonment for any term of years or for life, if death results to such individual. […]
"*Nuclear materials*"	**Sec. 831. Prohibited transactions involving nuclear materials** (a) Whoever, if one of the circumstances described in subsection (c) of this section occurs— (1) without lawful authority, intentionally receives, possesses, uses, transfers, alters, disposes of, or disperses any nuclear material or nuclear byproduct material and— (A) thereby knowingly causes the death of or serious bodily injury to any person or substantial damage to property or to the environment; or (B) circumstances exist, or have been represented to the defendant to exist, that are likely to cause the death or serious bodily injury to any person, or substantial damage to property or to the environment; (2) with intent to deprive another of nuclear material or nuclear byproduct material, knowingly— (A) takes and carries away nuclear material or nuclear byproduct material of another without authority; (B) makes an unauthorized use, disposition, or transfer, of nuclear material or nuclear byproduct material belonging to another; or (C) uses fraud and thereby obtains nuclear material or nuclear byproduct material belonging to another; (3) knowingly— (A) uses force; or (B) threatens or places another in fear that any person other than the actor will imminently be subject to bodily injury; and thereby takes nuclear material or nuclear byproduct material belonging to another from the person or presence of any other; (4) intentionally intimidates any person and thereby obtains nuclear material or nuclear byproduct material belonging to another; (5) with intent to compel any person, international organization, or governmental entity to do or refrain from doing any act, knowingly threatens to engage in conduct described in paragraph (2)(A) or (3) of this subsection; (6) knowingly threatens to use nuclear material or nuclear byproduct material to cause death or serious bodily injury to any person or substantial damage to property or to the environment under circumstances in which the threat may reasonably be understood as an expression of serious purposes; (7) attempts to commit an offense under paragraph (1), (2), (3), or (4) of this subsection; or (8) is a party to a conspiracy of two or more persons to commit an offense under paragraph (1), (2), (3), or (4) of this subsection, if any of the parties intentionally engages in any conduct in furtherance of such offense; shall be punished as provided in subsection (b) of this section. (b) The punishment […] (c) The circumstances referred to in subsection (a) of this section are that— (1) the offense is committed in the United States or the special maritime and territorial jurisdiction of the United States, or the special aircraft jurisdiction of the United States (as defined in section 46501 of title 49); (2) an offender or a victim is— (A) a national of the United States; or (B) a United States corporation or other legal entity; (3) after the conduct required for the offense occurs the defendant is found in the United States, even if the conduct required for the offense occurs outside the United States; (4) the conduct required for the offense occurs with respect to the carriage of a consignment of nuclear material or nuclear byproduct material by any means of transportation intended to go beyond the territory of the state where the shipment originates beginning with the departure from a facility of the shipper in that state and ending with the arrival at a facility of the receiver within the state of ultimate destination and either of such states is the United States; or (5) either—

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(A) the governmental entity under subsection (a)(5) is the United States; or (B) the threat under subsection (a)(6) is directed at the United States. […] (f) As used in this section— (1) the term "nuclear material" means material containing any— (A) plutonium; (B) uranium not in the form of ore or ore residue that contains the mixture of isotopes as occurring in nature; (C) enriched uranium, defined as uranium that contains the isotope 233 or 235 or both in such amount that the abundance ratio of the sum of those isotopes to the isotope 238 is greater than the ratio of the isotope 235 to the isotope 238 occurring in nature; or (D) uranium 233; (2) the term "nuclear byproduct material" means any material containing any radioactive isotope created through an irradiation process in the operation of a nuclear reactor or accelerator; (3) the term "international organization" means a public international organization designated as such pursuant to section 1 of the International Organizations Immunities Act (22 U.S.C. 288) or a public organization created pursuant to treaty or other agreement under international law as an instrument through or by which two or more foreign governments engage in some aspect of their conduct of international affairs; (4) the term "serious bodily injury" means bodily injury which involves— (A) a substantial risk of death; (B) extreme physical pain; (C) protracted and obvious disfigurement; or (D) protracted loss or impairment of the function of a bodily member, organ, or mental faculty; (5) the term "bodily injury" means— (A) a cut, abrasion, bruise, burn, or disfigurement; (B) physical pain; (C) illness; (D) impairment of a function of a bodily member, organ, or mental faculty; or (E) any other injury to the body, no matter how temporary; (6) the term "national of the United States" has the same meaning as in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22)); and (7) the term "United States corporation or other legal entity" means any corporation or other entity organized under the laws of the United States or any State, Commonwealth, territory, possession, or district of the United States.
"*Nuclear and weapons of mass destruction*"	**Sec. 832. Participation in nuclear and weapons of mass destruction threats to the United States** (a) Whoever, within the United States or subject to the jurisdiction of the United States, willfully participates in or knowingly provides material support or resources (as defined in section 2339A) to a nuclear weapons program or other weapons of mass destruction program of a foreign terrorist power, or attempts or conspires to do so, shall be imprisoned for not more than 20 years. (b) There is extraterritorial Federal jurisdiction over an offense under this section. (c) Whoever without lawful authority develops, possesses, or attempts or conspires to develop or possess a radiological weapon, or threatens to use or uses a radiological weapon against any person within the United States, or a national of the United States while such national is outside of the United States or against any property that is owned, leased, funded, or used by the United States, whether that property is within or outside of the United States, shall be imprisoned for any term of years or for life. (d) As used in this section— (1) "nuclear weapons program" means a program or plan for the development, acquisition, or production of any nuclear weapon or weapons; (2) "weapons of mass destruction program" means a program or plan for the development, acquisition, or production of any weapon or weapons of mass destruction (as defined in section 2332a (c)); (3) "foreign terrorist power" means a terrorist organization designated under section 219 of the Immigration and Nationality Act, or a state sponsor of terrorism designated under section 6(j) of the Export Administration Act of 1979 or section 620A of the Foreign Assistance Act of 1961; and (4) "nuclear weapon" means any weapon that contains or uses nuclear material as defined in section 831 (f)(1).
"*Plastic explosive*"	**Sec. 842. Unlawful acts** […] (m) (1) It shall be unlawful for any person to import or bring into the United States, or export from the United States, any plastic explosive that does not contain a detection agent. (2) This subsection does not apply to the importation or bringing into the United States, or the exportation from the United States, of any plastic explosive that was imported or brought into, or manufactured in the United States prior to the date of enactment of this subsection by or on behalf of any agency of the United States performing military or police functions (including any military reserve component) or by or on behalf of the National Guard of any State, not later than 15 years after the date of entry into force of the Convention on the Marking of Plastic Explosives, with

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Arson and bombing of property*"	respect to the United States. (n) (1) It shall be unlawful for any person to ship, transport, transfer, receive, or possess any plastic explosive that does not contain a detection agent. (2) This subsection does not apply to— (A) the shipment, transportation, transfer, receipt, or possession of any plastic explosive that was imported or brought into, or manufactured in the United States prior to the date of enactment of this subsection by any person during the period beginning on that date and ending 3 years after that date of enactment; or (B) the shipment, transportation, transfer, receipt, or possession of any plastic explosive that was imported or brought into, or manufactured in the United States prior to the date of enactment of this subsection by or on behalf of any agency of the United States performing a military or police function (including any military reserve component) or by or on behalf of the National Guard of any State, not later than 15 years after the date of entry into force of the Convention on the Marking of Plastic Explosives, with respect to the United States. […] **Sec. 844. Penalties** […] (f) […] (2) Whoever engages in conduct prohibited by this subsection, and as a result of such conduct, directly or proximately causes personal injury or creates a substantial risk of injury to any person, including any public safety officer performing duties, shall be imprisoned for not less than 7 years and not more than 40 years, fined under this title, or both. (3) Whoever engages in conduct prohibited by this subsection, and as a result of such conduct directly or proximately causes the death of any person, including any public safety officer performing duties, shall be subject to the death penalty, or imprisoned for not less than 20 years or for life, fined under this title, or both. […] (i) Whoever maliciously damages or destroys, or attempts to damage or destroy, by means of fire or an explosive, any building, vehicle, or other real or personal property used in interstate or foreign commerce or in any activity affecting interstate or foreign commerce shall be imprisoned for not less than 5 years and not more than 20 years, fined under this title, or both; and if personal injury results to any person, including any public safety officer performing duties as a direct or proximate result of conduct prohibited by this subsection, shall be imprisoned for not less than 7 years and not more than 40 years, fined under this title, or both; and if death results to any person, including any public safety officer performing duties as a direct or proximate result of conduct prohibited by this subsection, shall also be subject to imprisonment for any term of years, or to the death penalty or to life imprisonment. […]
"*Killing or attempted killing during an attack on a Federal facility with a dangerous weapon*"	**Sec. 930. Possession of firearms and dangerous weapons in Federal facilities** […] (c) A person who kills any person in the course of a violation of subsection (a) or (b), or in the course of an attack on a Federal facility involving the use of a firearm or other dangerous weapon, or attempts or conspires to do such an act, shall be punished as provided in sections 1111, 1112, 1113, and 1117. […]
"*Conspiracy to murder, kidnap, or maim person abroad*"	**Sec. 956. Conspiracy to kill, kidnap, maim, or injure persons or damage property in a foreign country** (a) (1) Whoever, within the jurisdiction of the United States, conspires with one or more other persons, regardless of where such other person or persons are located, to commit at any place outside the United States an act that would constitute the offense of murder, kidnapping, or maiming if committed in the special maritime and territorial jurisdiction of the United States shall, if any of the conspirators commits an act within the jurisdiction of the United States to effect any object of the conspiracy, be punished as provided in subsection (a)(2). […]
"*Protection of computers*"	**Sec. 1030. Fraud and related activity in connection with computers** (a) Whoever— (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; […] (5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; […]

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Killing or attempted killing of officers and employees of the United States*"	(c) […] (4) (A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of— (i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)— […] (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or (VI) damage affecting 10 or more protected computers during any 1-year period; […] **Sec. 1114. Protection of officers and employees of the United States** Whoever kills or attempts to kill any officer or employee of the United States or of any agency in any branch of the United States Government (including any member of the uniformed services) while such officer or employee is engaged in or on account of the performance of official duties, or any person assisting such an officer or employee in the performance of such duties or on account of that assistance, shall be punished— (1) in the case of murder, as provided under section 1111; (2) in the case of manslaughter, as provided under section 1112; or (3) in the case of attempted murder or manslaughter, as provided in section 1113.
"*Murder or manslaughter of foreign officials or internationally protected persons*"	**Sec. 1116. Murder or manslaughter of foreign officials, official guests, or internationally protected persons** (a) Whoever kills or attempts to kill a foreign official, official guest, or internationally protected person shall be punished as provided under sections 1111, 1112, and 1113 of this title. (b) For the purposes of this section: (1) "Family" includes (a) a spouse, parent, brother or sister, child, or person to whom the foreign official or internationally protected person stands in loco parentis, or (b) any other person living in his household and related to the foreign official or internationally protected person by blood or marriage. (2) "Foreign government" means the government of a foreign country, irrespective of recognition by the United States. (3) "Foreign official" means— (A) a Chief of State or the political equivalent, President, Vice President, Prime Minister, Ambassador, Foreign Minister, or other officer of Cabinet rank or above of a foreign government or the chief executive officer of an international organization, or any person who has previously served in such capacity, and any member of his family, while in the United States; and (B) any person of a foreign nationality who is duly notified to the United States as an officer or employee of a foreign government or international organization, and who is in the United States on official business, and any member of his family whose presence in the United States is in connection with the presence of such officer or employee. (4) "Internationally protected person" means— (A) a Chief of State or the political equivalent, head of government, or Foreign Minister whenever such person is in a country other than his own and any member of his family accompanying him; or (B) any other representative, officer, employee, or agent of the United States Government, a foreign government, or international organization who at the time and place concerned is entitled pursuant to international law to special protection against attack upon his person, freedom, or dignity, and any member of his family then forming part of his household. (5) "International organization" means a public international organization designated as such pursuant to section 1 of the International Organizations Immunities Act (22 U.S.C. 288) or a public organization created pursuant to treaty or other agreement under international law as an instrument through or by which two or more foreign governments engage in some aspect of their conduct of international affairs. (6) "Official guest" means a citizen or national of a foreign country present in the United States as an official guest of the Government of the United States pursuant to designation as such by the Secretary of State. (7) "National of the United States" has the meaning prescribed in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22)). (c) If the victim of an offense under subsection (a) is an internationally protected person outside the United States, the United States may exercise jurisdiction over the offense if (1) the victim is a representative, officer, employee, or agent of the United States, (2) an offender is a national of the United States, or (3) an offender is afterwards found in the United States. As used in this subsection, the United States includes all areas under the jurisdiction of the United States including any of the places within the provisions of sections 5 and 7 of this title and section 46501 (2) of title 49. (d) In the course of enforcement of this section and any other sections prohibiting a conspiracy or attempt to violate this section, the Attorney General may request assistance from any Federal, State, or local agency, including the Army, Navy, and Air Force, any statute, rule, or regulation to the contrary notwithstanding.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Hostage taking*"	**Sec. 1203. Hostage taking** (a) Except as provided in subsection (b) of this section, whoever, whether inside or outside the United States, seizes or detains and threatens to kill, to injure, or to continue to detain another person in order to compel a third person or a governmental organization to do or abstain from doing any act as an explicit or implicit condition for the release of the person detained, or attempts or conspires to do so, shall be punished by imprisonment for any term of years or for life and, if the death of any person results, shall be punished by death or life imprisonment. (b) (1) It is not an offense under this section if the conduct required for the offense occurred outside the United States unless— (A) the offender or the person seized or detained is a national of the United States; (B) the offender is found in the United States; or (C) the governmental organization sought to be compelled is the Government of the United States. (2) It is not an offense under this section if the conduct required for the offense occurred inside the United States, each alleged offender and each person seized or detained are nationals of the United States, and each alleged offender is found in the United States, unless the governmental organization sought to be compelled is the Government of the United States. (c) As used in this section, the term "national of the United States" has the meaning given such term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22)).
"*Government property*"	**Sec. 1361. Government property or contracts** Whoever willfully injures or commits any depredation against any property of the United States, or of any department or agency thereof, or any property which has been or is being manufactured or constructed for the United States, or any department or agency thereof, or attempts to commit any of the foregoing offenses, shall be punished as follows: If the damage or attempted damage to such property exceeds the sum of $1,000, by a fine under this title or imprisonment for not more than ten years, or both; if the damage or attempted damage to such property does not exceed the sum of $1,000, by a fine under this title or by imprisonment for not more than one year, or both.
"*Destruction of communication lines*"	**Sec. 1362. Communication lines, stations or systems** Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than ten years, or both. In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerted activities for the purposes of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used for the military or civil defense functions of the United States.
"*Injury to buildings or property within special jurisdiction*"	**Sec. 1363. Buildings or property within special maritime and territorial jurisdiction** Whoever, within the special maritime and territorial jurisdiction of the United States, willfully and maliciously destroys or injures any structure, conveyance, or other real or personal property, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than five years, or both, and if the building be a dwelling, or the life of any person be placed in jeopardy, shall be fined under this title or imprisoned not more than twenty years, or both.
"*Destruction of energy facility*"	**Sec. 1366. Destruction of an energy facility** (a) Whoever knowingly and willfully damages or attempts or conspires to damage the property of an energy facility in an amount that in fact exceeds or would if the attempted offense had been completed, or if the object of the conspiracy had been achieved, have exceeded $100,000, or damages or attempts or conspires to damage the property of an energy facility in any amount and causes or attempts or conspires to cause a significant interruption or impairment of a function of an energy facility, shall be punishable by a fine under this title or imprisonment for not more than 20 years, or both. […]
"*Presidential staff assassination and kidnapping*"	**Sec. 1751. Presidential and Presidential staff assassination, kidnapping, and assault; penalties** (a) Whoever kills (1) any individual who is the President of the United States, the President-elect, the Vice President, or, if there is no Vice President, the officer next in the order of succession to the Office of the President of the United States, the Vice President-elect, or any person who is acting as President under the Constitution and laws of the United States, or (2) any person appointed under section 105 (a)(2)(A) of title 3 employed in the Executive Office of the President or appointed under section 106 (a)(1)(A) of title 3 employed in the Office of the Vice President, shall be punished as provided by sections 1111 and 1112 of this title. (b) Whoever kidnaps any individual designated in subsection (a) of this section shall be punished (1) by imprisonment for any term of years or for life, or (2) by death or imprisonment for any term of years or for life, if death results to such individual. (c) Whoever attempts to kill or kidnap any individual designated in subsection (a) of this section shall be punished by imprisonment for any term of years or for life. (d) If two or more persons conspire to kill or kidnap any individual designated in subsection (a) of this section and one or more of such persons do any act to effect the object of the conspiracy, each shall be punished

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Terrorist attacks against mass transportation systems*"	(1) by imprisonment for any term of years or for life, or (2) by death or imprisonment for any term of years or for life, if death results to such individual. […] **Sec. 1992. Terrorist attacks and other violence against railroad carriers and against mass transportation systems on land, on water, or through the air** (a) General Prohibitions.— Whoever, in a circumstance described in subsection (c), knowingly and without lawful authority or permission— (1) wrecks, derails, sets fire to, or disables railroad on-track equipment or a mass transportation vehicle; (2) places any biological agent or toxin, destructive substance, or destructive device in, upon, or near railroad on-track equipment or a mass transportation vehicle with intent to endanger the safety of any person, or with a reckless disregard for the safety of human life; (3) places or releases a hazardous material or a biological agent or toxin on or near any property described in subparagraph (A) or (B) of paragraph (4), with intent to endanger the safety of any person, or with reckless disregard for the safety of human life; (4) sets fire to, undermines, makes unworkable, unusable, or hazardous to work on or use, or places any biological agent or toxin, destructive substance, or destructive device in, upon, or near any— (A) tunnel, bridge, viaduct, trestle, track, electromagnetic guideway, signal, station, depot, warehouse, terminal, or any other way, structure, property, or appurtenance used in the operation of, or in support of the operation of, a railroad carrier, and with intent to, or knowing or having reason to know,[1] such activity would likely, derail, disable, or wreck railroad on-track equipment; or (B) garage, terminal, structure, track, electromagnetic guideway, supply, or facility used in the operation of, or in support of the operation of, a mass transportation vehicle, and with intent to, or knowing or having reason to know,[1] such activity would likely, derail, disable, or wreck a mass transportation vehicle used, operated, or employed by a mass transportation provider; (5) removes an appurtenance from, damages, or otherwise impairs the operation of a railroad signal system or mass transportation signal or dispatching system, including a train control system, centralized dispatching system, or highway-railroad grade crossing warning signal; (6) with intent to endanger the safety of any person, or with a reckless disregard for the safety of human life, interferes with, disables, or incapacitates any dispatcher, driver, captain, locomotive engineer, railroad conductor, or other person while the person is employed in dispatching, operating, controlling, or maintaining railroad on-track equipment or a mass transportation vehicle; (7) commits an act, including the use of a dangerous weapon, with the intent to cause death or serious bodily injury to any person who is on property described in subparagraph (A) or (B) of paragraph (4); (8) surveils, photographs, videotapes, diagrams, or otherwise collects information with the intent to plan or assist in planning any of the acts described in paragraphs (1) through (6); (9) conveys false information, knowing the information to be false, concerning an attempt or alleged attempt to engage in a violation of this subsection; or (10) attempts, threatens, or conspires to engage in any violation of any of paragraphs (1) through (9), shall be fined under this title or imprisoned not more than 20 years, or both, and if the offense results in the death of any person, shall be imprisoned for any term of years or for life, or subject to death, except in the case of a violation of paragraph (8), (9), or (10). (b) Aggravated Offense.— Whoever commits an offense under subsection (a) of this section in a circumstance in which— (1) the railroad on-track equipment or mass transportation vehicle was carrying a passenger or employee at the time of the offense; (2) the railroad on-track equipment or mass transportation vehicle was carrying high-level radioactive waste or spent nuclear fuel at the time of the offense; or (3) the offense was committed with the intent to endanger the safety of any person, or with a reckless disregard for the safety of any person, and the railroad on-track equipment or mass transportation vehicle was carrying a hazardous material at the time of the offense that— (A) was required to be placarded under subpart F of part 172 of title 49, Code of Federal Regulations; and (B) is identified as class number 3, 4, 5, 6.1, or 8 and packing group I or packing group II, or class number 1, 2, or 7 under the hazardous materials table of section 172.101 of title 49, Code of Federal Regulations, shall be fined under this title or imprisoned for any term of years or life, or both, and if the offense resulted in the death of any person, the person may be sentenced to death. (c) Circumstances Required for Offense.— A circumstance referred to in subsection (a) is any of the following: (1) Any of the conduct required for the offense is, or, in the case of an attempt, threat, or conspiracy to engage in conduct, the conduct required for the completed offense would be, engaged in, on, against, or affecting a mass transportation provider, or a railroad carrier engaged in interstate or foreign commerce. (2) Any person travels or communicates across a State line in order to commit the offense, or transports materials across a State line in aid of the commission of the offense. (d) Definitions.— In this section— (1) the term "biological agent" has the meaning given to that term in section 178 (1); (2) the term "dangerous weapon" means a weapon, device, instrument, material, or substance, animate or inanimate, that is used for, or is readily capable of, causing death or serious bodily injury, including a pocket knife with a blade of less than 21/2 inches in length and a box cutter; (3) the term "destructive device" has the meaning given to that term in section 921 (a)(4); (4) the term "destructive substance" means an explosive substance, flammable material, infernal machine, or other chemical, mechanical, or radioactive device or material, or matter of a combustible, contaminative, corrosive, or explosive nature, except that the term "radioactive device" does not include any radioactive device or material used solely for medical, industrial, research, or other peaceful purposes; (5) the term "hazardous material" has the meaning given to that term in chapter 51 of title 49; (6) the term "high-level radioactive waste" has the meaning given to that term in section 2(12) of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101 (12)); (7) the term "mass transportation" has the meaning given to that term in section 5302 (a)(7) of title 49, except that the term includes intercity bus transportation [2] school bus, charter, and

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	sightseeing transportation and passenger vessel as that term is defined in section 2101 (22) of title 46, United States Code; (8) the term "on-track equipment" means a carriage or other contrivance that runs on rails or electromagnetic guideways; (9) the term "railroad on-track equipment" means a train, locomotive, tender, motor unit, freight or passenger car, or other on-track equipment used, operated, or employed by a railroad carrier; (10) the term "railroad" has the meaning given to that term in chapter 201 of title 49; (11) the term "railroad carrier" has the meaning given to that term in chapter 201 of title 49; (12) the term "serious bodily injury" has the meaning given to that term in section 1365; (13) the term "spent nuclear fuel" has the meaning given to that term in section 2(23) of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101 (23)); (14) the term "State" has the meaning given to that term in section 2266; (15) the term "toxin" has the meaning given to that term in section 178 (2); and (16) the term "vehicle" means any carriage or other contrivance used, or capable of being used, as a means of transportation on land, on water, or through the air.
"*Destruction of national defense property*"	**Sec. 2155. Destruction of national-defense materials, national-defense premises, or national-defense utilities** (a) Whoever, with intent to injure, interfere with, or obstruct the national defense of the United States, willfully injures, destroys, contaminates or infects, or attempts to so injure, destroy, contaminate or infect any national-defense material, national-defense premises, or national-defense utilities, shall be fined under this title or imprisoned not more than 20 years, or both, and, if death results to any person, shall be imprisoned for any term of years or for life. (b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section. **Sec. 2156. Production of defective national-defense material, national-defense premises, or national-defense utilities** (a) Whoever, with intent to injure, interfere with, or obstruct the national defense of the United States, willfully makes, constructs, or attempts to make or construct in a defective manner, any national-defense material, national-defense premises or national-defense utilities, or any tool, implement, machine, utensil, or receptacle used or employed in making, producing, manufacturing, or repairing any such national-defense material, national-defense premises or national-defense utilities, shall be fined under this title or imprisoned not more than ten years, or both. (b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.
"*Violence against maritime navigation*"	**Sec. 2280. Violence against maritime navigation** (a) Offenses.— (1) In general.— A person who unlawfully and intentionally— (A) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation; (B) performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship; (C) destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship; (D) places or causes to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship; (E) destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if such act is likely to endanger the safe navigation of a ship; (F) communicates information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safe navigation of a ship; (G) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (F); or (H) attempts or conspires to do any act prohibited under subparagraphs (A) through (G), shall be fined under this title, imprisoned not more than 20 years, or both; and if the death of any person results from conduct prohibited by this paragraph, shall be punished by death or imprisoned for any term of years or for life. (2) Threat to navigation.— A person who threatens to do any act prohibited under paragraph (1)(B), (C) or (E), with apparent determination and will to carry the threat into execution, if the threatened act is likely to endanger the safe navigation of the ship in question, shall be fined under this title, imprisoned not more than 5 years, or both. (b) Jurisdiction.— There is jurisdiction over the activity prohibited in subsection (a)— (1) in the case of a covered ship, if— (A) such activity is committed— (i) against or on board a ship flying the flag of the United States at the time the prohibited activity is committed; (ii) in the United States; or (iii) by a national of the United States or by a stateless person whose habitual residence is in the United States; (B) during the commission of such activity, a national of the United States is seized, threatened, injured or killed; or (C) the offender is later found in the United States after such activity is committed; (2) in the case of a ship navigating or scheduled to navigate solely within the territorial sea or internal waters of a country other than the United States, if the offender is later found in the United

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Violence against maritime fixed platforms*"	States after such activity is committed; and (3) in the case of any vessel, if such activity is committed in an attempt to compel the United States to do or abstain from doing any act. (c) Bar To Prosecution.— It is a bar to Federal prosecution under subsection (a) for conduct that occurred within the United States that the conduct involved was during or in relation to a labor dispute, and such conduct is prohibited as a felony under the law of the State in which it was committed. For purposes of this section, the term "labor dispute" has the meaning set forth in section 2(c) [1] of the Norris-LaGuardia Act, as amended (29 U.S.C. 113 (c)). (d) Delivery of Suspected Offender.— The master of a covered ship flying the flag of the United States who has reasonable grounds to believe that there is on board that ship any person who has committed an offense under Article 3 of the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation may deliver such person to the authorities of a State Party to that Convention. Before delivering such person to the authorities of another country, the master shall notify in an appropriate manner the Attorney General of the United States of the alleged offense and await instructions from the Attorney General as to what action to take. When delivering the person to a country which is a State Party to the Convention, the master shall, whenever practicable, and if possible before entering the territorial sea of such country, notify the authorities of such country of the master's intention to deliver such person and the reasons therefor. If the master delivers such person, the master shall furnish to the authorities of such country the evidence in the master's possession that pertains to the alleged offense. (e) Definitions.— In this section— "covered ship" means a ship that is navigating or is scheduled to navigate into, through or from waters beyond the outer limit of the territorial sea of a single country or a lateral limit of that country's territorial sea with an adjacent country. "national of the United States" has the meaning stated in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22)). "territorial sea of the United States" means all waters extending seaward to 12 nautical miles from the baselines of the United States determined in accordance with international law. "ship" means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles or any other floating craft, but does not include a warship, a ship owned or operated by a government when being used as a naval auxiliary or for customs or police purposes, or a ship which has been withdrawn from navigation or laid up. "United States", when used in a geographical sense, includes the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands and all territories and possessions of the United States. **Sec.2281. Violence against maritime fixed platforms** (a) Offenses.— (1) In general.— A person who unlawfully and intentionally— (A) seizes or exercises control over a fixed platform by force or threat thereof or any other form of intimidation; (B) performs an act of violence against a person on board a fixed platform if that act is likely to endanger its safety; (C) destroys a fixed platform or causes damage to it which is likely to endanger its safety; (D) places or causes to be placed on a fixed platform, by any means whatsoever, a device or substance which is likely to destroy that fixed platform or likely to endanger its safety; (E) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (D); or (F) attempts or conspires to do anything prohibited under subparagraphs (A) through (E), shall be fined under this title, imprisoned not more than 20 years, or both; and if death results to any person from conduct prohibited by this paragraph, shall be punished by death or imprisoned for any term of years or for life. (2) Threat to safety.— A person who threatens to do anything prohibited under paragraph (1)(B) or (C), with apparent determination and will to carry the threat into execution, if the threatened act is likely to endanger the safety of the fixed platform, shall be fined under this title, imprisoned not more than 5 years, or both. (b) Jurisdiction.— There is jurisdiction over the activity prohibited in subsection (a) if— (1) such activity is committed against or on board a fixed platform— (A) that is located on the continental shelf of the United States; (B) that is located on the continental shelf of another country, by a national of the United States or by a stateless person whose habitual residence is in the United States; or (C) in an attempt to compel the United States to do or abstain from doing any act; (2) during the commission of such activity against or on board a fixed platform located on a continental shelf, a national of the United States is seized, threatened, injured or killed; or (3) such activity is committed against or on board a fixed platform located outside the United States and beyond the continental shelf of the United States and the offender is later found in the United States. (c) Bar To Prosecution.— It is a bar to Federal prosecution under subsection (a) for conduct that occurred within the United States that the conduct involved was during or in relation to a labor dispute, and such conduct is prohibited as a felony under the law of the State in which it was committed. For purposes of this section, the term "labor dispute" has the meaning set forth in section 2(c) [1] of the Norris-LaGuardia Act, as amended (29 U.S.C. 113 (c)), and the term "State" means a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States. (d) Definitions.— In this section— "continental shelf" means the sea-bed and subsoil of the submarine areas that extend beyond a country's territorial sea to the limits provided by customary international law as reflected in Article 76 of the 1982 Convention on the Law of the Sea. "fixed platform" means an artificial island, installation or structure permanently attached to the sea-bed for the purpose of exploration or exploitation of resources or for other economic purposes. "national of the United States" has the meaning stated in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22)).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	"territorial sea of the United States" means all waters extending seaward to 12 nautical miles from the baselines of the United States determined in accordance with international law. "United States", when used in a geographical sense, includes the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands and all territories and possessions of the United States.
"*Certain homicides occurring outside the United States*"	**Sec. 2332. Criminal penalties** (a) Homicide.— Whoever kills a national of the United States, while such national is outside the United States, shall— (1) if the killing is murder (as defined in section 1111 (a)), be fined under this title, punished by death or imprisonment for any term of years or for life, or both; (2) if the killing is a voluntary manslaughter as defined in section 1112 (a) of this title, be fined under this title or imprisoned not more than ten years, or both; and (3) if the killing is an involuntary manslaughter as defined in section 1112 (a) of this title, be fined under this title or imprisoned not more than three years, or both. (b) Attempt or Conspiracy With Respect to Homicide.— Whoever outside the United States attempts to kill, or engages in a conspiracy to kill, a national of the United States shall— (1) in the case of an attempt to commit a killing that is a murder as defined in this chapter, be fined under this title or imprisoned not more than 20 years, or both; and (2) in the case of a conspiracy by two or more persons to commit a killing that is a murder as defined in section 1111 (a) of this title, if one or more of such persons do any overt act to effect the object of the conspiracy, be fined under this title or imprisoned for any term of years or for life, or both so fined and so imprisoned. (c) Other Conduct.— Whoever outside the United States engages in physical violence— (1) with intent to cause serious bodily injury to a national of the United States; or (2) with the result that serious bodily injury is caused to a national of the United States; shall be fined under this title or imprisoned not more than ten years, or both. (d) Limitation on Prosecution.— No prosecution for any offense described in this section shall be undertaken by the United States except on written certification of the Attorney General or the highest ranking subordinate of the Attorney General with responsibility for criminal prosecutions that, in the judgment of the certifying official, such offense was intended to coerce, intimidate, or retaliate against a government or a civilian population.
"*Use of weapons of mass destruction*"	**Sec. 2332a. Use of weapons of mass destruction** (a) Offense Against a National of the United States or Within the United States.— A person who, without lawful authority, uses, threatens, or attempts or conspires to use, a weapon of mass destruction— (1) against a national of the United States while such national is outside of the United States; (2) against any person or property within the United States, and (A) the mail or any facility of interstate or foreign commerce is used in furtherance of the offense; (B) such property is used in interstate or foreign commerce or in an activity that affects interstate or foreign commerce; (C) any perpetrator travels in or causes another to travel in interstate or foreign commerce in furtherance of the offense; or (D) the offense, or the results of the offense, affect interstate or foreign commerce, or, in the case of a threat, attempt, or conspiracy, would have affected interstate or foreign commerce; (3) against any property that is owned, leased or used by the United States or by any department or agency of the United States, whether the property is within or outside of the United States; or (4) against any property within the United States that is owned, leased, or used by a foreign government, shall be imprisoned for any term of years or for life, and if death results, shall be punished by death or imprisoned for any term of years or for life. (b) Offense by National of the United States Outside of the United States.— Any national of the United States who, without lawful authority, uses, or threatens, attempts, or conspires to use, a weapon of mass destruction outside of the United States shall be imprisoned for any term of years or for life, and if death results, shall be punished by death, or by imprisonment for any term of years or for life. (c) Definitions.— For purposes of this section— (1) the term "national of the United States" has the meaning given in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22)); (2) the term "weapon of mass destruction" means— (A) any destructive device as defined in section 921 of this title; (B) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; (C) any weapon involving a biological agent, toxin, or vector (as those terms are defined in section 178 of this title); or (D) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life; and (3) the term "property" includes all real and personal property.
"*Bombing of public places and facilities*"	**Sec. 2332f. Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities** (a) Offenses.— (1) In general.— Whoever unlawfully delivers, places, discharges, or detonates an explosive or other lethal device in, into, or against a place of public use, a state or government facility, a public transportation system, or an infrastructure facility— (A) with the intent to cause death or serious bodily injury, or (B) with the intent to cause extensive destruction of such a place, facility, or system, where such destruction results in or is likely to result in major economic loss,

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	shall be punished as prescribed in subsection (c). (2) Attempts and conspiracies.— Whoever attempts or conspires to commit an offense under paragraph (1) shall be punished as prescribed in subsection (c). (b) Jurisdiction.— There is jurisdiction over the offenses in subsection (a) if— (1) the offense takes place in the United States and— (A) the offense is committed against another state or a government facility of such state, including its embassy or other diplomatic or consular premises of that state; (B) the offense is committed in an attempt to compel another state or the United States to do or abstain from doing any act; (C) at the time the offense is committed, it is committed— (i) on board a vessel flying the flag of another state; (ii) on board an aircraft which is registered under the laws of another state; or (iii) on board an aircraft which is operated by the government of another state; (D) a perpetrator is found outside the United States; (E) a perpetrator is a national of another state or a stateless person; or (F) a victim is a national of another state or a stateless person; (2) the offense takes place outside the United States and— (A) a perpetrator is a national of the United States or is a stateless person whose habitual residence is in the United States; (B) a victim is a national of the United States; (C) a perpetrator is found in the United States; (D) the offense is committed in an attempt to compel the United States to do or abstain from doing any act; (E) the offense is committed against a state or government facility of the United States, including an embassy or other diplomatic or consular premises of the United States; (F) the offense is committed on board a vessel flying the flag of the United States or an aircraft which is registered under the laws of the United States at the time the offense is committed; or (G) the offense is committed on board an aircraft which is operated by the United States. (c) Penalties.— Whoever violates this section shall be punished as provided under section 2332a (a) of this title. (d) Exemptions to Jurisdiction.— This section does not apply to— (1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law, (2) activities undertaken by military forces of a state in the exercise of their official duties; or (3) offenses committed within the United States, where the alleged offender and the victims are United States citizens and the alleged offender is found in the United States, or where jurisdiction is predicated solely on the nationality of the victims or the alleged offender and the offense has no substantial effect on interstate or foreign commerce. (e) Definitions.— As used in this section, the term— (1) "serious bodily injury" has the meaning given that term in section 1365 (g)(3) of this title; [1] (2) "national of the United States" has the meaning given that term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22)); (3) "state or government facility" includes any permanent or temporary facility or conveyance that is used or occupied by representatives of a state, members of Government, the legislature or the judiciary or by officials or employees of a state or any other public authority or entity or by employees or officials of an intergovernmental organization in connection with their official duties; (4) "intergovernmental organization" includes international organization (as defined in section 1116 (b)(5) of this title); (5) "infrastructure facility" means any publicly or privately owned facility providing or distributing services for the benefit of the public, such as water, sewage, energy, fuel, or communications; (6) "place of public use" means those parts of any building, land, street, waterway, or other location that are accessible or open to members of the public, whether continuously, periodically, or occasionally, and encompasses any commercial, business, cultural, historical, educational, religious, governmental, entertainment, recreational, or similar place that is so accessible or open to the public; (7) "public transportation system" means all facilities, conveyances, and instrumentalities, whether publicly or privately owned, that are used in or for publicly available services for the transportation of persons or cargo; (8) "explosive" has the meaning given in section 844 (j) of this title insofar that it is designed, or has the capability, to cause death, serious bodily injury, or substantial material damage; (9) "other lethal device" means any weapon or device that is designed or has the capability to cause death, serious bodily injury, or substantial damage to property through the release, dissemination, or impact of toxic chemicals, biological agents, or toxins (as those terms are defined in section 178 of this title) or radiation or radioactive material; (10) "military forces of a state" means the armed forces of a state which are organized, trained, and equipped under its internal law for the primary purpose of national defense or security, and persons acting in support of those armed forces who are under their formal command, control, and responsibility; (11) "armed conflict" does not include internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature; and (12) "state" has the same meaning as that term has under international law, and includes all political subdivisions thereof.
"*Missile systems designed to destroy aircraft*"	**Sec. 2332g. Missile systems designed to destroy aircraft** (a) Unlawful Conduct.— (1) In general.— Except as provided in paragraph (3), it shall be unlawful for any person to knowingly produce, construct, otherwise acquire, transfer directly or indirectly, receive, possess, import, export, or use, or possess and threaten to use—

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(A) an explosive or incendiary rocket or missile that is guided by any system designed to enable the rocket or missile to— (i) seek or proceed toward energy radiated or reflected from an aircraft or toward an image locating an aircraft; or (ii) otherwise direct or guide the rocket or missile to an aircraft; (B) any device designed or intended to launch or guide a rocket or missile described in subparagraph (A); or (C) any part or combination of parts designed or redesigned for use in assembling or fabricating a rocket, missile, or device described in subparagraph (A) or (B). (2) Nonweapon.— Paragraph (1)(A) does not apply to any device that is neither designed nor redesigned for use as a weapon. (3) Excluded conduct.— This subsection does not apply with respect to— (A) conduct by or under the authority of the United States or any department or agency thereof or of a State or any department or agency thereof; or (B) conduct pursuant to the terms of a contract with the United States or any department or agency thereof or with a State or any department or agency thereof. (b) Jurisdiction.— Conduct prohibited by subsection (a) is within the jurisdiction of the United States if— (1) the offense occurs in or affects interstate or foreign commerce; (2) the offense occurs outside of the United States and is committed by a national of the United States; (3) the offense is committed against a national of the United States while the national is outside the United States; (4) the offense is committed against any property that is owned, leased, or used by the United States or by any department or agency of the United States, whether the property is within or outside the United States; or (5) an offender aids or abets any person over whom jurisdiction exists under this subsection in committing an offense under this section or conspires with any person over whom jurisdiction exists under this subsection to commit an offense under this section. (c) Criminal Penalties.— (1) In general.— Any person who violates, or attempts or conspires to violate, subsection (a) shall be fined not more than $2,000,000 and shall be sentenced to a term of imprisonment not less than 25 years or to imprisonment for life. (2) Other circumstances.— Any person who, in the course of a violation of subsection (a), uses, attempts or conspires to use, or possesses and threatens to use, any item or items described in subsection (a), shall be fined not more than $2,000,000 and imprisoned for not less than 30 years or imprisoned for life. (3) Special circumstances.— If the death of another results from a person's violation of subsection (a), the person shall be fined not more than $2,000,000 and punished by imprisonment for life. (d) Definition.— As used in this section, the term "aircraft" has the definition set forth in section 40102 (a)(6) of title 49, United States Code.
"*Radiological dispersal devices*"	**Sec. 2332h. Radiological dispersal devices** (a) Unlawful Conduct.— (1) In general.— Except as provided in paragraph (2), it shall be unlawful for any person to knowingly produce, construct, otherwise acquire, transfer directly or indirectly, receive, possess, import, export, or use, or possess and threaten to use— (A) any weapon that is designed or intended to release radiation or radioactivity at a level dangerous to human life; or (B) any device or other object that is capable of and designed or intended to endanger human life through the release of radiation or radioactivity. (2) Exception.— This subsection does not apply with respect to— (A) conduct by or under the authority of the United States or any department or agency thereof; or (B) conduct pursuant to the terms of a contract with the United States or any department or agency thereof. (b) Jurisdiction.— Conduct prohibited by subsection (a) is within the jurisdiction of the United States if— (1) the offense occurs in or affects interstate or foreign commerce; (2) the offense occurs outside of the United States and is committed by a national of the United States; (3) the offense is committed against a national of the United States while the national is outside the United States; (4) the offense is committed against any property that is owned, leased, or used by the United States or by any department or agency of the United States, whether the property is within or outside the United States; or (5) an offender aids or abets any person over whom jurisdiction exists under this subsection in committing an offense under this section or conspires with any person over whom jurisdiction exists under this subsection to commit an offense under this section. (c) Criminal Penalties.— (1) In general.— Any person who violates, or attempts or conspires to violate, subsection (a) shall be fined not more than $2,000,000 and shall be sentenced to a term of imprisonment not less than 25 years or to imprisonment for life. (2) Other circumstances.— Any person who, in the course of a violation of subsection (a), uses, attempts or conspires to use, or possesses and threatens to use, any item or items described in subsection (a), shall be fined not more than $2,000,000 and imprisoned for not less than 30 years or imprisoned for life. (3) Special circumstances.— If the death of another results from a person's violation of subsection (a), the person shall be fined not more than $2,000,000 and punished by imprisonment for life.
"*Harboring terrorists*"	**Sec. 2339. Harboring or concealing terrorists** (a) Whoever harbors or conceals any person who he knows, or has reasonable grounds to believe, has committed, or is about to commit, an offense under section 32 (relating to destruction of

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	aircraft or aircraft facilities), section 175 (relating to biological weapons), section 229 (relating to chemical weapons), section 831 (relating to nuclear materials), paragraph (2) or (3) of section 844 (f) (relating to arson and bombing of government property risking or causing injury or death), section 1366 (a) (relating to the destruction of an energy facility), section 2280 (relating to violence against maritime navigation), section 2332a (relating to weapons of mass destruction), or section 2332b (relating to acts of terrorism transcending national boundaries) of this title, section 236 (a) (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2284 (a)), or section 46502 (relating to aircraft piracy) of title 49, shall be fined under this title or imprisoned not more than ten years, or both. (b) […]
"*Material support to terrorist*"	**Sec. 2339A. Providing material support to terrorists** (a) Offense.— Whoever provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of section 32, 37, 81, 175, 229, 351, 831, 842 (m) or (n), 844 (f) or (i), 930 (c), 956, 1091, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, 2340A, or 2442 of this title, section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284), section 46502 or 60123 (b) of title 49, or any offense listed in section 2332b (g)(5)(B) (except for sections 2339A and 2339B) or in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act, shall be fined under this title, imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. A violation of this section may be prosecuted in any Federal judicial district in which the underlying offense was committed, or in any other Federal judicial district as provided by law. (b) Definitions.— As used in this section— (1) the term "material support or resources" means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials; (2) the term "training" means instruction or teaching designed to impart a specific skill, as opposed to general knowledge; and (3) the term "expert advice or assistance" means advice or assistance derived from scientific, technical or other specialized knowledge.
"*Material support to terrorist organizations*"	**Sec. 2339B. Providing material support or resources to designated foreign terrorist organizations** (a) Prohibited Activities.— (1) Unlawful conduct.— Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6)), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989). (2) Financial institutions […] (b) Civil Penalty […] (c) Injunction […] (d) Extraterritorial Jurisdiction.— (1) In general.— There is jurisdiction over an offense under subsection (a) if— (A) an offender is a national of the United States (as defined in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22))) or an alien lawfully admitted for permanent residence in the United States (as defined in section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(20))); (B) an offender is a stateless person whose habitual residence is in the United States; (C) after the conduct required for the offense occurs an offender is brought into or found in the United States, even if the conduct required for the offense occurs outside the United States; (D) the offense occurs in whole or in part within the United States; (E) the offense occurs in or affects interstate or foreign commerce; or (F) an offender aids or abets any person over whom jurisdiction exists under this paragraph in committing an offense under subsection (a) or conspires with any person over whom jurisdiction exists under this paragraph to commit an offense under subsection (a). (2) Extraterritorial jurisdiction.— There is extraterritorial Federal jurisdiction over an offense under this section. […]
"*Financing of terrorism*"	**Sec. 2339C. Prohibitions against the financing of terrorism** (a) Offenses.— (1) In general.— Whoever, in a circumstance described in subsection (b), by any means, directly or indirectly, unlawfully and willfully provides or collects funds with the intention that such funds be used, or with the knowledge that such funds are to be used, in full or in part, in order to carry out— (A) an act which constitutes an offense within the scope of a treaty specified in subsection (e)(7), as implemented by the United States, or (B) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act,

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	shall be punished as prescribed in subsection (d)(1). (2) Attempts and conspiracies.— Whoever attempts or conspires to commit an offense under paragraph (1) shall be punished as prescribed in subsection (d)(1). (3) Relationship to predicate act.— For an act to constitute an offense set forth in this subsection, it shall not be necessary that the funds were actually used to carry out a predicate act. (b) Jurisdiction.— There is jurisdiction over the offenses in subsection (a) in the following circumstances— (1) the offense takes place in the United States and— (A) a perpetrator was a national of another state or a stateless person; (B) on board a vessel flying the flag of another state or an aircraft which is registered under the laws of another state at the time the offense is committed; (C) on board an aircraft which is operated by the government of another state; (D) a perpetrator is found outside the United States; (E) was directed toward or resulted in the carrying out of a predicate act against— (i) a national of another state; or (ii) another state or a government facility of such state, including its embassy or other diplomatic or consular premises of that state; (F) was directed toward or resulted in the carrying out of a predicate act committed in an attempt to compel another state or international organization to do or abstain from doing any act; or (G) was directed toward or resulted in the carrying out of a predicate act— (i) outside the United States; or (ii) within the United States, and either the offense or the predicate act was conducted in, or the results thereof affected, interstate or foreign commerce; (2) the offense takes place outside the United States and— (A) a perpetrator is a national of the United States or is a stateless person whose habitual residence is in the United States; (B) a perpetrator is found in the United States; or (C) was directed toward or resulted in the carrying out of a predicate act against— (i) any property that is owned, leased, or used by the United States or by any department or agency of the United States, including an embassy or other diplomatic or consular premises of the United States; (ii) any person or property within the United States; (iii) any national of the United States or the property of such national; or (iv) any property of any legal entity organized under the laws of the United States, including any of its States, districts, commonwealths, territories, or possessions; (3) the offense is committed on board a vessel flying the flag of the United States or an aircraft which is registered under the laws of the United States at the time the offense is committed; (4) the offense is committed on board an aircraft which is operated by the United States; or (5) the offense was directed toward or resulted in the carrying out of a predicate act committed in an attempt to compel the United States to do or abstain from doing any act. (c) Concealment.— Whoever— (1) (A) is in the United States; or (B) is outside the United States and is a national of the United States or a legal entity organized under the laws of the United States (including any of its States, districts, commonwealths, territories, or possessions); and (2) knowingly conceals or disguises the nature, location, source, ownership, or control of any material support or resources, or any funds or proceeds of such funds— (A) knowing or intending that the support or resources are to be provided, or knowing that the support or resources were provided, in violation of section 2339B of this title; or (B) knowing or intending that any such funds are to be provided or collected, or knowing that the funds were provided or collected, in violation of subsection (a), shall be punished as prescribed in subsection (d)(2). (d) Penalties […] (e) Definitions.— In this section— (1) the term "funds" means assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including coin, currency, bank credits, travelers checks, bank checks, money orders, shares, securities, bonds, drafts, and letters of credit; (2) the term "government facility" means any permanent or temporary facility or conveyance that is used or occupied by representatives of a state, members of a government, the legislature, or the judiciary, or by officials or employees of a state or any other public authority or entity or by employees or officials of an intergovernmental organization in connection with their official duties; (3) the term "proceeds" means any funds derived from or obtained, directly or indirectly, through the commission of an offense set forth in subsection (a); (4) the term "provides" includes giving, donating, and transmitting; (5) the term "collects" includes raising and receiving; (6) the term "predicate act" means any act referred to in subparagraph (A) or (B) of subsection (a)(1); (7) the term "treaty" means— (A) the Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on December 16, 1970; (B) the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on September 23, 1971; (C) the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	December 14, 1973; (D) the International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on December 17, 1979; (E) the Convention on the Physical Protection of Nuclear Material, adopted at Vienna on March 3, 1980; (F) the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on February 24, 1988; (G) the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on March 10, 1988; (H) the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on March 10, 1988; or (I) the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on December 15, 1997; (8) the term "intergovernmental organization" includes international organizations; (9) the term "international organization" has the same meaning as in section 1116 (b)(5) of this title; (10) the term "armed conflict" does not include internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature; (11) the term "serious bodily injury" has the same meaning as in section 1365 (g)(3) of this title; [1] (12) the term "national of the United States" has the meaning given that term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22)); (13) the term "material support or resources" has the same meaning given that term in section 2339B (g)(4) of this title; and (14) the term "state" has the same meaning as that term has under international law, and includes all political subdivisions thereof. (f) Civil Penalty […]
"*Military-type training from a foreign terrorist organization*"	**Sec. 2339D. Receiving military-type training from a foreign terrorist organization** (a) Offense.— Whoever knowingly receives military-type training from or on behalf of any organization designated at the time of the training by the Secretary of State under section 219(a)(1) of the Immigration and Nationality Act as a foreign terrorist organization shall be fined under this title or imprisoned for ten years, or both. To violate this subsection, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (c)(4)), that the organization has engaged or engages in terrorist activity (as defined in section 212 of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989). (b) Extraterritorial Jurisdiction.— There is extraterritorial Federal jurisdiction over an offense under this section. There is jurisdiction over an offense under subsection (a) if— (1) an offender is a national of the United States (as defined in [1] 101(a)(22) of the Immigration and Nationality Act) or an alien lawfully admitted for permanent residence in the United States (as defined in section 101(a)(20) of the Immigration and Nationality Act); (2) an offender is a stateless person whose habitual residence is in the United States; (3) after the conduct required for the offense occurs an offender is brought into or found in the United States, even if the conduct required for the offense occurs outside the United States; (4) the offense occurs in whole or in part within the United States; (5) the offense occurs in or affects interstate or foreign commerce; or (6) an offender aids or abets any person over whom jurisdiction exists under this paragraph in committing an offense under subsection (a) or conspires with any person over whom jurisdiction exists under this paragraph to commit an offense under subsection (a). (c) Definitions.— As used in this section— (1) the term "military-type training" includes training in means or methods that can cause death or serious bodily injury, destroy or damage property, or disrupt services to critical infrastructure, or training on the use, storage, production, or assembly of any explosive, firearm or other weapon, including any weapon of mass destruction (as defined in section 2232a (c)(2) [2]); (2) the term "serious bodily injury" has the meaning given that term in section 1365 (h)(3); (3) the term "critical infrastructure" means systems and assets vital to national defense, national security, economic security, public health or safety including both regional and national infrastructure. Critical infrastructure may be publicly or privately owned; examples of critical infrastructure include gas and oil production, storage, or delivery systems, water supply systems, telecommunications networks, electrical power generation or delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), and transportation systems and services (including highways, mass transit, airlines, and airports); and (4) the term "foreign terrorist organization" means an organization designated as a terrorist organization under section 219(a)(1) of the Immigration and Nationality Act.
"*Torture*"	**Sec. 2340A. Torture** (a) Offense.— Whoever outside the United States commits or attempts to commit torture shall be fined under this title or imprisoned not more than 20 years, or both, and if death results to any person from conduct prohibited by this subsection, shall be punished by death or imprisoned for any term of years or for life. (b) Jurisdiction.— There is jurisdiction over the activity prohibited in subsection (a) if— (1) the alleged offender is a national of the United States; or (2) the alleged offender is present in the United States, irrespective of the nationality of the victim or alleged offender. (c) Conspiracy.— A person who conspires to commit an offense under this section shall be subject to the same penalties (other than the penalty of death) as the penalties prescribed for the offense, the commission of which was the object of the conspiracy.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Atomic weapons*"	SUBSECTION 2332b(5)(B)(ii) SPECIFICALLY REFERS TO: **Sec. 2122. Prohibitions governing atomic weapons** (a) It shall be unlawful, except as provided in section 2121 of this title, for any person, inside or outside of the United States, to knowingly participate in the development of, manufacture, produce, transfer, acquire, receive, possess, import, export, or use, or possess and threaten to use, any atomic weapon. Nothing in this section shall be deemed to modify the provisions of section 2051 (a) or 2131 of this title. (b) Conduct prohibited by subsection (a) of this section is within the jurisdiction of the United States if— (1) the offense occurs in or affects interstate or foreign commerce; the offense occurs outside of the United States and is committed by a national of the United States; (2) the offense is committed against a national of the United States while the national is outside the United States; (3) the offense is committed against any property that is owned, leased, or used by the United States or by any department or agency of the United States, whether the property is within or outside the United States; or (4) an offender aids or abets any person over whom jurisdiction exists under this subsection in committing an offense under this section or conspires with any person over whom jurisdiction exists under this subsection to commit an offense under this section.
"*Sabotage of nuclear facilities or fuel*"	**Sec. 2284. Sabotage of nuclear facilities or fuel** (a) Physical damage to facilities, etc. Any person who knowingly destroys or causes physical damage to— (1) any production facility or utilization facility licensed under this chapter; (2) any nuclear waste treatment, storage, or disposal facility licensed under this chapter; (3) any nuclear fuel for a utilization facility licensed under this chapter, or any spent nuclear fuel from such a facility; (4) any uranium enrichment, uranium conversion, or nuclear fuel fabrication facility licensed or certified by the Nuclear Regulatory Commission; (5) any production, utilization, waste storage, waste treatment, waste disposal, uranium enrichment, uranium conversion, or nuclear fuel fabrication facility subject to licensing or certification under this chapter during construction of the facility, if the destruction or damage caused or attempted to be caused could adversely affect public health and safety during the operation of the facility; (6) any primary facility or backup facility from which a radiological emergency preparedness alert and warning system is activated; or (7) any radioactive material or other property subject to regulation by the Commission that, before the date of the offense, the Commission determines, by order or regulation published in the Federal Register, is of significance to the public health and safety or to common defense and security; or attempts or conspires to do such an act, shall be fined not more than $10,000 or imprisoned for not more than 20 years, or both, and, if death results to any person, shall be imprisoned for any term of years or for life. (b) Unauthorized use or tampering with facilities, etc. Any person who knowingly causes an interruption of normal operation of any such facility through the unauthorized use of or tampering with the machinery, components, or controls of any such facility, or attempts or conspires to do such an act, shall be fined not more than $10,000 or imprisoned for not more than 20 years, or both, and, if death results to any person, shall be imprisoned for any term of years or for life.
"*Aircraft piracy*"	SUBSECTION 2332b(5)(B)(iii) SPECIFICALLY REFERS TO: **Sec. 46502. Aircraft piracy** (a) In Special Aircraft Jurisdiction.— (1) In this subsection— (A) "aircraft piracy" means seizing or exercising control of an aircraft in the special aircraft jurisdiction of the United States by force, violence, threat of force or violence, or any form of intimidation, and with wrongful intent. (B) an attempt to commit aircraft piracy is in the special aircraft jurisdiction of the United States although the aircraft is not in flight at the time of the attempt if the aircraft would have been in the special aircraft jurisdiction of the United States had the aircraft piracy been completed. (2) An individual committing or attempting or conspiring to commit aircraft piracy— (A) shall be imprisoned for at least 20 years; or (B) notwithstanding section 3559 (b) of title 18, if the death of another individual results from the commission or attempt, shall be put to death or imprisoned for life. (b) Outside Special Aircraft Jurisdiction.— (1) An individual committing or conspiring to commit an offense (as defined in the Convention for the Suppression of Unlawful Seizure of Aircraft) on an aircraft in flight outside the special aircraft jurisdiction of the United States— (A) shall be imprisoned for at least 20 years; or (B) notwithstanding section 3559 (b) of title 18, if the death of another individual results from the commission or attempt, shall be put to death or imprisoned for life. (2) There is jurisdiction over the offense in paragraph (1) if—

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(A) a national of the United States was aboard the aircraft; (B) an offender is a national of the United States; or (C) an offender is afterwards found in the United States. (3) For purposes of this subsection, the term "national of the United States" has the meaning prescribed in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(22)).
"*Interference with flight crew members*"	**Sec. 46504. Interference with flight crew members and attendants** An individual on an aircraft in the special aircraft jurisdiction of the United States who, by assaulting or intimidating a flight crew member or flight attendant of the aircraft, interferes with the performance of the duties of the member or attendant or lessens the ability of the member or attendant to perform those duties, or attempts or conspires to do such an act, shall be fined under title 18, imprisoned for not more than 20 years, or both. However, if a dangerous weapon is used in assaulting or intimidating the member or attendant, the individual shall be imprisoned for any term of years or for life.
"*Weapon or explosive on an aircraft*"	**Sec. 46505. Carrying a weapon or explosive on an aircraft** (a) Definition.— In this section, "loaded firearm" means a starter gun or a weapon designed or converted to expel a projectile through an explosive, that has a cartridge, a detonator, or powder in the chamber, magazine, cylinder, or clip. (b) General Criminal Penalty.— An individual shall be fined under title 18, imprisoned for not more than 10 years, or both, if the individual— (1) when on, or attempting to get on, an aircraft in, or intended for operation in, air transportation or intrastate air transportation, has on or about the individual or the property of the individual a concealed dangerous weapon that is or would be accessible to the individual in flight; (2) has placed, attempted to place, or attempted to have placed a loaded firearm on that aircraft in property not accessible to passengers in flight; or (3) has on or about the individual, or has placed, attempted to place, or attempted to have placed on that aircraft, an explosive or incendiary device. (c) Criminal Penalty Involving Disregard for Human Life.— An individual who willfully and without regard for the safety of human life, or with reckless disregard for the safety of human life, violates subsection (b) of this section, shall be fined under title 18, imprisoned for not more than 20 years, or both, and, if death results to any person, shall be imprisoned for any term of years or for life. (d) Nonapplication.— Subsection (b)(1) of this section does not apply to— (1) a law enforcement officer of a State or political subdivision of a State, or an officer or employee of the United States Government, authorized to carry arms in an official capacity; (2) another individual the Administrator of the Federal Aviation Administration or the Under Secretary of Transportation for Security by regulation authorizes to carry a dangerous weapon in air transportation or intrastate air transportation; or (3) an individual transporting a weapon (except a loaded firearm) in baggage not accessible to a passenger in flight if the air carrier was informed of the presence of the weapon. (e) Conspiracy.— If two or more persons conspire to violate subsection (b) or (c), and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in such subsection.
"*Application of certain criminal laws to acts on aircraft*"	**Sec. 46506. Application of certain criminal laws to acts on aircraft** An individual on an aircraft in the special aircraft jurisdiction of the United States who commits an act that— (1) if committed in the special maritime and territorial jurisdiction of the United States (as defined in section 7 of title 18) would violate section 113, 114, 661, 662, 1111, 1112, 1113, or 2111 or chapter 109A of title 18, shall be fined under title 18, imprisoned under that section or chapter, or both; or (2) if committed in the District of Columbia would violate section 9 of the Act of July 29, 1892 (D.C. Code § 22-1112), shall be fined under title 18, imprisoned under section 9 of the Act, or both.
"*Destruction of interstate gas or hazardous liquid pipeline facility*"	**Sec. 60123. Criminal penalties** (a) General Penalty.— A person knowingly and willfully violating section 60114 (b), 60118 (a), or 60128 of this title or a regulation prescribed or order issued under this chapter shall be fined under title 18, imprisoned for not more than 5 years, or both. (b) Penalty for Damaging or Destroying Facility.— A person knowingly and willfully damaging or destroying an interstate gas pipeline facility, an interstate hazardous liquid pipeline facility, or either an intrastate gas pipeline facility or intrastate hazardous liquid pipeline facility that is used in interstate or foreign commerce or in any activity affecting interstate or foreign commerce, or attempting or conspiring to do such an act, shall be fined under title 18, imprisoned for not more than 20 years, or both, and, if death results to any person, shall be imprisoned for any term of years or for life. (c) Penalty for Damaging or Destroying Sign.— A person knowingly and willfully defacing, damaging, removing, or destroying a pipeline sign or right-of-way marker required by a law or regulation of the United States shall be fined under title 18, imprisoned for not more than one year, or both. (d) Penalty for Not Using One-Call Notification System or Not Heeding Location Information or Markings.— A person shall be fined under title 18, imprisoned for not more than 5 years, or both, if the person— (1) knowingly and willfully engages in an excavation activity— (A) without first using an available one-call notification system to establish the location of underground facilities in the excavation area; or (B) without paying attention to appropriate location information or markings the operator of a pipeline facility establishes; and (2) subsequently damages— (A) a pipeline facility that results in death, serious bodily harm, or actual damage to property of more than $50,000; (B) a pipeline facility, and knows or has reason to know of the damage, but does not report the damage promptly to the operator of the pipeline facility and to other appropriate authorities; or

000402

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Narco-terrorism*"	(C) a hazardous liquid pipeline facility that results in the release of more than 50 barrels of product. Penalties under this subsection may be reduced in the case of a violation that is promptly reported by the violator. SUBSECTION 2332b(5)(B)(iv) SPECIFICALLY REFERS TO SECTION 1010A OF THE *Controlled Substance Import and Export Act*, WHICH IS CONTAINED IN SECTION 960a OF THE *US CODE* AND READS AS FOLLOWS: **Sec. 960a. Foreign terrorist organizations, terrorist persons and groups** (a) Prohibited acts Whoever engages in conduct that would be punishable under section 841 (a) [1] of this title if committed within the jurisdiction of the United States, or attempts or conspires to do so, knowing or intending to provide, directly or indirectly, anything of pecuniary value to any person or organization that has engaged or engages in terrorist activity (as defined in section 1182 (a)(3)(B) of title 8) or terrorism (as defined in section 2656f (d)(2) of title 22), shall be sentenced to a term of imprisonment of not less than twice the minimum punishment under section 841 (b)(1),[1] and not more than life, a fine in accordance with the provisions of title 18, or both. Notwithstanding section 3583 of title 18, any sentence imposed under this subsection shall include a term of supervised release of at least 5 years in addition to such term of imprisonment. (b) Jurisdiction There is jurisdiction over an offense under this section if— (1) the prohibited drug activity or the terrorist offense is in violation of the criminal laws of the United States; (2) the offense, the prohibited drug activity, or the terrorist offense occurs in or affects interstate or foreign commerce; (3) an offender provides anything of pecuniary value for a terrorist offense that causes or is designed to cause death or serious bodily injury to a national of the United States while that national is outside the United States, or substantial damage to the property of a legal entity organized under the laws of the United States (including any of its States, districts, commonwealths, territories, or possessions) while that property is outside of the United States; (4) the offense or the prohibited drug activity occurs in whole or in part outside of the United States (including on the high seas), and a perpetrator of the offense or the prohibited drug activity is a national of the United States or a legal entity organized under the laws of the United States (including any of its States, districts, commonwealths, territories, or possessions); or (5) after the conduct required for the offense occurs an offender is brought into or found in the United States, even if the conduct required for the offense occurs outside the United States. (c) Proof requirements To violate subsection (a), a person must have knowledge that the person or organization has engaged or engages in terrorist activity (as defined in section 1182 (a)(3)(B) of title 8) or terrorism (as defined in section 2656f (d)(2) of title 22). (d) Definition As used in this section, the term "anything of pecuniary value" has the meaning given the term in section 1958 (b)(1) of title 18.
United Kingdom "*Membership in a terrorist organization*"	***Terrorism Act 2000***[23]**:** **Sec. 11 Membership** (1) A person commits an offence if he belongs or professes to belong to a proscribed organisation. (2) It is a defence for a person charged with an offence under subsection (1) to prove— (a) that the organisation was not proscribed on the last (or only) occasion on which he became a member or began to profess to be a member, and (b) that he has not taken part in the activities of the organisation at any time while it was proscribed. (3) A person guilty of an offence under this section shall be liable— (a) on conviction on indictment, to imprisonment for a term not exceeding ten years, to a fine or to both, or (b) on summary conviction, to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both. (4) In subsection (2) "proscribed" means proscribed for the purposes of any of the following— (a) this Act; (b) the Northern Ireland (Emergency Provisions) Act 1996; (c) the Northern Ireland (Emergency Provisions) Act 1991; (d) the Prevention of Terrorism (Temporary Provisions) Act 1989; (e) the Prevention of Terrorism (Temporary Provisions) Act 1984; (f) the Northern Ireland (Emergency Provisions) Act 1978; (g) the Prevention of Terrorism (Temporary Provisions) Act 1976; (h) the Prevention of Terrorism (Temporary Provisions) Act 1974;

[23] UK *Terrorism Act 2000*: http://www.legislation.gov.uk/ukpga/2000/11/contents

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(i) the Northern Ireland (Emergency Provisions) Act 1973.
"*Support to a terrorist organization*"	**Sec. 12 Support** (1) A person commits an offence if— (a) he invites support for a proscribed organisation, and (b) the support is not, or is not restricted to, the provision of money or other property (within the meaning of section 15). (2) A person commits an offence if he arranges, manages or assists in arranging or managing a meeting which he knows is— (a) to support a proscribed organisation, (b) to further the activities of a proscribed organisation, or (c) to be addressed by a person who belongs or professes to belong to a proscribed organisation. (3) A person commits an offence if he addresses a meeting and the purpose of his address is to encourage support for a proscribed organisation or to further its activities. (4) Where a person is charged with an offence under subsection (2)(c) in respect of a private meeting it is a defence for him to prove that he had no reasonable cause to believe that the address mentioned in subsection (2)(c) would support a proscribed organisation or further its activities. (5) In subsections (2) to (4)— (a) "meeting" means a meeting of three or more persons, whether or not the public are admitted, and (b) a meeting is private if the public are not admitted. (6) A person guilty of an offence under this section shall be liable— (a) on conviction on indictment, to imprisonment for a term not exceeding ten years, to a fine or to both, or (b) on summary conviction, to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both.
"*Wearing the uniform of a terrorist organization*"	**Sec. 13 Uniform** (1) A person in a public place commits an offence if he— (a) wears an item of clothing, or (b) wears, carries or displays an article, in such a way or in such circumstances as to arouse reasonable suspicion that he is a member or supporter of a proscribed organization. (2) A constable in Scotland may arrest a person without a warrant if he has reasonable grounds to suspect that the person is guilty of an offence under this section. (3) A person guilty of an offence under this section shall be liable on summary conviction to— (a) imprisonment for a term not exceeding six months, (b) a fine not exceeding level 5 on the standard scale, or (c) both.
"*Fund-raising for a terrorist organization*"	**Sec. 15 Fund-raising** (1) A person commits an offence if he— (a) invites another to provide money or other property, and (b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism. (2) A person commits an offence if he— (a) receives money or other property, and (b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism. (3) A person commits an offence if he— (a) provides money or other property, and (b) knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism. (4) In this section a reference to the provision of money or other property is a reference to its being given, lent or otherwise made available, whether or not for consideration.
"*Use and possession of money for terrorism*"	**Sec. 16 Use and possession** (1) A person commits an offence if he uses money or other property for the purposes of terrorism. (2) A person commits an offence if he— (a) possesses money or other property, and

[24] UK *Anti-terrorism, Crime and Security Act 2001*: http://www.legislation.gov.uk/ukpga/2001/24/contents
[25] UK *Terrorism Act 2006*: http://www.legislation.gov.uk/ukpga/2006/11/contents

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Funding arrangements*" "*Money laundering*"	(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism. **Sec. 17 Funding arrangements** A person commits an offence if— (a) he enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to be made available to another, and (b) he knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism. **Sec. 18 Money laundering** (1) A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property— (a) by concealment, (b) by removal from the jurisdiction, (c) by transfer to nominees, or (d) in any other way. (2) It is a defence for a person charged with an offence under subsection (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property. THIS PROVISION IS TO BE READ IN CONJUNCTION WITH: **Sec. 14 Terrorist property** (1) In this Act "terrorist property" means— (a) money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation), (b) proceeds of the commission of acts of terrorism, and (c) proceeds of acts carried out for the purposes of terrorism. (2) In subsection (1)— (a) a reference to proceeds of an act includes a reference to any property which wholly or partly, and directly or indirectly, represents the proceeds of the act (including payments or other rewards in connection with its commission), and (b) the reference to an organisation's resources includes a reference to any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation.
"*Failure to disclose knowledge of terrorist funding*" "*Disclosure of information about a terrorist investigation (terrorist funding)*"	**Sec. 19 Disclosure of information: duty** (1) This section applies where a person— (a) believes or suspects that another person has committed an offence under any of sections 15 to 18, and (b) bases his belief or suspicion on information which comes to his attention— (i) in the course of a trade, profession or business, or (ii) in the course of his employment (whether or not in the course of a trade, profession or business). (1A) But this section does not apply if the information came to the person in the course of a business in the regulated sector. (2) The person commits an offence if he does not disclose to a constable as soon as is reasonably practicable— (a) his belief or suspicion, and (b) the information on which it is based. **Sec. 21D Tipping off: regulated sector** (1) A person commits an offence if— (a) the person discloses any matter within subsection (2); (b) the disclosure is likely to prejudice any investigation that might be conducted following the disclosure referred to in that subsection; and (c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector. (2) The matters are that the person or another person has made a disclosure under a provision of this Part— (a) to a constable, (b) in accordance with a procedure established by that person's employer for the making of disclosures under that provision, (c) to a nominated officer, or (d) to a member of staff of the Serious Organised Crime Agency authorised for the purposes of that provision by the Director General of that Agency, of information that came to that person in the course of a business in the regulated sector.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Failure to disclose information about act of terrorism*"	(3) A person commits an offence if— (a) the person discloses that an investigation into allegations that an offence under this Part has been committed is being contemplated or is being carried out; (b) the disclosure is likely to prejudice that investigation; and (c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector. (4) A person guilty of an offence under this section is liable— (a) on summary conviction to imprisonment for a term not exceeding three months, or to a fine not exceeding level 5 on the standard scale, or to both; (b) on conviction on indictment to imprisonment for a term not exceeding two years, or to a fine, or to both. (5) This section is subject to— (a) section 21E (disclosures within an undertaking or group etc), (b) section 21F (other permitted disclosures between institutions etc), and (c) section 21G (other permitted disclosures etc). **Sec. 38B Information about acts of terrorism** (1) This section applies where a person has information which he knows or believes might be of material assistance— (a) in preventing the commission by another person of an act of terrorism, or (b) in securing the apprehension, prosecution or conviction of another person, in the United Kingdom, for an offence involving the commission, preparation or instigation of an act of terrorism. (2) The person commits an offence if he does not disclose the information as soon as reasonably practicable in accordance with subsection (3). (3) Disclosure is in accordance with this subsection if it is made— (a) in England and Wales, to a constable, (b) in Scotland, to a constable, or (c) in Northern Ireland, to a constable or a member of Her Majesty's forces. (4) It is a defence for a person charged with an offence under subsection (2) to prove that he had a reasonable excuse for not making the disclosure. (5) A person guilty of an offence under this section shall be liable— (a) on conviction on indictment, to imprisonment for a term not exceeding five years, or to a fine or to both, or (b) on summary conviction, to imprisonment for a term not exceeding six months, or to a fine not exceeding the statutory maximum or to both. (6) Proceedings for an offence under this section may be taken, and the offence may for the purposes of those proceedings be treated as having been committed, in any place where the person to be charged is or has at any time been since he first knew or believed that the information might be of material assistance as mentioned in subsection (1).
"*Disclosure of information about a terrorist investigation (terrorist acts)*"	**Sec. 39 Disclosure of information, &c.** (1) Subsection (2) applies where a person knows or has reasonable cause to suspect that a constable is conducting or proposes to conduct a terrorist investigation. (2) The person commits an offence if he— (a) discloses to another anything which is likely to prejudice the investigation, or (b) interferes with material which is likely to be relevant to the investigation. (3) Subsection (4) applies where a person knows or has reasonable cause to suspect that a disclosure has been or will be made under any of sections 19 to [F821B][F9or 38B]. (4) The person commits an offence if he— (a) discloses to another anything which is likely to prejudice an investigation resulting from the disclosure under that section, or (b) interferes with material which is likely to be relevant to an investigation resulting from the disclosure under that section. (5) It is a defence for a person charged with an offence under subsection (2) or (4) to prove— (a) that he did not know and had no reasonable cause to suspect that the disclosure or interference was likely to affect a terrorist investigation, or (b) that he had a reasonable excuse for the disclosure or interference. (6) Subsections (2) and (4) do not apply to a disclosure which is made by a professional legal adviser— (a) to his client or to his client's representative in connection with the provision of legal advice by the adviser to the client and not with a view to furthering a criminal purpose, or (b) to any person for the purpose of actual or contemplated legal proceedings and not with a view to furthering a criminal purpose. (6A) Subsections (2) and (4) do not apply if— (a) the disclosure is of a matter within section 21D(2) or (3)(a) (terrorist property: tipping off), and (b) the information on which the disclosure is based came to the person in the course of a business in the regulated sector. (7) A person guilty of an offence under this section shall be liable— (a) on conviction on indictment, to imprisonment for a term not exceeding five years, to a fine or to both, or (b) on summary conviction, to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both. (8) For the purposes of this section— (a) a reference to conducting a terrorist investigation includes a reference to taking part in the conduct of, or assisting, a terrorist investigation, and

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(b) a person interferes with material if he falsifies it, conceals it, destroys it or disposes of it, or if he causes or permits another to do any of those things. (9) The reference in subsection (6A) to a business in the regulated sector is to be construed in accordance with Schedule 3A.
"*Weapons training*"	**Sec. 54 Weapons training** (1) A person commits an offence if he provides instruction or training in the making or use of— (a) firearms, (aa) radioactive material or weapons designed or adapted for the discharge of any radioactive material,] (b) explosives, or (c) chemical, biological or nuclear weapons. (2) A person commits an offence if he receives instruction or training in the making or use of— (a) firearms, (aa) radioactive material or weapons designed or adapted for the discharge of any radioactive material,] (b) explosives, or (c) chemical, biological or nuclear weapons. (3) A person commits an offence if he invites another to receive instruction or training and the receipt— (a) would constitute an offence under subsection (2), or (b) would constitute an offence under subsection (2) but for the fact that it is to take place outside the United Kingdom. (4) For the purpose of subsections (1) and (3)— (a) a reference to the provision of instruction includes a reference to making it available either generally or to one or more specific persons, and (b) an invitation to receive instruction or training may be either general or addressed to one or more specific persons. (5) It is a defence for a person charged with an offence under this section in relation to instruction or training to prove that his action or involvement was wholly for a purpose other than assisting, preparing for or participating in terrorism. (6) A person guilty of an offence under this section shall be liable— (a) on conviction on indictment, to imprisonment for a term not exceeding ten years, to a fine or to both, or (b) on summary conviction, to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both.
"*Directing terrorist organization*"	**Sec. 56 Directing terrorist organisation** (1) A person commits an offence if he directs, at any level, the activities of an organisation which is concerned in the commission of acts of terrorism. (2) A person guilty of an offence under this section is liable on conviction on indictment to imprisonment for life.
"*Possession for terrorist purposes*"	**Sec. 57 Possession for terrorist purposes** (1) A person commits an offence if he possesses an article in circumstances which give rise to a reasonable suspicion that his possession is for a purpose connected with the commission, preparation or instigation of an act of terrorism. (2) It is a defence for a person charged with an offence under this section to prove that his possession of the article was not for a purpose connected with the commission, preparation or instigation of an act of terrorism. (3) In proceedings for an offence under this section, if it is proved that an article— (a) was on any premises at the same time as the accused, or (b) was on premises of which the accused was the occupier or which he habitually used otherwise than as a member of the public, the court may assume that the accused possessed the article, unless he proves that he did not know of its presence on the premises or that he had no control over it. (4) A person guilty of an offence under this section shall be liable— (a) on conviction on indictment, to imprisonment for a term not exceeding 15 years, to a fine or to both, or (b) on summary conviction, to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both.
"*Collection of information for terrorist purpose*"	**Sec. 58 Collection of information** (1) A person commits an offence if— (a) he collects or makes a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or (b) he possesses a document or record containing information of that kind. (2) In this section "record" includes a photographic or electronic record. (3) It is a defence for a person charged with an offence under this section to prove that he had a reasonable excuse for his action or possession. (4) A person guilty of an offence under this section shall be liable—

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(a) on conviction on indictment, to imprisonment for a term not exceeding 10 years, to a fine or to both, or (b) on summary conviction, to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both.
"*Incitement to terrorism*"	**Sec. 59 England and Wales** (1) A person commits an offence if— (a) he incites another person to commit an act of terrorism wholly or partly outside the United Kingdom, and (b) the act would, if committed in England and Wales, constitute one of the offences listed in subsection (2). (2) Those offences are— (a) murder, (b) an offence under section 18 of the Offences against the Person Act 1861 (wounding with intent), (c) an offence under section 23 or 24 of that Act (poison), (d) an offence under section 28 or 29 of that Act (explosions), and (e) an offence under section 1(2) of the Criminal Damage Act 1971 (endangering life by damaging property). (3) A person guilty of an offence under this section shall be liable to any penalty to which he would be liable on conviction of the offence listed in subsection (2) which corresponds to the act which he incites. (4) For the purposes of subsection (1) it is immaterial whether or not the person incited is in the United Kingdom at the time of the incitement. (5) Nothing in this section imposes criminal liability on any person acting on behalf of, or holding office under, the Crown.
"*Terrorist attacks abroad against UK nationals*"	**Sec. 63B Terrorist attacks abroad by UK nationals or residents: jurisdiction** (1) If— (a) a United Kingdom national or a United Kingdom resident does anything outside the United Kingdom as an act of terrorism or for the purposes of terrorism, and (b) his action, if done in any part of the United Kingdom, would have constituted an offence listed in subsection (2), he shall be guilty in that part of the United Kingdom of the offence. (2) These are the offences— (a) murder, manslaughter, culpable homicide, rape, assault causing injury, assault to injury, kidnapping, abduction or false imprisonment, (b) an offence under section 4, 16, 18, 20, 21, 22, 23, 24, 28, 29, 30 or 64 of the Offences against the Person Act 1861, (c) an offence under any of sections 1 to 5 of the Forgery and Counterfeiting Act 1981, (d) the uttering of a forged document or an offence under section 46A of the Criminal Law (Consolidation) (Scotland) Act 1995, (e) an offence under section 1 or 2 of the Criminal Damage Act 1971, (f) an offence under Article 3 or 4 of the Criminal Damage (Northern Ireland) Order 1977, (g) malicious mischief, (h) wilful fire-raising.
"*Terrorist attacks abroad against UK nationals and protected persons*"	**Sec. 63C Terrorist attacks abroad on UK nationals, residents and diplomatic staff etc: jurisdiction** (1) If— (a) a person does anything outside the United Kingdom as an act of terrorism or for the purposes of terrorism, (b) his action is done to, or in relation to, a United Kingdom national, a United Kingdom resident or a protected person, and (c) his action, if done in any part of the United Kingdom, would have constituted an offence listed in subsection (2), he shall be guilty in that part of the United Kingdom of the offence. (2) These are the offences— (a) murder, manslaughter, culpable homicide, rape, assault causing injury, assault to injury, kidnapping, abduction or false imprisonment, (b) an offence under section 4, 16, 18, 20, 21, 22, 23, 24, 28, 29, 30 or 64 of the Offences against the Person Act 1861, (c) an offence under section 1, 2, 3, 4 or 5(1) or (3) of the Forgery and Counterfeiting Act 1981, (d) the uttering of a forged document or an offence under section 46A(1) of the Criminal Law (Consolidation) (Scotland) Act 1995. (3) For the purposes of this section and section 63D a person is a protected person if— (a) he is a member of a United Kingdom diplomatic mission within the meaning of Article 1(b) of the Vienna Convention on Diplomatic Relations signed in 1961 (as that Article has effect in the United Kingdom by virtue of section 2 of and Schedule 1 to the Diplomatic Privileges Act 1964), (b) he is a member of a United Kingdom consular post within the meaning of Article 1(g) of the Vienna Convention on Consular Relations signed in 1963 (as that Article has effect in the United Kingdom by virtue of section 1 of and Schedule 1 to the Consular Relations Act 1968), (c) he carries out any functions for the purposes of the the European Medicines Agency , or

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Terrorist attacks or threats abroad in connection with UK diplomatic premises*"	(d) he carries out any functions for the purposes of a body specified in an order made by the Secretary of State. (4) The Secretary of State may specify a body under subsection (3)(d) only if— (a) it is established by or under the Treaty establishing the European Community or the Treaty on European Union, and (b) the principal place in which its functions are carried out is a place in the United Kingdom. (5) If in any proceedings a question arises as to whether a person is or was a protected person, a certificate— (a) issued by or under the authority of the Secretary of State, and (b) stating any fact relating to the question, is to be conclusive evidence of that fact. **Sec. 63D Terrorist attacks or threats abroad in connection with UK diplomatic premises etc: jurisdiction** (1) If— (a) a person does anything outside the United Kingdom as an act of terrorism or for the purposes of terrorism, (b) his action is done in connection with an attack on relevant premises or on a vehicle ordinarily used by a protected person, (c) the attack is made when a protected person is on or in the premises or vehicle, and (d) his action, if done in any part of the United Kingdom, would have constituted an offence listed in subsection (2), he shall be guilty in that part of the United Kingdom of the offence. (2) These are the offences— (a) an offence under section 1 of the Criminal Damage Act 1971, (b) an offence under Article 3 of the Criminal Damage (Northern Ireland) Order 1977, (c) malicious mischief, (d) wilful fire-raising. (3) If— (a) a person does anything outside the United Kingdom as an act of terrorism or for the purposes of terrorism, (b) his action consists of a threat of an attack on relevant premises or on a vehicle ordinarily used by a protected person, (c) the attack is threatened to be made when a protected person is, or is likely to be, on or in the premises or vehicle, and (d) his action, if done in any part of the United Kingdom, would have constituted an offence listed in subsection (4), he shall be guilty in that part of the United Kingdom of the offence. (4) These are the offences— (a) an offence under section 2 of the Criminal Damage Act 1971, (b) an offence under Article 4 of the Criminal Damage (Northern Ireland) Order 1977, (c) breach of the peace (in relation to Scotland only). (5) "Relevant premises" means— (a) premises at which a protected person resides or is staying, or (b) premises which a protected person uses for the purpose of carrying out his functions as such a person.
"*Use of noxious substances*"	***Anti-terrorism, Crime and Security Act 2001***[24]**:** **Sec. 113 Use of noxious substances or things to cause harm and intimidate** (1) A person who takes any action which— (a) involves the use of a noxious substance or other noxious thing; (b) has or is likely to have an effect falling within subsection (2); and (c) is designed to influence the government [F1or an international governmental organisation] or to intimidate the public or a section of the public, is guilty of an offence. (2) Action has an effect falling within this subsection if it— (a) causes serious violence against a person anywhere in the world; (b) causes serious damage to real or personal property anywhere in the world; (c) endangers human life or creates a serious risk to the health or safety of the public or a section of the public; or (d) induces in members of the public the fear that the action is likely to endanger their lives or create a serious risk to their health or safety; but any effect on the person taking the action is to be disregarded. (3) A person who— (a) makes a threat that he or another will take any action which constitutes an offence under subsection (1); and

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(b) intends thereby to induce in a person anywhere in the world the fear that the threat is likely to be carried out, is guilty of an offence. (4) A person guilty of an offence under this section is liable— (a) on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum (or both); and (b) on conviction on indictment, to imprisonment for a term not exceeding fourteen years or a fine (or both). (5) In this section— "the government" means the government of the United Kingdom, of a part of the United Kingdom or of a country other than the United Kingdom; and "the public" includes the public of a country other than the United Kingdom.
"*Hoaxes involving noxious substances*"	**Sec. 114 Hoaxes involving noxious substances or things** (1) A person is guilty of an offence if he— (a) places any substance or other thing in any place; or (b) sends any substance or other thing from one place to another (by post, rail or any other means whatever); with the intention of inducing in a person anywhere in the world a belief that it is likely to be (or contain) a noxious substance or other noxious thing and thereby endanger human life or create a serious risk to human health. (2) A person is guilty of an offence if he communicates any information which he knows or believes to be false with the intention of inducing in a person anywhere in the world a belief that a noxious substance or other noxious thing is likely to be present (whether at the time the information is communicated or later) in any place and thereby endanger human life or create a serious risk to human health. (3) A person guilty of an offence under this section is liable— (a) on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum (or both); and (b) on conviction on indictment, to imprisonment for a term not exceeding seven years or a fine (or both).
"*Encouragement of terrorism*"	***Terrorism Act 2006***[25]**:** **Sec. 1 Encouragement of terrorism** (1) This section applies to a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism or Convention offences. (2) A person commits an offence if— (a) he publishes a statement to which this section applies or causes another to publish such a statement; and (b) at the time he publishes it or causes it to be published, he— (i) intends members of the public to be directly or indirectly encouraged or otherwise induced by the statement to commit, prepare or instigate acts of terrorism or Convention offences; or (ii) is reckless as to whether members of the public will be directly or indirectly encouraged or otherwise induced by the statement to commit, prepare or instigate such acts or offences. (3) For the purposes of this section, the statements that are likely to be understood by members of the public as indirectly encouraging the commission or preparation of acts of terrorism or Convention offences include every statement which— (a) glorifies the commission or preparation (whether in the past, in the future or generally) of such acts or offences; and (b) is a statement from which those members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances. (4) For the purposes of this section the questions how a statement is likely to be understood and what members of the public could reasonably be expected to infer from it must be determined having regard both— (a) to the contents of the statement as a whole; and (b) to the circumstances and manner of its publication. (5) It is irrelevant for the purposes of subsections (1) to (3)— (a) whether anything mentioned in those subsections relates to the commission, preparation or instigation of one or more particular acts of terrorism or Convention offences, of acts of terrorism or Convention offences of a particular description or of acts of terrorism or Convention offences generally; and, (b) whether any person is in fact encouraged or induced by the statement to commit, prepare or instigate any such act or offence. (6) In proceedings for an offence under this section against a person in whose case it is not proved that he intended the statement directly or indirectly to encourage or otherwise induce the commission, preparation or instigation of acts of terrorism or Convention offences, it is a defence for him to show— (a) that the statement neither expressed his views nor had his endorsement (whether by virtue of section 3 or otherwise); and (b) that it was clear, in all the circumstances of the statement's publication, that it did not express his views and (apart from the possibility of his having been given and failed to comply with a notice under subsection (3) of that section) did not have his endorsement. (7) A person guilty of an offence under this section shall be liable—

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Dissemination of terrorist publications*"	(a) on conviction on indictment, to imprisonment for a term not exceeding 7 years or to a fine, or to both; (b) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum, or to both; (c) on summary conviction in Scotland or Northern Ireland, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum, or to both. (8) In relation to an offence committed before the commencement of section 154(1) of the Criminal Justice Act 2003 (c. 44), the reference in subsection (7)(b) to 12 months is to be read as a reference to 6 months. **Sec. 2 Dissemination of terrorist publications** (1) A person commits an offence if he engages in conduct falling within subsection (2) and, at the time he does so— (a) he intends an effect of his conduct to be a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism; (b) he intends an effect of his conduct to be the provision of assistance in the commission or preparation of such acts; or (c) he is reckless as to whether his conduct has an effect mentioned in paragraph (a) or (b). (2) For the purposes of this section a person engages in conduct falling within this subsection if he— (a) distributes or circulates a terrorist publication; (b) gives, sells or lends such a publication; (c) offers such a publication for sale or loan; (d) provides a service to others that enables them to obtain, read, listen to or look at such a publication, or to acquire it by means of a gift, sale or loan; (e) transmits the contents of such a publication electronically; or (f) has such a publication in his possession with a view to its becoming the subject of conduct falling within any of paragraphs (a) to (e). (3) For the purposes of this section a publication is a terrorist publication, in relation to conduct falling within subsection (2), if matter contained in it is likely— (a) to be understood, by some or all of the persons to whom it is or may become available as a consequence of that conduct, as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism; or (b) to be useful in the commission or preparation of such acts and to be understood, by some or all of those persons, as contained in the publication, or made available to them, wholly or mainly for the purpose of being so useful to them. (4) For the purposes of this section matter that is likely to be understood by a person as indirectly encouraging the commission or preparation of acts of terrorism includes any matter which— (a) glorifies the commission or preparation (whether in the past, in the future or generally) of such acts; and (b) is matter from which that person could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by him in existing circumstances. (5) For the purposes of this section the question whether a publication is a terrorist publication in relation to particular conduct must be determined— (a) as at the time of that conduct; and (b) having regard both to the contents of the publication as a whole and to the circumstances in which that conduct occurs. (6) In subsection (1) references to the effect of a person's conduct in relation to a terrorist publication include references to an effect of the publication on one or more persons to whom it is or may become available as a consequence of that conduct. (7) It is irrelevant for the purposes of this section whether anything mentioned in subsections (1) to (4) is in relation to the commission, preparation or instigation of one or more particular acts of terrorism, of acts of terrorism of a particular description or of acts of terrorism generally. (8) For the purposes of this section it is also irrelevant, in relation to matter contained in any article whether any person— (a) is in fact encouraged or induced by that matter to commit, prepare or instigate acts of terrorism; or (b) in fact makes use of it in the commission or preparation of such acts. (9) In proceedings for an offence under this section against a person in respect of conduct to which subsection (10) applies, it is a defence for him to show— (a) that the matter by reference to which the publication in question was a terrorist publication neither expressed his views nor had his endorsement (whether by virtue of section 3 or otherwise); and (b) that it was clear, in all the circumstances of the conduct, that that matter did not express his views and (apart from the possibility of his having been given and failed to comply with a notice under subsection (3) of that section) did not have his endorsement. (10) This subsection applies to the conduct of a person to the extent that— (a) the publication to which his conduct related contained matter by reference to which it was a terrorist publication by virtue of subsection (3)(a); and (b) that person is not proved to have engaged in that conduct with the intention specified in subsection (1)(a). (11) A person guilty of an offence under this section shall be liable— (a) on conviction on indictment, to imprisonment for a term not exceeding 7 years or to a fine, or to both; (b) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum, or to both; (c) on summary conviction in Scotland or Northern Ireland, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum, or to both. (12) In relation to an offence committed before the commencement of section 154(1) of the Criminal Justice Act 2003 (c. 44), the reference in subsection (11)(b) to 12 months is to be read as a reference to 6 months.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(13) In this section— "lend" includes let on hire, and "loan" is to be construed accordingly; "publication" means an article or record of any description that contains any of the following, or any combination of them— (a) matter to be read; (b) matter to be listened to; (c) matter to be looked at or watched.
"*Preparation of terrorist acts*"	**Sec. 5 Preparation of terrorist acts** (1) A person commits an offence if, with the intention of— (a) committing acts of terrorism, or (b) assisting another to commit such acts, he engages in any conduct in preparation for giving effect to his intention. (2) It is irrelevant for the purposes of subsection (1) whether the intention and preparations relate to one or more particular acts of terrorism, acts of terrorism of a particular description or acts of terrorism generally. (3) A person guilty of an offence under this section shall be liable, on conviction on indictment, to imprisonment for life.
"*Training for terrorism*"	**Sec. 6 Training for terrorism** (1) A person commits an offence if— (a) he provides instruction or training in any of the skills mentioned in subsection (3); and (b) at the time he provides the instruction or training, he knows that a person receiving it intends to use the skills in which he is being instructed or trained— (i) for or in connection with the commission or preparation of acts of terrorism or Convention offences; or (ii) for assisting the commission or preparation by others of such acts or offences. (2) A person commits an offence if— (a) he receives instruction or training in any of the skills mentioned in subsection (3); and (b) at the time of the instruction or training, he intends to use the skills in which he is being instructed or trained— (i) for or in connection with the commission or preparation of acts of terrorism or Convention offences; or (ii) for assisting the commission or preparation by others of such acts or offences. (3) The skills are— (a) the making, handling or use of a noxious substance, or of substances of a description of such substances; (b) the use of any method or technique for doing anything else that is capable of being done for the purposes of terrorism, in connection with the commission or preparation of an act of terrorism or Convention offence or in connection with assisting the commission or preparation by another of such an act or offence; and (c) the design or adaptation for the purposes of terrorism, or in connection with the commission or preparation of an act of terrorism or Convention offence, of any method or technique for doing anything. (4) It is irrelevant for the purposes of subsections (1) and (2)— (a) whether any instruction or training that is provided is provided to one or more particular persons or generally; (b) whether the acts or offences in relation to which a person intends to use skills in which he is instructed or trained consist of one or more particular acts of terrorism or Convention offences, acts of terrorism or Convention offences of a particular description or acts of terrorism or Convention offences generally; and (c) whether assistance that a person intends to provide to others is intended to be provided to one or more particular persons or to one or more persons whose identities are not yet known. (5) A person guilty of an offence under this section shall be liable— (a) on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine, or to both; (b) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum, or to both; (c) on summary conviction in Scotland or Northern Ireland, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum, or to both. (6) In relation to an offence committed before the commencement of section 154(1) of the Criminal Justice Act 2003 (c. 44), the reference in subsection (5)(b) to 12 months is to be read as a reference to 6 months. (7) In this section— "noxious substance" means— (a) a dangerous substance within the meaning of Part 7 of the Anti-terrorism, Crime and Security Act 2001 (c. 24); or (b) any other substance which is hazardous or noxious or which may be or become hazardous or noxious only in certain circumstances; "substance" includes any natural or artificial substance (whatever its origin or method of production and whether in solid or liquid form or in the form of a gas or vapour) and any mixture of substances.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Attendance at a place used for terrorist training*"	**Sec. 8 Attendance at a place used for terrorist training** (1) A person commits an offence if— (a) he attends at any place, whether in the United Kingdom or elsewhere; (b) while he is at that place, instruction or training of the type mentioned in section 6(1) of this Act or section 54(1) of the Terrorism Act 2000 (c. 11) (weapons training) is provided there; (c) that instruction or training is provided there wholly or partly for purposes connected with the commission or preparation of acts of terrorism or Convention offences; and (d) the requirements of subsection (2) are satisfied in relation to that person. (2) The requirements of this subsection are satisfied in relation to a person if— (a) he knows or believes that instruction or training is being provided there wholly or partly for purposes connected with the commission or preparation of acts of terrorism or Convention offences; or (b) a person attending at that place throughout the period of that person's attendance could not reasonably have failed to understand that instruction or training was being provided there wholly or partly for such purposes. (3) It is immaterial for the purposes of this section— (a) whether the person concerned receives the instruction or training himself; and (b) whether the instruction or training is provided for purposes connected with one or more particular acts of terrorism or Convention offences, acts of terrorism or Convention offences of a particular description or acts of terrorism or Convention offences generally. (4) A person guilty of an offence under this section shall be liable— (a) on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine, or to both; (b) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum, or to both; (c) on summary conviction in Scotland or Northern Ireland, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum, or to both. (5) In relation to an offence committed before the commencement of section 154(1) of the Criminal Justice Act 2003 (c. 44), the reference in subsection (4)(b) to 12 months is to be read as a reference to 6 months. (6) References in this section to instruction or training being provided include references to its being made available.
"*Making and possession of devices*"	**Sec. 9 Making and possession of devices or materials** (1) A person commits an offence if— (a) he makes or has in his possession a radioactive device, or (b) he has in his possession radioactive material, with the intention of using the device or material in the course of or in connection with the commission or preparation of an act of terrorism or for the purposes of terrorism, or of making it available to be so used. (2) It is irrelevant for the purposes of subsection (1) whether the act of terrorism to which an intention relates is a particular act of terrorism, an act of terrorism of a particular description or an act of terrorism generally. (3) A person guilty of an offence under this section shall be liable, on conviction on indictment, to imprisonment for life. (4) In this section— "radioactive device" means— (a) a nuclear weapon or other nuclear explosive device; (b) a radioactive material dispersal device; (c) a radiation-emitting device; "radioactive material" means nuclear material or any other radioactive substance which— (a) contains nuclides that undergo spontaneous disintegration in a process accompanied by the emission of one or more types of ionising radiation, such as alpha radiation, beta radiation, neutron particles or gamma rays; and (b) is capable, owing to its radiological or fissile properties, of— (i) causing serious bodily injury to a person; (ii) causing serious damage to property; (iii) endangering a person's life; or (iv) creating a serious risk to the health or safety of the public. (5) In subsection (4)— "device" includes any of the following, whether or not fixed to land, namely, machinery, equipment, appliances, tanks, containers, pipes and conduits; "nuclear material" has the same meaning as in the Nuclear Material (Offences) Act 1983 (c. 18) (see section 6 of that Act).
"*Misuse of devices*"	**Sec. 10 Misuse of devices or material and misuse and damage of facilities** (1) A person commits an offence if he uses—

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Terrorist threats relating to devices, materials or facilities*"	(a) a radioactive device, or (b) radioactive material, in the course of or in connection with the commission of an act of terrorism or for the purposes of terrorism. (2) A person commits an offence if, in the course of or in connection with the commission of an act of terrorism or for the purposes of terrorism, he uses or damages a nuclear facility in a manner which— (a) causes a release of radioactive material; or (b) creates or increases a risk that such material will be released. (3) A person guilty of an offence under this section shall be liable, on conviction on indictment, to imprisonment for life. (4) In this section— "nuclear facility" means— (a) a nuclear reactor, including a reactor installed in or on any transportation device for use as an energy source in order to propel it or for any other purpose; or (b) a plant or conveyance being used for the production, storage, processing or transport of radioactive material; "radioactive device" and "radioactive material" have the same meanings as in section 9. (5) In subsection (4)— "nuclear reactor" has the same meaning as in the Nuclear Installations Act 1965 (c. 57) (see section 26 of that Act); "transportation device" means any vehicle or any space object (within the meaning of the Outer Space Act 1986 (c. 38)). **Sec. 11 Terrorist threats relating to devices, materials or facilities** (1) A person commits an offence if, in the course of or in connection with the commission of an act of terrorism or for the purposes of terrorism— (a) he makes a demand— (i) for the supply to himself or to another of a radioactive device or of radioactive material; (ii) for a nuclear facility to be made available to himself or to another; or (iii) for access to such a facility to be given to himself or to another; (b) he supports the demand with a threat that he or another will take action if the demand is not met; and (c) the circumstances and manner of the threat are such that it is reasonable for the person to whom it is made to assume that there is real risk that the threat will be carried out if the demand is not met. (2) A person also commits an offence if— (a) he makes a threat falling within subsection (3) in the course of or in connection with the commission of an act of terrorism or for the purposes of terrorism; and (b) the circumstances and manner of the threat are such that it is reasonable for the person to whom it is made to assume that there is real risk that the threat will be carried out, or would be carried out if demands made in association with the threat are not met. (3) A threat falls within this subsection if it is— (a) a threat to use radioactive material; (b) a threat to use a radioactive device; or (c) a threat to use or damage a nuclear facility in a manner that releases radioactive material or creates or increases a risk that such material will be released. (4) A person guilty of an offence under this section shall be liable, on conviction on indictment, to imprisonment for life. (5) In this section— "nuclear facility" has the same meaning as in section 10; "radioactive device" and "radioactive material" have the same meanings as in section 9.
Australia "*Terrorist acts*"	***Criminal Code Act 1995***[26]**:** **Sec. 101.1 Terrorist acts** (1) A person commits an offence if the person engages in a terrorist act. Penalty: Imprisonment for life. (2) Section 15.4 (extended geographical jurisdiction—category D) applies to an offence against subsection (1). THIS PROVISION IS TO BE READ IN CONJUNCTION WITH: **Sec. 100.1 Definitions** (Please refer to Chart a.2, *supra*).

[26] Australian *Criminal Code Act 1995*: http://www.comlaw.gov.au/Details/C2011C00123

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Providing or receiving training connected with terrorist acts*"	**Sec. 101.2 Providing or receiving training connected with terrorist acts** (1) A person commits an offence if: (a) the person provides or receives training; and (b) the training is connected with preparation for, the engagement of a person in, or assistance in a terrorist act; and (c) the person mentioned in paragraph (a) knows of the connection described in paragraph (b). Penalty: Imprisonment for 25 years. (2) A person commits an offence if: (a) the person provides or receives training; and (b) the training is connected with preparation for, the engagement of a person in, or assistance in a terrorist act; and (c) the person mentioned in paragraph (a) is reckless as to the existence of the connection described in paragraph (b). Penalty: Imprisonment for 15 years. (3) A person commits an offence under this section even if: (a) a terrorist act does not occur; or (b) the training is not connected with preparation for, the engagement of a person in, or assistance in a specific terrorist act; or (c) the training is connected with preparation for, the engagement of a person in, or assistance in more than one terrorist act. (4) Section 15.4 (extended geographical jurisdiction—category D) applies to an offence against this section. (5) If, in a prosecution for an offence (the prosecuted offence) against a subsection of this section, the trier of fact is not satisfied that the defendant is guilty of the offence, but is satisfied beyond reasonable doubt that the defendant is guilty of an offence (the alternative offence) against another subsection of this section, the trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.
"*Possessing things connected with terrorist acts*"	**Sec. 101.4 Possessing things connected with terrorist acts** (1) A person commits an offence if: (a) the person possesses a thing; and (b) the thing is connected with preparation for, the engagement of a person in, or assistance in a terrorist act; and (c) the person mentioned in paragraph (a) knows of the connection described in paragraph (b). Penalty: Imprisonment for 15 years. (2) A person commits an offence if: (a) the person possesses a thing; and (b) the thing is connected with preparation for, the engagement of a person in, or assistance in a terrorist act; and (c) the person mentioned in paragraph (a) is reckless as to the existence of the connection described in paragraph (b). Penalty: Imprisonment for 10 years. (3) A person commits an offence under subsection (1) or (2) even if: (a) a terrorist act does not occur; or (b) the thing is not connected with preparation for, the engagement of a person in, or assistance in a specific terrorist act; or (c) the thing is connected with preparation for, the engagement of a person in, or assistance in more than one terrorist act. (4) Section 15.4 (extended geographical jurisdiction—category D) applies to an offence against this section. (5) Subsections (1) and (2) do not apply if the possession of the thing was not intended to facilitate preparation for, the engagement of a person in, or assistance in a terrorist act. Note: A defendant bears an evidential burden in relation to the matter in subsection (5) (see subsection 13.3(3)). (6) If, in a prosecution for an offence (the prosecuted offence) against a subsection of this section, the trier of fact is not satisfied that the defendant is guilty of the offence, but is satisfied beyond reasonable doubt that the defendant is guilty of an offence (the alternative offence) against another subsection of this section, the trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.
"*Collecting or making documents likely to facilitate terrorist acts*"	**Sec. 101.5 Collecting or making documents likely to facilitate terrorist acts** (1) A person commits an offence if: (a) the person collects or makes a document; and (b) the document is connected with preparation for, the engagement of a person in, or assistance in a terrorist act; and (c) the person mentioned in paragraph (a) knows of the connection described in paragraph (b). Penalty: Imprisonment for 15 years. (2) A person commits an offence if: (a) the person collects or makes a document; and (b) the document is connected with preparation for, the engagement of a person in, or assistance in a terrorist act; and

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(c) the person mentioned in paragraph (a) is reckless as to the existence of the connection described in paragraph (b). Penalty: Imprisonment for 10 years. (3) A person commits an offence under subsection (1) or (2) even if: (a) a terrorist act does not occur; or (b) the document is not connected with preparation for, the engagement of a person in, or assistance in a specific terrorist act; or (c) the document is connected with preparation for, the engagement of a person in, or assistance in more than one terrorist act. (4) Section 15.4 (extended geographical jurisdiction—category D) applies to an offence against this section. (5) Subsections (1) and (2) do not apply if the collection or making of the document was not intended to facilitate preparation for, the engagement of a person in, or assistance in a terrorist act. Note: A defendant bears an evidential burden in relation to the matter in subsection (5) (see subsection 13.3(3)). (6) If, in a prosecution for an offence (the prosecuted offence) against a subsection of this section, the trier of fact is not satisfied that the defendant is guilty of the offence, but is satisfied beyond reasonable doubt that the defendant is guilty of an offence (the alternative offence) against another subsection of this section, the trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.
"*Other acts done in preparation for, or planning, terrorist acts*"	**Sec. 101.6 Other acts done in preparation for, or planning, terrorist acts** (1) A person commits an offence if the person does any act in preparation for, or planning, a terrorist act. Penalty: Imprisonment for life. (2) A person commits an offence under subsection (1) even if: (a) a terrorist act does not occur; or (b) the person's act is not done in preparation for, or planning, a specific terrorist act; or (c) the person's act is done in preparation for, or planning, more than one terrorist act. (3) Section 15.4 (extended geographical jurisdiction—category D) applies to an offence against subsection (1).
"*Directing a terrorist organization*"	**Sec. 102.2 Directing the activities of a terrorist organisation** (1) A person commits an offence if: (a) the person intentionally directs the activities of an organisation; and (b) the organisation is a terrorist organisation; and (c) the person knows the organisation is a terrorist organisation. Penalty: Imprisonment for 25 years. (2) A person commits an offence if: (a) the person intentionally directs the activities of an organisation; and (b) the organisation is a terrorist organisation; and (c) the person is reckless as to whether the organisation is a terrorist organisation. Penalty: Imprisonment for 15 years.
"*Membership in a terrorist organization*"	**Sec. 102.3 Membership of a terrorist organisation** (1) A person commits an offence if: (a) the person intentionally is a member of an organisation; and (b) the organisation is a terrorist organisation; and (c) the person knows the organisation is a terrorist organisation. Penalty: Imprisonment for 10 years. (2) Subsection (1) does not apply if the person proves that he or she took all reasonable steps to cease to be a member of the organisation as soon as practicable after the person knew that the organisation was a terrorist organisation. Note: A defendant bears a legal burden in relation to the matter in subsection (2) (see section 13.4).
"*Recruiting for a terrorist organization*"	**Sec. 102.4 Recruiting for a terrorist organisation** (1) A person commits an offence if: (a) the person intentionally recruits a person to join, or participate in the activities of, an organisation; and (b) the organisation is a terrorist organisation; and (c) the first-mentioned person knows the organisation is a terrorist organisation. Penalty: Imprisonment for 25 years. (2) A person commits an offence if:

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(a) the person intentionally recruits a person to join, or participate in the activities of, an organisation; and (b) the organisation is a terrorist organisation; and (c) the first-mentioned person is reckless as to whether the organisation is a terrorist organisation. Penalty: Imprisonment for 15 years.
"*Training a terrorist organization or receiving training from a terrorist organization*"	**Sec. 102.5 Training a terrorist organisation or receiving training from a terrorist organisation** (1) A person commits an offence if: (a) the person intentionally provides training to, or intentionally receives training from, an organisation; and (b) the organisation is a terrorist organisation; and (c) the person is reckless as to whether the organisation is a terrorist organisation. Penalty: Imprisonment for 25 years. (2) A person commits an offence if: (a) the person intentionally provides training to, or intentionally receives training from, an organisation; and (b) the organisation is a terrorist organisation that is covered by paragraph (b) of the definition of terrorist organisation in subsection 102.1(1). Penalty: Imprisonment for 25 years. (3) Subject to subsection (4), strict liability applies to paragraph (2)(b). (4) Subsection (2) does not apply unless the person is reckless as to the circumstance mentioned in paragraph (2)(b). Note: A defendant bears an evidential burden in relation to the matter in subsection (4) (see subsection 13.3(3)).
"*Getting funds to, from or for a terrorist organization*"	**Sec. 102.6 Getting funds to, from or for a terrorist organisation** (1) A person commits an offence if: (a) the person intentionally: (i) receives funds from, or makes funds available to, an organisation (whether directly or indirectly); or (ii) collects funds for, or on behalf of, an organisation (whether directly or indirectly); and (b) the organisation is a terrorist organisation; and (c) the person knows the organisation is a terrorist organisation. Penalty: Imprisonment for 25 years. (2) A person commits an offence if: (a) the person intentionally: (i) receives funds from, or makes funds available to, an organisation (whether directly or indirectly); or (ii) collects funds for, or on behalf of, an organisation (whether directly or indirectly); and (b) the organisation is a terrorist organisation; and (c) the person is reckless as to whether the organisation is a terrorist organisation. Penalty: Imprisonment for 15 years. (3) Subsections (1) and (2) do not apply to the person's receipt of funds from the organisation if the person proves that he or she received the funds solely for the purpose of the provision of: (a) legal representation for a person in proceedings relating to this Division; or (b) assistance to the organisation for it to comply with a law of the Commonwealth or a State or Territory. Note: A defendant bears a legal burden in relation to the matter in subsection (3) (see section 13.4).
"*Providing support to a terrorist organization*"	**Sec. 102.7 Providing support to a terrorist organisation** (1) A person commits an offence if: (a) the person intentionally provides to an organisation support or resources that would help the organisation engage in an activity described in paragraph (a) of the definition of terrorist organisation in this Division; and (b) the organisation is a terrorist organisation; and (c) the person knows the organisation is a terrorist organisation. Penalty: Imprisonment for 25 years. (2) A person commits an offence if: (a) the person intentionally provides to an organisation support or resources that would help the organisation engage in an activity described in paragraph (a) of the definition of terrorist organisation in this Division; and (b) the organisation is a terrorist organisation; and (c) the person is reckless as to whether the organisation is a terrorist organisation.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Associating with terrorist organizations*"	Penalty: Imprisonment for 15 years. **Sec. 102.8 Associating with terrorist organisations** (1) A person commits an offence if: (a) on 2 or more occasions: (i) the person intentionally associates with another person who is a member of, or a person who promotes or directs the activities of, an organisation; and (ii) the person knows that the organisation is a terrorist organisation; and (iii) the association provides support to the organisation; and (iv) the person intends that the support assist the organisation to expand or to continue to exist; and (v) the person knows that the other person is a member of, or a person who promotes or directs the activities of, the organisation; and (b) the organisation is a terrorist organisation because of paragraph (b) of the definition of terrorist organisation in this Division (whether or not the organisation is a terrorist organisation because of paragraph (a) of that definition also). Penalty: Imprisonment for 3 years. (2) A person commits an offence if: (a) the person has previously been convicted of an offence against subsection (1); and (b) the person intentionally associates with another person who is a member of, or a person who promotes or directs the activities of, an organisation; and (c) the person knows that the organisation is a terrorist organisation; and (d) the association provides support to the organisation; and (e) the person intends that the support assist the organisation to expand or to continue to exist; and (f) the person knows that the other person is a member of, or a person who promotes or directs the activities of, the organisation; and (g) the organisation is a terrorist organisation because of paragraph (b) of the definition of terrorist organisation in this Division (whether or not the organisation is a terrorist organisation because of paragraph (a) of that definition also). Penalty: Imprisonment for 3 years. (3) Strict liability applies to paragraphs (1)(b) and (2)(g). (4) This section does not apply if: (a) the association is with a close family member and relates only to a matter that could reasonably be regarded (taking into account the person's cultural background) as a matter of family or domestic concern; or (b) the association is in a place being used for public religious worship and takes place in the course of practising a religion; or (c) the association is only for the purpose of providing aid of a humanitarian nature; or (d) the association is only for the purpose of providing legal advice or legal representation in connection with: (i) criminal proceedings or proceedings related to criminal proceedings (including possible criminal proceedings in the future); or (ii) proceedings relating to whether the organisation in question is a terrorist organisation; or (iii) a decision made or proposed to be made under Division 3 of Part III of the Australian Security Intelligence Organisation Act 1979, or proceedings relating to such a decision or proposed decision; or (iv) a listing or proposed listing under section 15 of the Charter of the United Nations Act 1945 or an application or proposed application to revoke such a listing, or proceedings relating to such a listing or application or proposed listing or application; or (v) proceedings conducted by a military commission of the United States of America established under a Military Order of 13 November 2001 made by the President of the United States of America and entitled "Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism"; or (vi) proceedings for a review of a decision relating to a passport or other travel document or to a failure to issue such a passport or other travel document (including a passport or other travel document that was, or would have been, issued by or on behalf of the government of a foreign country). Note: A defendant bears an evidential burden in relation to the matters in subsection (4). See subsection 13.3(3). (5) This section does not apply unless the person is reckless as to the circumstance mentioned in paragraph (1)(b) and (2)(g) (as the case requires). Note: A defendant bears an evidential burden in relation to the matter in subsection (5). See subsection 13.3(3). (6) This section does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication. Note: A defendant bears an evidential burden in relation to the matter in subsection (6). See subsection 13.3(3). (7) A person who is convicted of an offence under subsection (1) in relation to the person's conduct on 2 or more occasions is not liable to be punished for an offence under subsection (1) for other conduct of the person that takes place: (a) at the same time as that conduct; or (b) within 7 days before or after any of those occasions.
"*Financing terrorism*"	**Sec. 103.1 Financing terrorism**

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Financing a terrorist*"	(1) A person commits an offence if: (a) the person provides or collects funds; and (b) the person is reckless as to whether the funds will be used to facilitate or engage in a terrorist act. Penalty: Imprisonment for life. Note: Intention is the fault element for the conduct described in paragraph (1)(a). See subsection 5.6(1). (2) A person commits an offence under subsection (1) even if: (a) a terrorist act does not occur; or (b) the funds will not be used to facilitate or engage in a specific terrorist act; or (c) the funds will be used to facilitate or engage in more than one terrorist act. **Sec. 103.2 Financing a terrorist** (1) A person commits an offence if: (a) the person intentionally: (i) makes funds available to another person (whether directly or indirectly); or (ii) collects funds for, or on behalf of, another person (whether directly or indirectly); and (b) the first-mentioned person is reckless as to whether the other person will use the funds to facilitate or engage in a terrorist act. Penalty: Imprisonment for life. (2) A person commits an offence under subsection (1) even if: (a) a terrorist act does not occur; or (b) the funds will not be used to facilitate or engage in a specific terrorist act; or (c) the funds will be used to facilitate or engage in more than one terrorist act.
New Zealand "*Terrorist act*"	***Terrorism Suppression Act 2002***[27]**:** SECTIONS 4(1), 5 AND 6 ARE TO BE READ TOGETHER: **Sec. 4 Interpretation** (1) In this Act, unless the context otherwise requires,— […] *specified terrorism convention* means any treaty specified in Schedule 3[28] […] *terrorist act in armed conflict* means an act— (a) that occurs in a situation of armed conflict; and (b) the purpose of which, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or abstain from doing any act; and (c) that is intended to cause death or serious bodily injury to a civilian or other person not taking an active part in the hostilities in that situation; and (d) that is not excluded from the application of the Financing Convention by article 3 of that Convention […] **Sec. 5 Terrorist act defined** (1) An act is a terrorist act for the purposes of this Act if— (a) the act falls within subsection (2); or (b) the act is an act against a specified terrorism convention (as defined in section 4(1)); or (c) the act is a terrorist act in armed conflict (as defined in section 4(1)). (2) An act falls within this subsection if it is intended to cause, in any 1 or more countries, 1 or more of the outcomes specified in subsection (3), and is carried out for the purpose of advancing an ideological, political, or religious cause, and with the following intention: (a) to induce terror in a civilian population; or (b) to unduly compel or to force a government or an international organisation to do or abstain from doing any act. (3) The outcomes referred to in subsection (2) are—

[27] NZ *Terrorism Suppression Act 2002*: http://www.legislation.govt.nz/act/public/2002/0034/latest/whole.html#dlm151491
[28] NZ *Terrorism Suppression Act 2002*, Schedule 3: http://www.legislation.govt.nz/act/public/2002/0034/latest/DLM154155.html

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Terrorist bombing*"	(a) the death of, or other serious bodily injury to, 1 or more persons (other than a person carrying out the act): (b) a serious risk to the health or safety of a population: (c) destruction of, or serious damage to, property of great value or importance, or major economic loss, or major environmental damage, if likely to result in 1 or more outcomes specified in paragraphs (a), (b), and (d): (d) serious interference with, or serious disruption to, an infrastructure facility, if likely to endanger human life: (e) introduction or release of a disease-bearing organism, if likely to devastate the national economy of a country. (4) However, an act does not fall within subsection (2) if it occurs in a situation of armed conflict and is, at the time and in the place that it occurs, in accordance with rules of international law applicable to the conflict. (5) To avoid doubt, the fact that a person engages in any protest, advocacy, or dissent, or engages in any strike, lockout, or other industrial action, is not, by itself, a sufficient basis for inferring that the person— (a) is carrying out an act for a purpose, or with an intention, specified in subsection (2); or (b) intends to cause an outcome specified in subsection (3). **Sec. 6A Terrorist act** (1) A person commits an offence who engages in a terrorist act. (2) A person who commits a terrorist act is liable on conviction on indictment to imprisonment for life or a lesser term. **Sec. 7 Terrorist bombing** (1) A person commits an offence who, intentionally and without lawful justification or excuse, delivers, places, discharges, or detonates an explosive or other lethal device in, into, or against a relevant place, facility, or system, with the intent to cause— (a) death or serious bodily injury; or (b) extensive destruction— (i) of the relevant place, facility, or system; and (ii) that results, or is likely to result, in major economic loss. (2) In subsection (1), relevant place, facility, or system means— (a) a place of public use: (b) a State or government facility: (c) a public transportation system: (d) an infrastructure facility. (3) A person who commits terrorist bombing is liable on conviction on indictment to imprisonment for life or a lesser term.
"*Financing of terrorism*"	**Sec. 8 Financing of terrorism** (1) A person commits an offence who, directly or indirectly, wilfully and without lawful justification or reasonable excuse, provides or collects funds intending that they be used, or knowing that they are to be used, in full or in part, in order to carry out 1 or more acts of a kind that, if they were carried out, would be 1 or more terrorist acts. (2) [Repealed] (2A) A person commits an offence who, directly or indirectly, wilfully and without lawful justification or reasonable excuse, provides or collects funds intending that they benefit, or knowing that they will benefit, an entity that the person knows is an entity that carries out, or participates in the carrying out of, 1 or more terrorist acts. (3) In a prosecution for financing of terrorism, it is not necessary for the prosecutor to prove that the funds collected or provided were actually used, in full or in part, to carry out a terrorist act. (4) A person who commits financing of terrorism is liable on conviction on indictment to imprisonment for a term not exceeding 14 years.
"*Dealing with property*"	**Sec. 9 Prohibition on dealing with property of, or derived or generated from property of, designated terrorist entity** (1) A person commits an offence who, without lawful justification or reasonable excuse, deals with any property knowing that the property is— (a) property owned or controlled, directly or indirectly, by a designated terrorist entity; or (b) property derived or generated from any property of the kind specified in paragraph (a). (2) For the purposes of subsection (1), examples of a reasonable excuse for dealing with property referred to in those provisions are— (a) where the dealing with the property comprises an act that does no more than satisfy essential human needs of (or of a dependant of) an individual designated under this Act: (b) where a financial institution acts to freeze assets of a designated terrorist entity. (3) Subsection (1) does not apply—

[29] NZ *Crimes Act 1961*: http://www.legislation.govt.nz/act/public/1961/0043/latest/whole.html?search=ts_act_crimes+act_resel&p=1#dlm327382

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Making property, or financial or related services, available to designated terrorist entity*"	(a) if the Prime Minister has, under section 11, authorised the dealing with the property; or (b) if the property concerned is the subject of a direction under section 48 and the dealing concerned forms part of the exercise by the Official Assignee of his or her powers under section 80 of the Criminal Proceeds (Recovery) Act 2009 (as modified and applied by section 51(a)). (4) A person who commits an offence against subsection (1) is liable on conviction on indictment to imprisonment for a term not exceeding 7 years. (5) [Repealed] (6) A reference in the definition of deal with in section 4 to the transfer of property that is a security includes a reference to a transfer of the security by way of loan, mortgage, pledge, or bailment, whether in respect of a legal or an equitable interest. **Sec. 10 Prohibition on making property, or financial or related services, available to designated terrorist entity** (1) A person commits an offence who makes available, or causes to be made available, directly or indirectly, without lawful justification or reasonable excuse, any property, or any financial or related services, either to, or for the benefit of, an entity, knowing that the entity is a designated terrorist entity. (2) [Repealed] (3) An example of making property available with a reasonable excuse, for the purposes of subsection (1), is where the property (for example, items of food, clothing, or medicine) is made available in an act that does no more than satisfy essential human needs of (or of a dependant of) an individual designated under this Act. (4) Subsection (1) does not apply if the Prime Minister has, under section 11, authorised the making available of the property or services. (5) A person who commits an offence against subsection (1) is liable on conviction on indictment to imprisonment for a term not exceeding 7 years. (6) In this section, make available, in relation to any property or services, means to make the property or services available in any way and by any means (for example, to send, transfer, deliver, or provide the property or services). (7) A reference in subsection (6) to the transfer of property that is a security includes a reference to a transfer of the security by way of loan, mortgage, pledge, or bailment, whether in respect of a legal or an equitable interest. SECTIONS 9(1) AND 10(1) ARE TO BE READ IN CONJUNCTION WITH: **Sec.11 Authorisations by Prime Minister** (1) The Prime Minister may, by notice in writing, permit any activity or transaction or class or classes of activities or transactions that would otherwise be prohibited by section 9(1) or section 10(1). (2) Any authorisation of that kind— (a) may be subject to terms or conditions; and (b) may be amended, revoked, or revoked and replaced. (3) If a person has obtained an authorisation of that kind, another person involved in carrying out the activity or transaction or class or classes of activities or transactions to which the authorisation relates is not subject to section 9(1) or section 10(1). (4) However, subsection (3) does not apply if— (a) the authorisation is subject to terms or conditions imposed under subsection (2)(a); and (b) those terms or conditions are not satisfied.
"*Recruiting members of terrorist groups*"	**Sec.12 Recruiting members of terrorist groups** (1) A person commits an offence who recruits another person as a member of a group or organisation, knowing that the group or organisation is— (a) a designated terrorist entity; or (b) an entity that carries out, or participates in the carrying out of, 1 or more terrorist acts. (2) A person who commits an offence against subsection (1) is liable on conviction on indictment to imprisonment for a term not exceeding 14 years.
"*Participating in terrorist groups*"	**Sec.13 Participating in terrorist groups** (1) A person commits an offence who participates in a group or organisation for the purpose stated in subsection (2), knowing that or being reckless as to whether the group or organisation is— (a) a designated terrorist entity; or (b) an entity that carries out, or participates in the carrying out of, 1 or more terrorist acts. (2) The purpose referred to in subsection (1) is to enhance the ability of any entity (being an entity of the kind referred to in subsection (1)(a) or (b)) to carry out, or to participate in the carrying out of, 1 or more terrorist acts. (3) A person who commits an offence against subsection (1) is liable on conviction on indictment to imprisonment for a term not exceeding 14 years.
"*Harbouring or concealing terrorists*"	**Sec.13A Harbouring or concealing terrorists** (1) A person commits an offence who, with the intention of assisting another person to avoid arrest, escape lawful custody, or avoid conviction, harbours or conceals that person,— (a) knowing, or being reckless as to whether, that person intends to carry out a terrorist act; or

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(b) knowing, or being reckless as to whether, that person has carried out a terrorist act. (2) A person who commits an offence against subsection (1) is liable on conviction on indictment to a term of imprisonment not exceeding 7 years.
"*Use and movement of unmarked plastic explosives*"	**Sec. 13B Offences involving use and movement of unmarked plastic explosives** (1) A person commits an offence and is liable on conviction on indictment to a term of imprisonment not exceeding 10 years or a fine not exceeding $500,000, or both, who— (a) possesses, uses, or manufactures unmarked plastic explosives, knowing they are unmarked; or (b) imports or exports unmarked plastic explosives to or from New Zealand, knowing they are unmarked. (2) Subsection (1) does not apply in respect of unmarked plastic explosives (not being explosives to which subsection (3) applies) that were lawfully manufactured in, or imported into New Zealand before the commencement of this section and that may, subject to the Hazardous Substances and New Organisms Act 1996, be transported or possessed by— (a) a person who performs military or Police functions during the period that begins with the entry into force of this section and ends 15 years later; or (b) any other person during the period that begins with the entry into force of this section and ends 3 years later. (3) Nothing in this section applies to unmarked plastic explosives— (a) that are manufactured or held in limited quantities for sole use in any of the following activities that are duly approved by the Environmental Risk Management Authority: (i) research, development, or testing of new or modified explosives; or (ii) training in explosives detection or testing of explosives detection equipment; or (iii) forensic science activities; or (b) that are destined to be, and are incorporated as, an integral part of a duly authorised military device in New Zealand within 3 years after the date on which this section comes into force.
"*Offences involving nuclear material*"	**Sec.13C Offences involving physical protection of nuclear material** (1) A person commits an offence who,— (a) without lawful authority, receives, possesses, uses, transfers, alters, disposes of, or disperses nuclear material, knowing it is nuclear material, and— (i) that causes death, injury, or disease to any person or substantial damage to property; or (ii) with intent to cause, or being reckless as to whether it causes death, injury, or disease to any person or substantial damage to property; or (iii) that causes, or is likely to cause, substantial damage to the environment; or (b) commits theft, as defined in section 219 of the Crimes Act 1961, of nuclear material knowing that it was nuclear material; or (c) fraudulently obtains nuclear material, knowing that it was nuclear material; or (d) makes a demand for nuclear material by threat, or by use of force, or by any other form of intimidation with intent to steal it; or (e) with intent to intimidate, threatens to use nuclear material to cause— (i) death, injury, or disease to any person; or (ii) substantial damage to any property or to the environment; or (f) with intent to compel any person, international organisation, or State to do, or refrain from doing, any act, threatens to steal nuclear material; or (g) without lawful authority, commits an act, or threatens to commit an act against a nuclear facility, or interferes with the operation of a nuclear facility with intent to cause, or being reckless as to whether it causes, death or serious injury to any person or substantial damage to property or to the environment by exposure to radiation or release of radioactive substances. (2) A person who commits an offence against subsection (1) is liable on conviction on indictment to imprisonment for a term not exceeding 10 years, or a fine not exceeding $500,000, or both.
"*Offence involving radioactive material (importation, acquisition, etc.)*"	**Sec. 13D Importation, acquisition, etc, of radioactive material** A person commits an offence and is liable on conviction on indictment to a term of imprisonment not exceeding 10 years who imports, acquires, possesses, or has control over any radioactive material with intent to use it to commit an offence involving bodily injury, or the threat of violence, to any person.
"*Offences involving radioactive material and devices*"	**Sec. 13E Offences involving radioactive material and radioactive devices** (1) A person commits an offence who— (a) makes or possesses a radioactive device or possesses radioactive material with intent to cause death or serious injury to any person or substantial damage to property or to the environment; or (b) uses radioactive material or a radioactive device or uses or damages a nuclear facility in a manner that releases or risks the release of radioactive material— (i) with intent to cause death or serious injury to any person or substantial damage to property or to the environment; or (ii) with intent to compel any person, international organisation, or State to do, or refrain from doing an act; or (c) threatens to commit an offence set out in paragraph (b); or (d) unlawfully and intentionally demands radioactive material by threat, in circumstances that indicate the credibility of the threat; or (e) by use of force,— (i) uses or threatens to use radioactive material or a radioactive device; or (ii) uses or damages or threatens to use or damage a nuclear facility.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Offences also applying outside New Zealand*"	(2) A person who commits an offence against subsection (1) is liable on conviction on indictment to imprisonment for a term not exceeding 10 years, or a fine not exceeding $500,000, or both. **Sec. 14 Offences also apply in certain cases outside New Zealand** (1) Each of sections 7 to 13 and 13B to 13E applies in respect of acts that occurred wholly outside New Zealand, as provided in sections 15 to 18. (2) Subsection (1) does not affect the application of sections 7 to 13 in respect of— (a) acts that occurred wholly within New Zealand; or (b) an offence that, under section 7 of the Crimes Act 1961, is deemed to be committed in New Zealand; or (c) acts that, under section 8A of that Act, are deemed to have taken place within New Zealand. **Sec. 15 Offences apply to acts outside New Zealand by New Zealand citizens or on New Zealand aircraft and ships** Proceedings may be brought in a New Zealand court for any offence against this Act (other than one against section 43 or section 47 or section 47G) if the acts alleged to constitute the offence occurred wholly outside New Zealand, but were done— (a) by a New Zealand citizen: (b) by a person who is ordinarily resident in New Zealand but is not a citizen of any State: (c) by any other person on board any aircraft— (i) registered or required to be registered in New Zealand under the Civil Aviation Act 1990; or (ii) for the time being used as an aircraft of the New Zealand Defence Force: (d) by any other person on board any ship— (i) registered under the Ship Registration Act 1992; or (ii) not registered under that Act but required to be registered under that Act; or (iii) for the time being used as a ship of the New Zealand Defence Force. **Sec. 16 Further acts outside New Zealand to which terrorist bombing applies** Proceedings may also be brought in a New Zealand court for terrorist bombing if the acts alleged to constitute the offence occurred wholly outside New Zealand, but were done— (a) against a New Zealand citizen; or (b) against a State or government facility of New Zealand abroad (for example, a New Zealand embassy, or other New Zealand diplomatic or consular premises); or (c) in an attempt to compel the Government of New Zealand to do or abstain from doing any act. **Sec. 17 Further acts outside New Zealand to which financing of terrorism applies** Proceedings may also be brought in a New Zealand court for financing of terrorism if the acts alleged to constitute the offence occurred wholly outside New Zealand, but were directed towards, or resulted in, 1 or more terrorist acts being done— (a) within New Zealand; or (b) against a New Zealand citizen; or (c) against a State or government facility of New Zealand abroad (for example, New Zealand diplomatic or consular premises); or (d) in an attempt to compel the Government of New Zealand to do or abstain from doing any act. **Sec. 18 Offences also apply to acts outside New Zealand if alleged offender is in New Zealand and is not extradited** Even if the acts alleged to constitute the offence occurred wholly outside New Zealand, proceedings may be brought for terrorist bombing, financing of terrorism, a nuclear terrorism offence, or a nuclear material offence if the person to be charged has been found in New Zealand and has not been extradited.
"*Causing disease or sickness in animals*"	***Crimes Act 1961***[29]**:** **Sec. 4 298A Causing disease or sickness in animals** (1) Every one is liable to imprisonment for a term not exceeding 10 years who, without lawful justification or reasonable excuse, directly or indirectly causes or produces in an animal a disease or sickness that causes a situation of a kind described in subsection (2) to occur, either— (a) intending a situation of that kind to occur; or (b) being reckless as to whether a situation of that kind occurs. (2) A situation of a kind referred to in subsection (1) is a situation that— (a) constitutes a serious risk to the health or safety of an animal population; and (b) is likely, directly or indirectly, to cause major damage to the national economy of New Zealand.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Contaminating food, crops, water, or other products*"	**Sec. 298B Contaminating food, crops, water, or other products** Every one is liable to imprisonment for a term not exceeding 10 years who contaminates food, crops, water, or any other products, without lawful justification or reasonable excuse, and either knowing or being reckless as to whether the food, crops, water, or products are intended for human consumption, and— (a) intending to harm a person or reckless as to whether any person is harmed; or (b) intending to cause major economic loss to a person or reckless as to whether major economic loss is caused to any person; or (c) intending to cause major damage to the national economy of New Zealand or reckless as to whether major damage is caused to the national economy of New Zealand.
"*Threats of harm to people or property*"	**Sec. 307A Threats of harm to people or property** (1) Everyone is liable to imprisonment for a term not exceeding 7 years if, without lawful justification or reasonable excuse, and intending to achieve the effect stated in subsection (2), he or she— (a) threatens to do an act likely to have one or more of the results described in subsection (3); or (b) communicates information— (i) that purports to be about an act likely to have one or more of the results described in subsection (3); and (ii) that he or she believes to be false. (2) The effect is causing a significant disruption of one or more of the following things: (a) the activities of the civilian population of New Zealand: (b) something that is or forms part of an infrastructure facility in New Zealand: (c) civil administration in New Zealand (whether administration undertaken by the Government of New Zealand or by institutions such as local authorities, District Health Boards, or boards of trustees of schools): (d) commercial activity in New Zealand (whether commercial activity in general or commercial activity of a particular kind). (3) The results are— (a) creating a risk to the health of one or more people: (b) causing major property damage: (c) causing major economic loss to one or more persons: (d) causing major damage to the national economy of New Zealand. (4) To avoid doubt, the fact that a person engages in any protest, advocacy, or dissent, or engages in any strike, lockout, or other industrial action, is not, by itself, a sufficient basis for inferring that a person has committed an offence against subsection (1).
"*Terrorist offence*"	**Section 3124 Interpretation** (1) In this Part, unless the context otherwise requires,— […] *terrorist offence* means an offence against any of sections 7, 8, 9, 10, 12, 13, and 13A of the Terrorism Suppression Act 2002. […]
France "*Acts of terrorism*" 1° Deliberate attacks upon life, deliberate attacks on integrity of the person, abduction, holding of persons against their will, highjacking of an aircraft, ship or other means of transport; 2° Theft, extortion, destruction of and	ACCORDING TO THE ***CODE PÉNAL*** **(FRENCH PENAL CODE)**[30], THE OFFENCES LISTED BELOW ARE INDICTABLE WHEN CONNECTED WITH AN INDIVIDUAL OR COLLECTIVE OPERATION AIMED AT SERIOUSLY DISTURBING PUBLIC ORDER BY INTIMIDATION OR TERROR: **Art. 421-1** Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes : 1° Les atteintes volontaires à la vie, les atteintes volontaires à l'intégrité de la personne, l'enlèvement et la séquestration ainsi que le détournement d'aéronef, de navire ou de tout autre moyen de transport, définis par le livre II du présent code[31] ; 2° Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le livre III du présent code[32] ; 3° Les infractions en matière de groupes de combat et de mouvements dissous définies par les articles 431-13 à 431-17 et les infractions définies par les articles 434-6 et 441-2 à 441-5 [please see below] ;

[30] *Code pénal français* (French Penal Code): http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719&dateTexte=20110416 (in French).
[31] For Section II (Terrorism) of the French Penal Code, please refer to: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (in French).
[32] For Section III (Computer offences) in the French Penal Code, please refer to:
http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006418127&idSectionTA=LEGISCTA000006165324&cidTexte=LEGITEXT000006070719&dateTexte=20110416 (in French).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

damage to property, computer offences (as defined in Section III of the French Penal Code); 3° Offences involving prohibited combat groups and movements; 4° Offences involving firearms, explosives or nuclear substances; 5° Handling the proceeds of one of the above offences; 6° Money laundering (as defined in Chapter IV, Title II, Section III of the French Penal Code); 7° Insider offences. "*Offences involving prohibited combat groups and movements*"	4° Les infractions en matière d'armes, de produits explosifs ou de matières nucléaires définies par le I de l'article L. 1333-9, les articles L. 1333-11 et L. 1333-13-2, le II des articles L. 1333-13-3 et L. 1333-13-4, les articles L. 1333-13-6, L. 2339-2, L. 2339-5, L. 2339-8 et L. 2339-9 à l'exception des armes de la 6e catégorie, L. 2339-14, L. 2339-16, L. 2341-1, L. 2341-4, L. 2341-5, L. 2342-57 à L. 2342-62, L. 2353-4, le 1° de l'article L. 2353-5 et l' article L. 2353-13 du code de la défense [please see below] ; 5° Le recel du produit de l'une des infractions prévues aux 1° à 4° ci-dessus ; 6° Les infractions de blanchiment prévues au chapitre IV du titre II du livre III du présent code[33] ; 7° Les délits d'initié prévus à l'article L. 465-1 du code monétaire et financier [please see below]. ARTICLE 421-1 OF THE *CODE PÉNAL* (FRENCH PENAL CODE) REFERS TO: ***Code pénal* (French Penal Code)[34]:** **Art. 431-13** Constitue un groupe de combat, en dehors des cas prévus par la loi, tout groupement de personnes détenant ou ayant accès à des armes, doté d'une organisation hiérarchisée et susceptible de troubler l'ordre public. **Art. 431-14** Le fait de participer à un groupe de combat est puni de trois ans d'emprisonnement et de 45000 euros d'amende. **Art. 431-15** Le fait de participer au maintien ou à la reconstitution, ouverte ou déguisée, d'une association ou d'un groupement dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées est puni de trois ans d'emprisonnement et de 45000 euros d'amende. Lorsque l'association ou le groupement maintenu ou reconstitué est un groupe de combat au sens de l'article 431-14, la peine est portée à cinq ans d'emprisonnement et à 75000 euros d'amende. **Art. 431-16** Le fait d'organiser un groupe de combat est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. **Art. 431-17** Le fait d'organiser le maintien ou la reconstitution, ouverte ou déguisée, d'un groupe de combat dissous en application de la loi du 10 janvier 1936 précitée est puni de sept ans d'emprisonnement et de 100000 euros d'amende.
"*Providing support to a terrorist*"	**Arti. 434-6** Le fait de fournir à la personne auteur ou complice d'un crime ou d'un acte de terrorisme puni d'au moins dix ans d'emprisonnement un logement, un lieu de retraite, des subsides, des moyens d'existence ou tout autre moyen de la soustraire aux recherches ou à l'arrestation est puni de trois ans d'emprisonnement et de 45000 euros d'amende. Les peines sont portées à cinq ans d'emprisonnement et à 75000 euros d'amende lorsque l'infraction est commise de manière habituelle. Sont exceptés des dispositions qui précèdent : 1° Les parents en ligne directe et leurs conjoints, ainsi que les frères et soeurs et leurs conjoints, de l'auteur ou complice du crime ou de l'acte de terrorisme ;

[33] For Chapter IV, Tile II, Section III (Money laundering) of the French Penal Code, please refer to: http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006418127&idSectionTA=LEGISCTA000006165324&cidTexte=LEGITEXT000006070719&dateTexte=20110416 (in French).
[34] *Code pénal français* (French Penal Code): http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719&dateTexte=20110416 (in French).
[35] *Code français de la defense* (French Defence Code): http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307&dateTexte=20080505 (in French).
[36] *Code français monétaire et financier* (French Monetary and Financial Code): http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026 (in French).
[37] *Code pénal français* (French Penal Code): http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719&dateTexte=20110416 (in French).
[38] *Loi française du 29 juillet 1881 sur la liberté de la presse* (French Act of 29 July 1881 on Freedom of the Press): http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722&dateTexte=20110427 (in French).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Offences related to the forgery of documents*"	2° Le conjoint de l'auteur ou du complice du crime ou de l'acte de terrorisme, ou la personne qui vit notoirement en situation maritale avec lui. **Art. 441-2** Le faux commis dans un document délivré par une administration publique aux fins de constater un droit, une identité ou une qualité ou d'accorder une autorisation est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. L'usage du faux mentionné à l'alinéa précédent est puni des mêmes peines. Les peines sont portées à sept ans d'emprisonnement et à 100000 euros d'amende lorsque le faux ou l'usage de faux est commis : 1° Soit par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public agissant dans l'exercice de ses fonctions ; 2° Soit de manière habituelle ; 3° Soit dans le dessein de faciliter la commission d'un crime ou de procurer l'impunité à son auteur. **Art. 441-3** La détention frauduleuse de l'un des faux documents définis à l'article 441-2 est punie de deux ans d'emprisonnement et de 30000 euros d'amende. La peine est portée à cinq ans d'emprisonnement et à 75000 euros d'amende en cas de détention frauduleuse de plusieurs faux documents. **Art. 441-4** Le faux commis dans une écriture publique ou authentique ou dans un enregistrement ordonné par l'autorité publique est puni de dix ans d'emprisonnement et de 150000 euros d'amende. L'usage du faux mentionné à l'alinéa qui précède est puni des mêmes peines. Les peines sont portées à quinze ans de réclusion criminelle et à 225000 euros d'amende lorsque le faux ou l'usage de faux est commis par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public agissant dans l'exercice de ses fonctions ou de sa mission. **Art. 441-5** Le fait de procurer frauduleusement à autrui un document délivré par une administration publique aux fins de constater un droit, une identité ou une qualité ou d'accorder une autorisation est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Les peines sont portées à sept ans d'emprisonnement et à 100000 euros d'amende lorsque l'infraction est commise : 1° Soit par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public agissant dans l'exercice de ses fonctions ; 2° Soit de manière habituelle ; 3° Soit dans le dessein de faciliter la commission d'un crime ou de procurer l'impunité à son auteur.
"*Offences involving firearms, explosives or nuclear substances*"	***Code de la défense* (French Defense Code)[35]:** **Art. L1333-9** I.- Est puni d'un emprisonnement de dix ans et d'une amende de 7 500 000 euros : 1° Le fait d'exercer sans autorisation les activités mentionnées à l'article L. 1333-2 ou de fournir des renseignements inexacts afin d'obtenir ladite autorisation ; 2° Le fait de s'approprier indûment les matières nucléaires mentionnées à l'article L. 1333-1 ; 3° Le fait d'abandonner ou de disperser les matières nucléaires mentionnées à l'article L. 1333-1 ; 4° Le fait d'altérer ou de détériorer les matières nucléaires mentionnées a l'article L. 1333-1 ; 5° Le fait de détruire des éléments de structure dans lesquels sont conditionnées les matières nucléaires mentionnées à l'article L. 1333-1. […] **Art. L1333-11** Pour l'application de la convention sur la protection physique des matières nucléaires, publiée par le décret n° 92-110 du 3 février 1992, est puni des peines prévues aux articles L. 1333-9 et L. 1333-10 le fait de détenir, transférer, utiliser ou transporter, hors du territoire de la République, les matières nucléaires entrant dans le champ d'application des articles 1er et 2 de la convention précitée, sans y avoir été autorisé par les autorités étrangères compétentes. **Art. L1333-13-2** Le fait de provoquer, d'encourager ou d'inciter quiconque, de quelque manière que ce soit, à commettre les infractions prévues au I de l'article L. 1333-9 et aux articles L. 1333-11 et L. 1333-13-1, lorsque ce fait a été suivi d'effet, est puni des peines prévues pour ces infractions. Lorsque les faits mentionnés au premier alinéa du présent article ne sont pas suivis d'effet en raison de circonstances indépendantes de la volonté de leur auteur, la peine est de trois ans d'emprisonnement et de 45 000 € d'amende.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

Art. L1333-13-3
I.- Les infractions définies aux articles L. 1333-12 et L. 1333-13-1 sont punies de dix ans d'emprisonnement et de 150 000 € d'amende lorsqu'elles sont commises en bande organisée.
II.- Les infractions définies aux articles L. 1333-9 et L. 1333-11 sont punies de quinze ans de réclusion criminelle et de 7,5 millions d'euros d'amende lorsqu'elles sont commises en bande organisée.
Art. L1333-13-4
I.- Les infractions définies à l'article L. 1333-13-1 sont punies de quinze ans de réclusion criminelle et de 7,5 millions d'euros d'amende lorsqu'elles sont en relation avec une entreprise individuelle ou collective ayant pour but de permettre à quiconque de se doter d'une arme nucléaire.
La peine est portée à vingt ans de réclusion criminelle et à 7,5 millions d'euros d'amende lorsque les infractions sont commises en bande organisée.
II.- Les infractions définies aux 1° et 2° du I de l'article L. 1333-9 et aux articles L. 1333-11, L. 1333-12 et L. 1333-13-2 sont punies de vingt ans de réclusion criminelle et de 7,5 millions d'euros d'amende lorsqu'elles sont en relation avec une entreprise individuelle ou collective ayant pour but de permettre à quiconque de se doter d'une arme nucléaire.
Ces faits sont punis de trente ans de réclusion criminelle et de 7,5 millions d'euros d'amende lorsqu'ils sont commis en bande organisée.
III.- Constitue une arme nucléaire, pour la poursuite des infractions mentionnées au présent article, tout engin explosif dont l'énergie a pour origine la fission de noyaux d'atomes.

Art. L1333-13-6
Le fait de provoquer, d'encourager ou d'inciter quiconque de quelque manière que ce soit à commettre les infractions prévues aux articles L. 1333-13-3 à L. 1333-13-5, lorsque ce fait a été suivi d'effet, est puni des peines prévues pour ces infractions.
Lorsque les faits mentionnés au premier alinéa du présent article ne sont pas suivis d'effet en raison de circonstances indépendantes de la volonté de leur auteur, la peine est de sept ans d'emprisonnement et de 100 000 € d'amende.

Art. L2339-2
I.- Est puni d'un emprisonnement de sept ans et d'une amende de 100 000 euros quiconque, sans y être régulièrement autorisé, se livre à la fabrication ou au commerce des matériels de guerre ou d'armes ou de munitions de défense de l'une des catégories mentionnées au I de l'article L. 2332-1, ou exerce son activité en qualité d'intermédiaire ou d'agent de publicité à l'occasion de la fabrication ou du commerce des matériels, armes ou munitions desdites catégories.
Les peines sont portées à dix ans d'emprisonnement et à 500 000 euros d'amende lorsque l'infraction est commise en bande organisée.
La confiscation du matériel fabriqué ou du matériel à vendre, ainsi que sa vente aux enchères publiques, est ordonnée par le même jugement.
L'autorité administrative peut prescrire ou faire effectuer la mise hors d'usage, aux frais du délinquant, du matériel avant sa mise aux enchères publiques.
II.- Les personnes morales peuvent être déclarées responsables pénalement de ces infractions dans les conditions prévues par l'article 121-2 du code pénal.
Les peines encourues par ces personnes morales sont :
1° L'amende, suivant les modalités prévues par l'article 131-38 du code pénal ;
2° Les peines mentionnées aux 1°, 2°, 4°, 5°, 8° et 9° de l'article 131-39 du code pénal.

Art. L2339-5
Sont punies d'un emprisonnement de trois ans et d'une amende de 3 750 euros l'acquisition, la cession ou la détention, sans l'autorisation prévue au I de l'article L. 2332-1, une ou plusieurs armes de la 1re ou de la 4e catégorie ou leurs munitions en violation des dispositions des articles L. 2336-1, L. 2337-3 ou L. 2337-4.
La peine d'emprisonnement est portée à cinq ans et l'interdiction de séjour peut être prononcée suivant les modalités prévues par l'article 131-31 du code pénal, si le coupable a été antérieurement condamné à l'emprisonnement ou à une peine plus grave pour crime ou délit.
Les peines sont portées à dix ans d'emprisonnement et à 500 000 euros d'amende lorsque l'infraction est commise en bande organisée.
Le tribunal ordonne, en outre, la confiscation des armes ou des munitions.

Art. L2339-8
La détention d'un dépôt d'armes ou de munitions de la 1re, 4e ou 6e catégorie est punie d'un emprisonnement de cinq ans et d'une amende de 3 750 euros.
Les peines sont portées à dix ans d'emprisonnement et à 500 000 euros d'amende lorsque l'infraction est commise en bande organisée.
La peine est portée à dix ans d'emprisonnement et la peine complémentaire d'interdiction de séjour peut être prononcée suivant les modalités prévues par l'article 131-31 du code pénal lorsque le coupable a antérieurement été condamné à l'emprisonnement ou à une peine plus grave pour crime ou délit.
Le tribunal ordonne, en outre, la confiscation des armes ou des munitions.
Ces dispositions ne sont pas applicables, dans la mesure où ils exercent leur industrie ou leur commerce, aux fabricants et aux vendeurs régulièrement autorisés.

Art. L2339-9
I.- Quiconque, hors de son domicile et sauf les exceptions résultant des dispositions des articles L. 2338-1 et L. 2338-2, est trouvé porteur ou effectue sans motif légitime le transport d'une ou plusieurs armes de 1re, 4e ou 6e catégorie, ou d'éléments constitutifs de ces armes des 1re et 4e catégories ou des munitions correspondantes, même s'il en est régulièrement détenteur, est puni:
1° S'il s'agit d'une arme de la 1re ou de la 4e catégorie ou d'éléments constitutifs de ces armes ou de munitions correspondantes, d'un emprisonnement de cinq ans et d'une amende de 3 750

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

euros ;
2° S'il s'agit d'une arme de la 6e catégorie, d'un emprisonnement de trois ans et d'une amende de 3 750 euros.
II.- L'emprisonnement peut être porté à dix ans dans les cas suivants :
1° Si l'auteur des faits a été antérieurement condamné pour crime ou délit à une peine égale ou supérieure à un an d'emprisonnement ferme ou à une peine plus grave ;
2° Si le transport d'armes est effectué par au moins deux personnes ;
3° Si deux personnes au moins sont trouvées ensemble porteuses d'armes.
III.- Dans tous les cas prévus au présent article, le tribunal ordonne la confiscation des armes.
IV.- La peine complémentaire de l'interdiction de séjour peut être prononcée suivant les modalités prévues par l'article 131-31 du code pénal.

Art. L2339-14
Les infractions définies au premier alinéa du I de l'article L. 2339-2, à l'article L. 2339-4, au premier alinéa des articles L. 2339-5 et L. 2339-8, au 1° du I de l'article L. 2339-9 et au premier alinéa de l'article L. 2339-10 sont punies de quinze ans de réclusion criminelle et un million et demi d'euros d'amende lorsqu'elles concernent des missiles, fusées ou autres systèmes sans pilote capables de conduire à leur cible des armes nucléaires telles que définies au III de l'article L. 1333-13-4, chimiques ou biologiques et spécialement conçus à cet usage.
Ces faits sont punis de vingt ans de réclusion criminelle et de trois millions d'euros d'amende lorsqu'ils sont commis en bande organisée.

Art. L2339-16
Le fait de se faire délivrer indûment, par quelque moyen frauduleux que ce soit, les autorisations ou agréments mentionnés au I de l'article L. 2332-1, aux articles L. 2335-1 à L. 2335-3, au 2° du I de l'article L. 2336-1 et à l'article L. 2337-4 est puni de dix ans d'emprisonnement et un million et demi d'euros d'amende lorsque ces autorisations ou agréments concernent des missiles, fusées ou autres systèmes sans pilote capables de conduire à leur cible des armes nucléaires telles que définies au III de l'article L. 1333-13-4, chimiques ou biologiques et spécialement conçus à cet usage.

Art. L2341-1
Sont interdits la mise au point, la fabrication, la détention, le stockage, l'acquisition et la cession des agents microbiologiques, des autres agents biologiques et des toxines biologiques, quels qu'en soient l'origine et le mode de production, des types et en quantité non destinés à des fins prophylactiques, de protection ou à d'autres fins pacifiques.

Art. L2341-4
Les infractions aux dispositions des articles L. 2341-1 et L. 2341-2 sont punies d'un emprisonnement de cinq ans et d'une amende de 75 000 euros ou de l'une de ces deux peines seulement. Les peines sont portées à dix ans d'emprisonnement et à 500 000 euros d'amende lorsque l'infraction est commise en bande organisée.
En cas de condamnation, le tribunal ordonne la confiscation, en vue de leur destruction, des agents ou toxines définis à l'article L. 2341-1.
Il peut en outre ordonner, conjointement ou non :
1° La fermeture totale ou partielle, à titre définitif ou pour une durée de cinq ans au plus, de l'établissement ayant permis de commettre l'infraction ;
2° La confiscation des équipements ayant servi à la mise au point, à la fabrication, à la détention ou au stockage de ces agents ou toxines ;
3° L'interdiction, suivant les modalités prévues par l'article 131-27 du code pénal, d'exercer l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Art. L2341-5
Le fait de provoquer, d'encourager ou d'inciter quiconque, de quelque manière que ce soit, à commettre les infractions prévues à l'article L. 2341-4, lorsque ce fait a été suivi d'effet, est puni des peines prévues pour ces infractions. Lorsque les faits mentionnés au premier alinéa du présent article ne sont pas suivis d'effet en raison de circonstances indépendantes de la volonté de leur auteur, la peine est de sept ans d'emprisonnement et de 100 000 € d'amende.

Art. L2342-57
Est puni de la réclusion criminelle à perpétuité et de 7 500 000 euros d'amende le fait d'employer :
1° Une arme chimique ;
2° Un produit chimique inscrit au tableau 1 à des fins autres que médicales, pharmaceutiques, de recherche ou de protection.
Les deux premiers alinéas de l'article 132-23 du code pénal relatif à la période de sûreté sont applicables aux infractions prévues par le présent article.

Art. L2342-58
Sont punies de la réclusion criminelle à perpétuité et de 7 500 000 euros d'amende la conception, la construction ou l'utilisation d'une installation :
1° De fabrication d'armes chimiques ;
2° De fabrication de munitions chimiques non remplies et de matériels destinés à l'emploi d'armes chimiques.
La modification d'installations ou de matériels de toute nature dans le but d'exercer une activité interdite par la sous-section 1 de la première section du présent chapitre est punie des mêmes

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

peines.
Les deux premiers alinéas de l'article 132-23 du code pénal relatif à la période de sûreté sont applicables aux infractions prévues par le présent article.

Art. L2342-59
Est puni de la réclusion criminelle à perpétuité et de 7 500 000 euros d'amende le fait de diriger ou d'organiser un groupement ayant pour objet l'emploi, la mise au point, la fabrication, le stockage, la détention, la conservation, l'acquisition, la cession, l'importation, l'exportation, le transit, le commerce ou le courtage :
1° D'une arme chimique ;
2° D'un produit chimique inscrit au tableau 1 à des fins autres que médicales, pharmaceutiques, de recherche ou de protection.
Les deux premiers alinéas de l'article 132-23 du code pénal relatif à la période de sûreté sont applicables aux infractions prévues par le présent article.

Art. L2342-60
Sont punis de vingt ans de réclusion criminelle et de 3 000 000 euros d'amende la mise au point, la fabrication, le stockage, la détention, la conservation, l'acquisition, la cession, l'importation, l'exportation, le transit, le commerce ou le courtage :
1° D'une arme chimique autre qu'une arme chimique ancienne ou qu'une arme chimique abandonnée ;
2° D'un produit chimique inscrit au tableau 1 à des fins autres que des fins médicales, pharmaceutiques, de recherche ou de protection.
Sont punis des mêmes peines l'importation, l'exportation, le commerce ou le courtage de tout matériel de fabrication d'armes chimiques ou de tout document ou objet en vue de permettre ou de faciliter la violation des dispositions de la sous-section 1 de la première section du présent chapitre.
Est punie de la même peine la communication de toute information en vue de permettre ou de faciliter la violation des dispositions de la sous-section 1 de la première section du présent chapitre.
Les deux premiers alinéas de l'article 132-23 du code pénal relatif à la période de sûreté sont applicables aux infractions prévues par le présent article.

Art. L2342-61
Le fait de provoquer, d'encourager ou d'inciter quiconque de quelque manière que ce soit à commettre les infractions prévues aux articles L. 2342-57, L. 2342-58 et L. 2342-60, lorsque ce fait a été suivi d'effet, est puni des peines prévues pour ces infractions.
Lorsque les faits mentionnés au premier alinéa ne sont pas suivis d'effet en raison de circonstances indépendantes de la volonté de leur auteur, la peine est de sept ans d'emprisonnement et de 100 000 euros d'amende.

Art. L2342-62
Sont punis de cinq ans d'emprisonnement et de 75 000 euros d'amende l'acquisition, la cession, l'importation, l'exportation, le transit, le commerce ou le courtage d'une arme chimique ancienne ou d'une arme chimique abandonnée.

Art. L2353-4
Sont punies d'un emprisonnement de cinq ans et d'une amende de 3 750 euros :
1° La fabrication, sans autorisation, d'un engin explosif ou incendiaire ou d'un produit explosif, quelle que soit sa composition ;
2° La fabrication de tout autre élément ou substance destinés à entrer dans la composition d'un produit explosif.
Les peines sont portées à dix ans d'emprisonnement et à 500 000 Euros d'amende lorsque l'infraction est commise en bande organisée.
La peine privative de liberté encourue par l'auteur ou le complice des infractions prévues au présent article est réduite de moitié, si ayant averti l'autorité administrative ou judiciaire, il a permis de faire cesser les agissements incriminés et d'identifier, le cas échéant, les autres auteurs ou complices.

Art. L2353-5
Sont punis d'un emprisonnement de cinq ans et d'une amende de 4 500 euros :
1° Le fait de vendre ou d'exporter des produits explosifs figurant sur une liste établie par décret, ou de produire ou d'importer tout produit explosif, en violation de l'article L. 2352-1 ou des textes pris pour son application ; […]

Art. L2353-13
L'acquisition, la détention, le transport ou le port illégal de produits explosifs ou d'engins explosifs sont punis selon les dispositions du chapitre IX du titre III du présent livre applicables aux armes de la 1re catégorie.
Les dispositions du premier alinéa ne sont pas applicables à l'acquisition, à la détention, au transport ou au port d'une quantité de 2 kilogrammes au plus de poudre noire ou de poudre à usage civil, en vue de la confection de munitions de chasse ou de tir.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Insider offences*"	***Code monétaire et financier* (French Monetary and Financial Code)[36]:** **Art. L465-1** Est puni de deux ans d'emprisonnement et d'une amende de 1 500 000 euros dont le montant peut être porté au-delà de ce chiffre, jusqu'au décuple du montant du profit éventuellement réalisé, sans que l'amende puisse être inférieure à ce même profit, le fait, pour les dirigeants d'une société mentionnée à l'article L. 225-109 du code de commerce, et pour les personnes disposant, à l'occasion de l'exercice de leur profession ou de leurs fonctions, d'informations privilégiées sur les perspectives ou la situation d'un émetteur dont les titres sont négociés sur un marché réglementé ou sur les perspectives d'évolution d'un instrument financier ou d'un actif visé au II de l'article L. 421-1 admis sur un marché réglementé, de réaliser ou de permettre de réaliser, soit directement, soit par personne interposée, une ou plusieurs opérations avant que le public ait connaissance de ces informations. Est puni d'un an d'emprisonnement et de 150 000 euros d'amende le fait, pour toute personne disposant dans l'exercice de sa profession ou de ses fonctions d'une information privilégiée sur les perspectives ou la situation d'un émetteur dont les titres sont négociés sur un marché réglementé ou sur les perspectives d'évolution d'un instrument financier ou d'un actif visé au II de l'article L. 421-1 admis sur un marché réglementé, de la communiquer à un tiers en dehors du cadre normal de sa profession ou de ses fonctions. Est puni d'un an d'emprisonnement et d'une amende de 150 000 euros dont le montant peut être porté au-delà de ce chiffre, jusqu'au décuple du montant du profit réalisé, sans que l'amende puisse être inférieure à ce même profit, le fait pour toute personne autre que celles visées aux deux alinéas précédents, possédant en connaissance de cause des informations privilégiées sur la situation ou les perspectives d'un émetteur dont les titres sont négociés sur un marché réglementé ou sur les perspectives d'évolution d'un instrument financier ou d'un actif visé au II de l'article L. 421-1 admis sur un marché réglementé, de réaliser ou de permettre de réaliser, directement ou indirectement, une opération ou de communiquer à un tiers ces informations, avant que le public en ait connaissance. Lorsque les informations en cause concernent la commission d'un crime ou d'un délit, les peines encourues sont portées à sept ans d'emprisonnement et à 1 500 000 euros si le montant des profits réalisés est inférieur à ce chiffre.
"*Endangering human, animal or environmental health by introducing substances into the air, soil, sub-soil, foodstuffs or foodstuff ingredients, or water*" "*Conspiracy to commit terrorist offences*" "*Funding of a terrorist operation*" "*Failure to account for resources*"	IN ADDITION TO THE ABOVEMENTIONED OFFENCES LISTED IN ARTICLE 421-1 OF THE *CODE PÉNAL* (FRENCH PENAL CODE), THE FRENCH PENAL CODE AND THE *LOI DU 29 JUILLET 1881 SUR LA LIBERTÉ DE LA PRESSE* (ACT OF 29 JULY 1881 ON FREEDOM OF THE PRESS) SPECIFICALLY PUNISHE THE FOLLOWING TERRORIST, OR POTENTIALLY TERRORIST OFFENCES: ***Code pénal* (French Penal Code)[37]:** **Art. 421-2** Constitue également un acte de terrorisme, lorsqu'il est intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, le fait d'introduire dans l'atmosphère, sur le sol, dans le sous-sol, dans les aliments ou les composants alimentaires ou dans les eaux, y compris celles de la mer territoriale, une substance de nature à mettre en péril la santé de l'homme ou des animaux ou le milieu naturel. **Art. 421-2-1** Constitue également un acte de terrorisme le fait de participer à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un des actes de terrorisme mentionnés aux articles précédents. [Please see also Article 421-6 below]. **Art. 421-2-2** Constitue également un acte de terrorisme le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme prévus au présent chapitre, indépendamment de la survenance éventuelle d'un tel acte. **Art. 421-2-3** Le fait de ne pouvoir justifier de ressources correspondant à son train de vie, tout en étant en relations habituelles avec une ou plusieurs personnes se livrant à l'un ou plusieurs des actes visés aux articles 421-1 à 421-2-2, est puni de sept ans d'emprisonnement et de 100 000 Euros d'amende. **Art. 421-3** Le maximum de la peine privative de liberté encourue pour les infractions mentionnées à l'article 421-1 est relevé ainsi qu'il suit lorsque ces infractions constituent des actes de terrorisme : 1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle ; 2° Il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle ; 3° Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle ; 4° Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans d'emprisonnement ; 5° Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de sept ans d'emprisonnement ; 6° Il est porté à sept ans d'emprisonnement lorsque l'infraction est punie de cinq ans d'emprisonnement ; 7° Il est porté au double lorsque l'infraction est punie d'un emprisonnement de trois ans au plus.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	Les deux premiers alinéas de l'article 132-23 relatif à la période de sûreté sont applicables aux crimes, ainsi qu'aux délits punis de dix ans d'emprisonnement, prévus par le présent article. **Art. 421-4** L'acte de terrorisme défini à l'article 421-2 est puni de vingt ans de réclusion criminelle et de 350000 euros d'amende. Lorsque cet acte a entraîné la mort d'une ou plusieurs personnes, il est puni de la réclusion criminelle à perpétuité et de 750000 euros d'amende. Les deux premiers alinéas de l'article 132-23 relatif à la période de sûreté sont applicables au crime prévu par le présent article.
"*Direction and organization of a criminal association for the purpose of preparing terrorist acts*"	**Art. 421-5** Les actes de terrorisme définis aux articles 421-2-1 et 421-2-2 sont punis de dix ans d'emprisonnement et de 225000 euros d'amende. Le fait de diriger ou d'organiser le groupement ou l'entente défini à l'article 421-2-1 est puni de vingt ans de réclusion criminelle et de 500 000 Euros d'amende. La tentative du délit défini à l'article 421-2-2 est punie des mêmes peines. Les deux premiers alinéas de l'article 132-23 relatif à la période de sûreté sont applicables aux infractions prévues par le présent article.
"*Concealment of the authors of a terrorist act*"	**Art. 421-6** Les peines sont portées à vingt ans de réclusion criminelle et 350 000 euros d'amende lorsque le groupement ou l'entente définie à l'article 421-2-1 a pour objet la préparation : 1° Soit d'un ou plusieurs crimes d'atteintes aux personnes visés au 1° de l'article 421-1 ; 2° Soit d'une ou plusieurs destructions par substances explosives ou incendiaires visées au 2° de l'article 421-1 et devant être réalisées dans des circonstances de temps ou de lieu susceptibles d'entraîner la mort d'une ou plusieurs personnes ; 3° Soit de l'acte de terrorisme défini à l'article 421-2 lorsqu'il est susceptible d'entraîner la mort d'une ou plusieurs personnes. Le fait de diriger ou d'organiser un tel groupement ou une telle entente est puni de trente ans de réclusion criminelle et 500 000 euros d'amende. Les deux premiers alinéas de l'article 132-23 relatifs à la période de sûreté sont applicables aux crimes prévus par le présent article.
"*Disclosure of information which may impede a investigation related to acts of terrorist*"	**Art. 434-7-2** Sans préjudice des droits de la défense, le fait, pour toute personne qui, du fait de ses fonctions, a connaissance, en application des dispositions du code de procédure pénale, d'informations issues d'une enquête ou d'une instruction en cours concernant un crime ou un délit, de révéler sciemment ces informations à des personnes qu'elle sait susceptibles d'être impliquées comme auteurs, coauteurs, complices ou receleurs, dans la commission de ces infractions, lorsque cette révélation est réalisée dans le dessein d'entraver le déroulement des investigations ou la manifestation de la vérité, est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsque l'enquête ou l'instruction concerne un crime ou un délit puni de dix ans d'emprisonnement relevant des dispositions de l'article 706-73 du code de procédure pénale, les peines sont portées à cinq ans d'emprisonnement et à 75 000 euros d'amende.
"*Direct incitement to, and justification of, terrorism*"	***Loi du 29 juillet 1881 sur la liberté de la presse* (Act of 29 July 1881 on Freedom of the Press)[38]:** **Art. 24** Seront punis de cinq ans d'emprisonnement et de 45 000 euros d'amende ceux qui, par l'un des moyens énoncés à l'article précédent, auront directement provoqué, dans le cas où cette provocation n'aurait pas été suivie d'effet, à commettre l'une des infractions suivantes : 1° Les atteintes volontaires à la vie, les atteintes volontaires à l'intégrité de la personne et les agressions sexuelles, définies par le livre II du code pénal ; 2° Les vols, les extorsions et les destructions, dégradations et détériorations volontaires dangereuses pour les personnes, définis par le livre III du code pénal. Ceux qui, par les mêmes moyens, auront directement provoqué à l'un des crimes et délits portant atteinte aux intérêts fondamentaux de la nation prévus par le titre Ier du livre IV du code pénal, seront punis des mêmes peines. Seront punis de la même peine ceux qui, par l'un des moyens énoncés en l'article 23, auront fait l'apologie des crimes visés au premier alinéa, des crimes de guerre, des crimes contre l'humanité ou des crimes et délits de collaboration avec l'ennemi. Seront punis des peines prévues par l'alinéa 1er ceux qui, par les mêmes moyens, auront provoqué directement aux actes de terrorisme prévus par le titre II du livre IV du code pénal, ou qui en auront fait l'apologie. Tous cris ou chants séditieux proférés dans les lieux ou réunions publics seront punis de l'amende prévue pour les contraventions de la 5° classe. Ceux qui, par l'un des moyens énoncés à l'article 23, auront provoqué à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, seront punis d'un an d'emprisonnement et de 45 000 euros d'amende ou de l'une de ces deux peines seulement. Seront punis des peines prévues à l'alinéa précédent ceux qui, par ces mêmes moyens, auront provoqué à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap ou auront provoqué, à l'égard des mêmes personnes, aux discriminations prévues par les articles 225-2 et 432-7 du code pénal. En cas de condamnation pour l'un des faits prévus par les deux alinéas précédents, le tribunal pourra en outre ordonner : 1° Sauf lorsque la responsabilité de l'auteur de l'infraction est retenue sur le fondement de l'article 42 et du premier alinéa de l'article 43 de la présente loi ou des trois premiers alinéas de l'article

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle, la privation des droits énumérés aux 2° et 3° de l'article 131-26 du code pénal pour une durée de cinq ans au plus ; 2° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 du code pénal.

b.3 – Proscribed Organizations

Country	Grounds of proscription and List of organizations
Canada "*Definition*" "*Grounds of proscription*"	***Criminal Code***[39]**:** **Sec. 83.01(1) Definitions** (1) The following definitions apply in this Part. […] "entity" means a person, group, trust, partnership or fund or an unincorporated association or organization. "listed entity" means an entity on a list established by the Governor in Council under section 83.05. […] "terrorist group" means (a) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or (b) a listed entity, and includes an association of such entities. […] **Sec. 83.05 List of Entities** (1) The Governor in Council may, by regulation, establish a list on which the Governor in Council may place any entity if, on the recommendation of the Minister of Public Safety and Emergency Preparedness, the Governor in Council is satisfied that there are reasonable grounds to believe that (a) the entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or (b) the entity is knowingly acting on behalf of, at the direction of or in association with an entity referred to in paragraph (a). Recommendation (1.1) The Minister may make a recommendation referred to in subsection (1) only if he or she has reasonable grounds to believe that the entity to which the recommendation relates is an entity referred to in paragraph (1)(a) or (b). Application to Minister (2) On application in writing by a listed entity, the Minister shall decide whether there are reasonable grounds to recommend to the Governor in Council that the applicant no longer be a listed entity. Deeming (3) If the Minister does not make a decision on the application referred to in subsection (2) within 60 days after receipt of the application, he or she is deemed to have decided to recommend that the applicant remain a listed entity. Notice of the decision to the applicant (4) The Minister shall give notice without delay to the applicant of any decision taken or deemed to have been taken respecting the application referred to in subsection (2). Judicial review (5) Within 60 days after the receipt of the notice of the decision referred to in subsection (4), the applicant may apply to a judge for judicial review of the decision. Reference (6) When an application is made under subsection (5), the judge shall, without delay (a) examine, in private, any security or criminal intelligence reports considered in listing the applicant and hear any other evidence or information that may be presented by or on behalf of the Minister and may, at his or her request, hear all or part of that evidence or information in the absence of the applicant and any counsel representing the applicant, if the judge is of the opinion that the disclosure of the information would injure national security or endanger the safety of any person; (b) provide the applicant with a statement summarizing the information available to the judge so as to enable the applicant to be reasonably informed of the reasons for the decision, without disclosing any information the disclosure of which would, in the judge's opinion, injure national security or endanger the safety of any person; (c) provide the applicant with a reasonable opportunity to be heard; and (d) determine whether the decision is reasonable on the basis of the information available to the judge and, if found not to be reasonable, order that the applicant no longer be a listed entity. Evidence (6.1) The judge may receive into evidence anything that, in the opinion of the judge, is reliable and appropriate, even if it would not otherwise be admissible under Canadian law, and may base his

[39] Canadian *Criminal Code*: http://laws-lois.justice.gc.ca/fra/lois/C-46/

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

"*Listed entities*"	or her decision on that evidence. Publication (7) The Minister shall cause to be published, without delay, in the Canada Gazette notice of a final order of a court that the applicant no longer be a listed entity. New application (8) A listed entity may not make another application under subsection (2), except if there has been a material change in its circumstances since the time when the entity made its last application or if the Minister has completed the review under subsection (9). Review of list (9) Two years after the establishment of the list referred to in subsection (1), and every two years after that, the Minister shall review the list to determine whether there are still reasonable grounds, as set out in subsection (1), for an entity to be a listed entity and make a recommendation to the Governor in Council as to whether the entity should remain a listed entity. The review does not affect the validity of the list. Completion of review (10) The Minister shall complete the review as soon as possible and in any event, no later than 120 days after its commencement. After completing the review, he or she shall cause to be published, without delay, in the Canada Gazette notice that the review has been completed. Definition of "judge" (11) In this section, "judge" means the Chief Justice of the Federal Court or a judge of that Court designated by the Chief Justice. For a catalogue of listed entities, see: http://www.publicsafety.gc.ca/prg/ns/le/cle-eng.aspx For official reference, refer to the "Assented to" Acts service in Part III of the Canada Gazette at: http://www.gazette.gc.ca/index-eng.html
United States "*Grounds of proscription*" "*List of proscribed organizations*"	***Executive Order E.O. 13224***[40]**:** **Sec. 1** Except to the extent required by section 203(b) of IEEPA (50 U.S.C. 1702(b)), or provided in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of this order, all property and interests in property of the following persons that are in the United States or that hereafter come within the United States, or that hereafter come within the possession or control of United States persons are blocked: (a) foreign persons listed in the Annex to this order; (b) foreign persons determined by the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, to have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States; (c) persons determined by the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General, to be owned or controlled by, or to act for or on behalf of those persons listed in the Annex to this order or those persons determined to be subject to subsection 1(b), 1(c), or 1(d)(i) of this order; (d) except as provided in section 5 of this order and after such consultation, if any, with foreign authorities as the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, deems appropriate in the exercise of his discretion, persons determined by the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General; (i) to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, such acts of terrorism or those persons listed in the Annex to this order or determined to be subject to this order; or (ii) to be otherwise associated with those persons listed in the Annex to this order or those persons determined to be subject to subsection 1(b), 1(c), or 1(d)(i) of this order. **Sec. 3** For purposes of this order: […] (d) the term ''terrorism'' means an activity that— (i) involves a violent act or an act dangerous to human life, property, or infrastructure; and (ii) appears to be intended— (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking. Available in the **Annex** of the ***Executive Order E.O. 13224*** at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr25se01-133.pdf An up-to-date list is available at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/terror.pdf

[40] US *Executive Order E.O. 13224*: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr25se01-133.pdf

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

United Kingdom "*Grounds of proscription*" "*List of proscribed organizations*"	***Terrorism Act 2000***[41]**:** **Sec. 3 Proscription** (1) For the purposes of this Act an organisation is proscribed if— (a) it is listed in Schedule 2, or (b) it operates under the same name as an organisation listed in that Schedule. (2) Subsection (1)(b) shall not apply in relation to an organisation listed in Schedule 2 if its entry is the subject of a note in that Schedule. (3) The Secretary of State may by order— (a) add an organisation to Schedule 2; (b) remove an organisation from that Schedule; (c) amend that Schedule in some other way. (4) The Secretary of State may exercise his power under subsection (3)(a) in respect of an organisation only if he believes that it is concerned in terrorism. (5) For the purposes of subsection (4) an organisation is concerned in terrorism if it— (a) commits or participates in acts of terrorism, (b) prepares for terrorism, (c) promotes or encourages terrorism, or (d) is otherwise concerned in terrorism. (5A) The cases in which an organisation promotes or encourages terrorism for the purposes of subsection (5)(c) include any case in which activities of the organisation— (a) include the unlawful glorification of the commission or preparation (whether in the past, in the future or generally) of acts of terrorism; or (b) are carried out in a manner that ensures that the organisation is associated with statements containing any such glorification. (5B) The glorification of any conduct is unlawful for the purposes of subsection (5A) if there are persons who may become aware of it who could reasonably be expected to infer that what is being glorified, is being glorified as— (a) conduct that should be emulated in existing circumstances, or (b) conduct that is illustrative of a type of conduct that should be so emulated. (5C) In this section— "glorification" includes any form of praise or celebration, and cognate expressions are to be construed accordingly; "statement" includes a communication without words consisting of sounds or images or both. (6) Where the Secretary of State believes— (a) that an organisation listed in Schedule 2 is operating wholly or partly under a name that is not specified in that Schedule (whether as well as or instead of under the specified name), or (b) that an organisation that is operating under a name that is not so specified is otherwise for all practical purposes the same as an organisation so listed, he may, by order, provide that the name that is not specified in that Schedule is to be treated as another name for the listed organisation. (7) Where an order under subsection (6) provides for a name to be treated as another name for an organisation, this Act shall have effect in relation to acts occurring while— (a) the order is in force, and (b) the organisation continues to be listed in Schedule 2, as if the organisation were listed in that Schedule under the other name, as well as under the name specified in the Schedule. (8) The Secretary of State may at any time by order revoke an order under subsection (6) or otherwise provide for a name specified in such an order to cease to be treated as a name for a particular organisation. (9) Nothing in subsections (6) to (8) prevents any liability from being established in any proceedings by proof that an organisation is the same as an organisation listed in Schedule 2, even though it is or was operating under a name specified neither in Schedule 2 nor in an order under subsection (6). Available in the **Schedule 2** of **Part II** of the ***Terrorism Act 2000*** at http://www.legislation.gov.uk/ukpga/2000/11/schedule/2
Australia "*Definition*"	***Criminal Code Act 1995***[42]**:** **Sec. 102.1 Definitions** (1) In this Division: […] *terrorist organisation* means:

[41] UK *Terrorism Act 2000*: http://www.legislation.gov.uk/ukpga/2000/11/contents
[42] Australian *Criminal Code Act 1995*: http://www.comlaw.gov.au/Details/C2011C00123

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Grounds of proscription*" "*List of proscribed organizations*"	(a) an organisation that is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not a terrorist act occurs); or (b) an organisation that is specified by the regulations for the purposes of this paragraph (see subsections (2), (3) and (4)). […] **Sec. 102.1 Definitions** (1) In this Division: […] (2) Before the Governor-General makes a regulation specifying an organisation for the purposes of paragraph (b) of the definition of terrorist organisation in this section, the Minister must be satisfied on reasonable grounds that the organisation: (a) is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not a terrorist act has occurred or will occur); or (b) advocates the doing of a terrorist act (whether or not a terrorist act has occurred or will occur). […] Available in the **Criminal Code Regulations 2002** at: http://www.comlaw.gov.au/Details/F2011C00190
New Zealand "*Grounds of proscription*"	***Terrorism Suppression Act 2002***[43]**:** **Sec. 20 Interim designation as terrorist or associated entity** (1) The Prime Minister may designate an entity as a terrorist entity under this section if the Prime Minister has good cause to suspect that the entity has knowingly carried out, or has knowingly participated in the carrying out of, 1 or more terrorist acts. (2) On or after designating an entity as a terrorist entity under this Act, the Prime Minister may designate 1 or more other entities as an associated entity under this section. (3) The Prime Minister may exercise the power given by subsection (2) only if the Prime Minister has good cause to suspect that the other entity— (a) is knowingly facilitating the carrying out of 1 or more terrorist acts by, or with the participation of, the terrorist entity (for example, by financing those acts, in full or in part); or (b) is acting on behalf of, or at the direction of,— (i) the terrorist entity, knowing that the terrorist entity has done what is referred to in subsection (1); or (ii) an entity designated as an associated entity under subsection (2) and paragraph (a), knowing that the associated entity is doing what is referred to in paragraph (a); or (c) is an entity (other than an individual) that is wholly owned or effectively controlled, directly or indirectly, by the terrorist entity, or by an entity designated under subsection (2) and paragraph (a) or paragraph (b). (4) Before designating an entity as a terrorist or associated entity under this section, the Prime Minister must consult with the Attorney-General and the Minister of Foreign Affairs and Trade about the proposed designation. (5) After an entity is designated as a terrorist or associated entity under this section, the Prime Minister and the Attorney-General must, if practicable before the making of the designation is publicly notified under section 21(c) and, if not so practicable, as soon as possible after that notification,— (a) advise the Leader of the Opposition of the making of the designation; and (b) if requested to do so by the Leader of the Opposition, brief that Leader as to the factual basis for the making of the designation. **21 Further provisions relating to interim designation** A designation under section 20— (a) may be made in respect of an entity only once, and therefore may not be made in respect of an entity who— (i) is the subject of an earlier designation made under section 20 that has not yet expired or been revoked; or (ii) was the subject of a designation under section 20 that has expired or been revoked: (b) takes effect on being made, and must be made in writing signed by the Prime Minister: (c) must be publicly notified— (i) by a notice (in the prescribed form (if any)) indicating that it has been made being published in the Gazette as soon as practicable; and (ii) in any other way the Prime Minister directs under section 28(1): (d) must also be notified— (i) by a notice (in the prescribed form (if any)) indicating that it has been made being given (in the prescribed manner (if any)) with all reasonable speed to the designated entity, if practicable, where that entity or a representative of it is in New Zealand; and (ii) by a notice indicating that it has been made being given to any other persons or bodies, as the Prime Minister directs under section 28(2): (e) expires on the close of the 30th day after the day on which it is made, unless it has earlier been revoked by the Prime Minister under section 34, or by the making of a final designation in

[43] NZ *Terrorism Suppression Act 2002*: http://www.legislation.govt.nz/act/public/2002/0034/latest/whole.html#dlm151491

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*List of proscribed organizations*"	respect of the entity concerned, under section 22: (f) operates until it expires or is revoked but, if it is made the subject of any judicial review (whether under Part 1 of the Judicature Amendment Act 1972 or otherwise) or other proceedings before a court and is not sooner revoked under section 23(b) or section 34, continues to operate until those proceedings are withdrawn or finally determined. **Sec, 22 Final designation as terrorist or associated entity** (1) The Prime Minister may designate an entity as a terrorist entity under this section if the Prime Minister believes on reasonable grounds that the entity has knowingly carried out, or has knowingly participated in the carrying out of, 1 or more terrorist acts. (2) On or after designating an entity as a terrorist entity under this Act, the Prime Minister may designate 1 or more other entities as an associated entity under this section. (3) The Prime Minister may exercise the power given by subsection (2) only if the Prime Minister believes on reasonable grounds that the other entity— (a) is knowingly facilitating the carrying out of 1 or more terrorist acts by, or with the participation of, the terrorist entity (for example, by financing those acts, in full or in part); or (b) is acting on behalf of, or at the direction of,— (i) the terrorist entity, knowing that the terrorist entity has done what is referred to in subsection (1); or (ii) an entity designated as an associated entity under subsection (2) and paragraph (a), knowing that the associated entity is doing what is referred to in paragraph (a); or (c) is an entity (other than an individual) that is wholly owned or effectively controlled, directly or indirectly, by the terrorist entity, or by an entity designated under subsection (2) and paragraph (a) or paragraph (b). (4) Before designating an entity as a terrorist or associated entity under this section, the Prime Minister must consult with the Attorney-General about the proposed designation. **Sec. 23 Further provisions relating to final designation** A designation under section 22— (a) may be made in respect of an entity who— (i) has never been the subject of a designation made under section 20; or (ii) is the subject of a designation under section 20 that has not yet expired or been revoked; or (iii) was the subject of a designation under section 20 that has expired or been revoked: (b) if it is made in respect of an entity who is the subject of a designation made under section 20 and that has not yet expired or been revoked, revokes that designation under section 20: (c) may be made in respect of an entity who was earlier the subject of a designation made under section 22 and that has expired or been revoked (the earlier designation) only if it is based on information that became available after the expiry or revocation of the earlier designation and is significantly different from the information on which the earlier designation was based: (d) takes effect on being made, and must be made in writing signed by the Prime Minister: (e) must be publicly notified— (i) by a notice (in the prescribed form (if any)) indicating that it has been made being published in the Gazette as soon as practicable; and (ii) in any other way the Prime Minister directs under section 28(1): (f) must also be notified— (i) by a notice (in the prescribed form (if any)) indicating that it has been made being given (in the prescribed manner (if any)) with all reasonable speed to the designated entity, if practicable, where that entity or a representative of it is in New Zealand; and (ii) by a notice indicating that it has been made being given to any other persons or bodies, as the Prime Minister directs under section 28(2): (g) [Repealed] (h) operates until it expires or is revoked but, if it is made the subject of any judicial review (whether under Part 1 of the Judicature Amendment Act 1972 or otherwise) or other proceedings before a court and is not sooner revoked under section 34, continues to operate until those proceedings are withdrawn or finally determined. [*Please also refer to sections 24 to 42 of the* Terrorism Suppression Act 2002] Information about and list of designated terrorist individuals and organisations are available at: http://www.police.govt.nz/service/counterterrorism/designated-terrorists.html
France	As a member state of the European Union (EU), France has adhered to the EU joint position on the collective application of specific measures to combat terrorism. These EU measures include the designation of persons, groups and entities involved in "terrorist acts", as provided in the **Common Position 2001/931/CFSP** and the **Regulation 2580/2001** adopted by the Council of the European Union on 27 December 2001. The list of organisations drawn-up under the EU Common Position and Regulation, and the Common Position itself have been updated several times since the year 2001. Information about the EU terrorist list and related regime can be found at: http://www.consilium.europa.eu/showPage.aspx?id=1878&lang=en

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(c) Current POLICE POWERS Specifically Created to Investigate Terrorism Offences in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011)

Since the events of 11 September 2001, the legislative trend has been towards broadening the powers and tools available to the police and law enforcement agencies in order to strengthen their capacity to prevent, detect and investigate terrorism-related activity. As is the case with the definition of new terrorist offences (Title (b) *supra*), countries surveyed have approached the issue of extending investigative measures in different ways, based on their pre-existing legislation, social values, and framework of fundamental rights and freedoms. While some countries surveyed primarily focused on the enlargement of police powers proper (such as the United Kingdom and Australia), other countries have centred their efforts on the gathering and sharing of intelligence information from a greater variety of sources (such as the United States). In most (but not all) countries, the expanded powers and/or investigative measures exceed those that apply in regular criminal investigations. This Title of the research provides an overview of most important investigative tools created or broadened after 11 September 2001 in Canada, the United States (US), the United Kingdom (UK), Australia, New Zealand (NZ), and France.

c.1 – Police Powers and Other Investigative Tools	
Country	**Summary of legal framework and approach**
Canada	In 2001, the *Anti-terrorism Act* introduced provisions in the *Criminal Code* that provided law enforcement officials with two (2) new investigative tools: investigative hearings and preventive arrests. The former was governed by section 83.28 of the *Criminal Code*, and the later by section 83.3 of the *Code*. Investigative hearings were available only in the case of terrorist offences that had been committed or that could be committed. Under the conditions set out in the *Criminal Code*, a peace officer could compelled a person to attend a hearing before a judge, answer questions, and bring along anything in his or her possession relevant to a terrorist offence investigation. With respect to preventive arrests, a peace officer who believed that a terrorist activity would be carried out, could, after satisfying specific conditions set out in the *Criminal Code*, lay an information concerning that person before a provincial court judge, who could in turn order that person to appear before him or her. Once an information had been laid and summons issued or, alternatively, if there were grounds for laying the information and it could not be laid due to exigent circumstances, a peace officer could arrest the person without warrant and detain that person in custody. Subject that the relevant conditions were met, a judge could order that the detention of that person be continued for up to 12 months, or that the person be released under certain terms and conditions. These provisions were allowed to sunset on 1 March 2007, but in April 2010 the *Bill C-17 An Act to Amend the Criminal Code (Investigative Hearing and Recognizance with Conditions)* proposed to reinstate these anti-terrorism measures. This *Bill* was before the Parliament at its dissolution for the general election in March 2011 (see also Titles (d) and (e), *infra*). With respect to other tools available under Canadian law to detect and investigate terrorism, it is to be noticed that, unlike other countries, such as the US, the *Anti-terrorism Act* did not significantly alter Canada's approach to electronic surveillance and communication interception. In almost all cases, prior judicial authorisation is still required before electronic surveillance or communication interception can be conducted, including for foreign intelligence purpose.[44] The sole exception to this is when private communication is intercepted by the Communication Security Establishment (CSE), in which case prior authorisation from the Minister of National Defence is required.[45] With regard to information gathering and sharing, the *Anti-terrorism Act* has similarly done little to enlarge the powers of investigative agencies. The *Act* has, however, significantly enhanced the capacity to keep secret information related to national security or terrorist entities.[46]
United States	Since the events of 11 September 2001, the US has passed many laws that deal with terrorism. An assessment of all relevant existing pieces of US legislation is beyond the bounds of what could practically be achieved with this research. As indicated previously, the research focuses on US federal law and in particular, on the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorist Act* (*USA Patriot Act*) and the *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, which are the key legislative instruments used by the US to detect and investigate terrorism. Unlike other countries, such as the UK, the legislative framework that the US has put into place to enhance the investigation of terrorism has been primarily directed towards the gathering and sharing of intelligence information. It is to be noticed that, with respect to the situation in the US, there was no need to introduce investigative tools comparable to the investigative hearings or preventive arrests in Canada, because US law already contained equivalent tools: the grand jury process and the material witness arrest process. The *USA Patriot Act* did, however, introduce some changes to the grand jury process, and the response to the events of 11 September 2001 appears to have changed how the material arrest process is being used. Further information about these investigative tools is provided directly in the Chart c.2 below. With respect to electronic surveillance and communication

[44] On this subject, please refer to sections 21 to 28 of the *Canadian Security Intelligence Service (CSIS) Act*: http://laws-lois.justice.gc.ca/eng/acts/C-23/FullText.html
[45] On this subject, please refer to sections 273.61 to 273.7 of the Canadian *National Defence Act*: http://laws-lois.justice.gc.ca/eng/acts/N-5/FullText.html
[46] On this subject, see sections 38.13 and 38.131 of the *Canada Evidence Act*: http://laws-lois.justice.gc.ca/eng/acts/C-5/FullText.html and sections 83.05(6) and 85.06 of the *Criminal Code*: http://laws-lois.justice.gc.ca/eng/acts/C-46/FullText.html

000437

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	interception, the *USA Patriot Act* broadened the capacity of law enforcement officials to obtain certain types of courts order for electronic surveillance or communication interception. It also amended existing laws to broaden the types of information that may be obtained under such orders in certain circumstances. Examples of these changes are provided under the Chart c.2 below (see FISA surveillance order and FISA roving order). As regard information gathering, amendments to the *United States Code* introduced by the *USA Patriot Act* provide investigative agencies with more power and authority to gather and share foreign intelligence information from a greater variety of sources. Examples of these changes are for instance intelligence information obtained through a legally authorised wiretap[47] and FISA access to tangible items.[48]
United Kingdom	In the UK, the legislation enacted as of the mid-1970s to address Northern Ireland paramilitary violence provided police officers with broadened powers of investigation in terrorism-related cases, particularly in the area of detention of suspects for questioning. Since the *Terrorism Act 2000* and the events of 11 September 2001, the UK Parliament has further extended these powers, and police officers investigating terrorism offences can currently draw on powers that appreciably exceed those that apply in regular criminal offences investigations. Some of these powers relate specifically to investigation proper, while some other arise in the context of public order and pre-emption, such as stop and search powers. The new investigative powers that have been created by the UK Parliament are found mainly in the *Serious Organised Crimes and Police Act 2005* and the *Terrorism Act 2000* (as amended by the *Criminal Justice Act 2003* and the *Terrorism Act 2006*). The Chart b.2 below provides an overview of the most important police investigative powers available in terrorist cases under UK law. For other powers, such as forfeiture of terrorist property or freezing of assets, please refer directly to the *Anti-Terrorism, Crime & Security Act 2001*.[49] With respect to investigative powers specifically designed for offences related to fund-raising, money laundering, etc., please refer directly to the *Serious Organised Crime and Police Act 2005* (as amended by the *Terrorism Act 2006*).[50] It is to be noticed that police, customs, and immigration officers also have extended counter-terrorism powers, such as powers to stop, question, detain and search persons, to require them to produce identification, and to request information on passengers or crew or their vehicles from ship or aircraft owners or their agents.[51]
Australia	Like the UK, Australia's anti-terrorism legislation made after the events of 11 September 2001 has significantly broadened the powers available to investigating terrorism offences. The new investigative police powers created by the Australian Parliament are found mainly in the *Crimes Act 1914*, as amended by the *Anti-Terrorism Act 2004*. The Chart c.2 below provides an overview of the most important police powers available in Australian law under the *Crimes Act 1914*. It is worth noting that other statutes also provide for investigative powers, in particular: the *Australian Security Intelligence Organisation Act 1979*[52] (which ensures the Australian Security Intelligence Organisation ability to effectively collect information that is necessary to prevent a terrorist act, and obtain warrant to detain and question a person who may have information important to the gathering of intelligence in relation to terrorism offences); the *Customs Act 1901*[53] (which enhances the controls Customs has in place to monitor terrorism-related activities at borders); the *Surveillance Devices Act 2004*[54] (which established procedures for officers to obtain warrants, emergency authorisations and tracking device authorisations); and the *Telecommunication (Interception) Act 1979*[55] (which permitted law enforcement agencies to seek telecommunications interceptions warrants in connection with the investigation of terrorism offences).
New Zealand	As stated previously, NZ enacted the *Terrorism Suppression Act 2002* and six (6) separate statutes coming from the *Counter-Terrorism Bill 2003* after the events of 11 September 2001. While the *Terrorism Suppression Act 2002* focuses primarily on establishing a civil process to designate terrorists and criminal offences for supporting them, the six (6) other statutes centres on broadening criminal penalties and investigative powers that can be applied to terrorism acts. The new investigative powers created by the NZ Parliament are found in mainly three (3) Acts, namely the *Crimes Act 1961*, the *Summary Proceedings Act 1957*, and the *New Zealand Security Intelligence Service Act 1969*. The *Terrorism Suppression Act 2002* also provides for specific powers related to customs and forfeiture of property.[56] The Chart c.2 below provides an overview of the most important investigative powers currently available in NZ law. It is to be noticed that legislatives changes implemented by NZ after September 2001 are not as far-reaching as legislative measures adopted by UK or Australia for instance.

[47] On this subject, please refer directly to section 203 of the *USA Patriot Act*: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf
[48] On this subject, please refer directly to section 215 of the *USA Patriot Act*: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf For other examples of increased information gathering and sharing powers provided to federal intelligence authorities, see also sections 358 and 505 of the *USA Patriot Act*.
[49] UK *Anti-Terrorism, Crime & Security Act 2001*: http://www.legislation.gov.uk/ukpga/2001/24/contents
[50] UK *Serious Organised Crime and Police Act 2005*: http://www.legislation.gov.uk/ukpga/2005/15/contents
[51] On this subject, please refer directly to section 53, Shedule 7 of the UK *Terrorism Act 2000*: http://www.legislation.gov.uk/ukpga/2000/11/contents
[52] *Australian Security Intelligence Organisation Act 1979* (as amended by the *ASIO Legislation Amendment Act 2003* and the *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003*): http://www.comlaw.gov.au/Details/C2011C00144
[53] Australian *Customs Act 1901* (as amended by *Border Security Legislation Act 2002*): http://www.comlaw.gov.au/Details/C2011C00225
[54] Australian *Surveillance Devices Act 2004*: http://www.comlaw.gov.au/Details/C2010C00363
[55] Australian *Telecommunication (Interception and Access) Act 1979* (as modified by the *Telecommunication Interception Legislation Amendment Act 2002*): http://www.comlaw.gov.au/Details/C2011C00146
[56] Please refer directly to sections 47A to 47G and sections 55 to 61 of NZ *Terrorism Supression Act 2002*: http://www.legislation.govt.nz/act/public/2002/0034/latest/DLM151491.html

000438

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

France	As stated previously, since the events of 11 September 2001, France has adopted a series of laws that reinforced its basic legislation and procedural regulations related to terrorism. Under French law, special rules apply to the investigation of terrorism offences by police officers, as well as to the judicial investigation by investigative magistrates (*juges d'instruction*). These powers are found in the *Code de procédure pénale* (French Code of Penal Procedure) and relate to special police custody, special investigation techniques, and special measures to facilitate judicial investigation of terrorism offences or organised crime, of which terrorism form part according to French criminal law. The Chart c.2 below presents an overview of the most important powers existing under the current French Code of Penal Procedure with respect to the investigation of terrorism offences. It is to be noticed that, in addition to these investigative powers, French law also provides for certain other enhanced measures, such as facilities for computerised checking of vehicle registration data, and photographing of occupants.[57]

c.2 – Police Powers and Other Investigative Tools	
Country	**Definitions**
Canada "*Investigative hearings*"	***Criminal Code*[58]:** **Sec. 83.28*** (1) In this section and section 83.29, "judge" means a provincial court judge or a judge of a superior court of criminal jurisdiction. Order for gathering evidence (2) Subject to subsection (3), a peace officer may, for the purposes of an investigation of a terrorism offence, apply ex parte to a judge for an order for the gathering of information. Attorney General's consent (3) A peace officer may make an application under subsection (2) only if the prior consent of the Attorney General was obtained. Making of order (4) A judge to whom an application is made under subsection (2) may make an order for the gathering of information if the judge is satisfied that the consent of the Attorney General was obtained as required by subsection (3) and (a) that there are reasonable grounds to believe that (i) a terrorism offence has been committed, and (ii) information concerning the offence, or information that may reveal the whereabouts of a person suspected by the peace officer of having committed the offence, is likely to be obtained as a result of the order; or (b) that (i) there are reasonable grounds to believe that a terrorism offence will be committed, (ii) there are reasonable grounds to believe that a person has direct and material information that relates to a terrorism offence referred to in subparagraph (i), or that may reveal the whereabouts of an individual who the peace officer suspects may commit a terrorism offence referred to in that subparagraph, and (iii) reasonable attempts have been made to obtain the information referred to in subparagraph (ii) from the person referred to in that subparagraph. Contents of order (5) An order made under subsection (4) may (a) order the examination, on oath or not, of a person named in the order; (b) order the person to attend at the place fixed by the judge, or by the judge designated under paragraph (d), as the case may be, for the examination and to remain in attendance until excused by the presiding judge; (c) order the person to bring to the examination any thing in their possession or control, and produce it to the presiding judge; (d) designate another judge as the judge before whom the examination is to take place; and (e) include any other terms or conditions that the judge considers desirable, including terms or conditions for the protection of the interests of the person named in the order and of third parties or for the protection of any ongoing investigation. Execution of order (6) An order made under subsection (4) may be executed anywhere in Canada. Variation of order

[57] Please refer directly to section 26 of the *Law. No. 2003-239 of 18 March 2003* (on internal security): http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005634107&dateTexte=20110503
[58] Canadian *Criminal Code*: http://laws-lois.justice.gc.ca/fra/lois/C-46/

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Preventive arrests*"	(7) The judge who made the order under subsection (4), or another judge of the same court, may vary its terms and conditions. Obligation to answer questions and produce things (8) A person named in an order made under subsection (4) shall answer questions put to the person by the Attorney General or the Attorney General's agent, and shall produce to the presiding judge things that the person was ordered to bring, but may refuse if answering a question or producing a thing would disclose information that is protected by any law relating to non-disclosure of information or to privilege. Judge to rule (9) The presiding judge shall rule on any objection or other issue relating to a refusal to answer a question or to produce a thing. No person excused from complying with subsection (8) (10) No person shall be excused from answering a question or producing a thing under subsection (8) on the ground that the answer or thing may tend to incriminate the person or subject the person to any proceeding or penalty, but (a) no answer given or thing produced under subsection (8) shall be used or received against the person in any criminal proceedings against that person, other than a prosecution under section 132 or 136; and (b) no evidence derived from the evidence obtained from the person shall be used or received against the person in any criminal proceedings against that person, other than a prosecution under section 132 or 136. Right to counsel (11) A person has the right to retain and instruct counsel at any stage of the proceedings. Order for custody of thing (12) The presiding judge, if satisfied that any thing produced during the course of the examination will likely be relevant to the investigation of any terrorism offence, shall order that the thing be given into the custody of the peace officer or someone acting on the peace officer's behalf. **Sec. 83.29**[*] *Arrest warrant* (1) The judge who made the order under subsection 83.28(4), or another judge of the same court, may issue a warrant for the arrest of the person named in the order if the judge is satisfied, on an information in writing and under oath, that the person (a) is evading service of the order; (b) is about to abscond; or (c) did not attend the examination, or did not remain in attendance, as required by the order. *Execution of warrant* (2) A warrant issued under subsection (1) may be executed at any place in Canada by any peace officer having jurisdiction in that place. *Person to be brought before judge* (3) A peace officer who arrests a person in the execution of a warrant issued under subsection (1) shall, without delay, bring the person, or cause the person to be brought, before the judge who issued the warrant or another judge of the same court. The judge in question may, to ensure compliance with the order, order that the person be detained in custody or released on recognizance, with or without sureties. **Sec. 83.3**" *Preventive arrests* Attorney General's consent required to lay information (1) The consent of the Attorney General is required before a peace officer may lay an information under subsection (2). Terrorist activity (2) Subject to subsection (1), a peace officer may lay an information before a provincial court judge if the peace officer (a) believes on reasonable grounds that a terrorist activity will be carried out; and (b) suspects on reasonable grounds that the imposition of a recognizance with conditions on a person, or the arrest of a person, is necessary to prevent the carrying out of the terrorist activity. Appearance (3) A provincial court judge who receives an information under subsection (2) may cause the person to appear before the provincial court judge. Arrest without warrant (4) Notwithstanding subsections (2) and (3), if (a) either (i) the grounds for laying an information referred to in paragraphs (2)(a) and (b) exist but, by reason of exigent circumstances, it would be impracticable to lay an information under subsection (2), or (ii) an information has been laid under subsection (2) and a summons has been issued, and (b) the peace officer suspects on reasonable grounds that the detention of the person in custody is necessary in order to prevent a terrorist activity, the peace officer may arrest the person without warrant and cause the person to be detained in custody, to be taken before a provincial court judge in accordance with subsection (6).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	Duty of peace officer (5) If a peace officer arrests a person without warrant in the circumstance described in subparagraph (4)(a)(i), the peace officer shall, within the time prescribed by paragraph (6)(a) or (b), (a) lay an information in accordance with subsection (2); or (b) release the person. When person to be taken before judge (6) A person detained in custody shall be taken before a provincial court judge in accordance with the following rules: (a) if a provincial court judge is available within a period of twenty-four hours after the person has been arrested, the person shall be taken before a provincial court judge without unreasonable delay and in any event within that period, and (b) if a provincial court judge is not available within a period of twenty-four hours after the person has been arrested, the person shall be taken before a provincial court judge as soon as possible, unless, at any time before the expiry of the time prescribed in paragraph (a) or (b) for taking the person before a provincial court judge, the peace officer, or an officer in charge within the meaning of Part XV, is satisfied that the person should be released from custody unconditionally, and so releases the person. How person dealt with (7) When a person is taken before a provincial court judge under subsection (6), (a) if an information has not been laid under subsection (2), the judge shall order that the person be released; or (b) if an information has been laid under subsection (2), (i) the judge shall order that the person be released unless the peace officer who laid the information shows cause why the detention of the person in custody is justified on one or more of the following grounds: (A) the detention is necessary to ensure the person's appearance before a provincial court judge in order to be dealt with in accordance with subsection (8), (B) the detention is necessary for the protection or safety of the public, including any witness, having regard to all the circumstances including (I) the likelihood that, if the person is released from custody, a terrorist activity will be carried out, and (II) any substantial likelihood that the person will, if released from custody, interfere with the administration of justice, and (C) any other just cause and, without limiting the generality of the foregoing, that the detention is necessary in order to maintain confidence in the administration of justice, having regard to all the circumstances, including the apparent strength of the peace officer's grounds under subsection (2), and the gravity of any terrorist activity that may be carried out, and (ii) the judge may adjourn the matter for a hearing under subsection (8) but, if the person is not released under subparagraph (i), the adjournment may not exceed forty-eight hours. Hearing before judge (8) The provincial court judge before whom the person appears pursuant to subsection (3) (a) may, if satisfied by the evidence adduced that the peace officer has reasonable grounds for the suspicion, order that the person enter into a recognizance to keep the peace and be of good behaviour for any period that does not exceed twelve months and to comply with any other reasonable conditions prescribed in the recognizance, including the conditions set out in subsection (10), that the provincial court judge considers desirable for preventing the carrying out of a terrorist activity; and (b) if the person was not released under subparagraph (7)(b)(i), shall order that the person be released, subject to the recognizance, if any, ordered under paragraph (a). Refusal to enter into recognizance (9) The provincial court judge may commit the person to prison for a term not exceeding twelve months if the person fails or refuses to enter into the recognizance. Conditions — firearms (10) Before making an order under paragraph (8)(a), the provincial court judge shall consider whether it is desirable, in the interests of the safety of the person or of any other person, to include as a condition of the recognizance that the person be prohibited from possessing any firearm, cross-bow, prohibited weapon, restricted weapon, prohibited device, ammunition, prohibited ammunition or explosive substance, or all of those things, for any period specified in the recognizance, and where the provincial court judge decides that it is so desirable, the provincial court judge shall add such a condition to the recognizance. Surrender, etc. (11) If the provincial court judge adds a condition described in subsection (10) to a recognizance, the provincial court judge shall specify in the recognizance the manner and method by which (a) the things referred to in that subsection that are in the possession of the person shall be surrendered, disposed of, detained, stored or dealt with; and (b) the authorizations, licences and registration certificates held by the person shall be surrendered. Reasons (12) If the provincial court judge does not add a condition described in subsection (10) to a recognizance, the provincial court judge shall include in the record a statement of the reasons for not adding the condition. Variance of conditions (13) The provincial court judge may, on application of the peace officer, the Attorney General or the person, vary the conditions fixed in the recognizance. Other provisions to apply (14) Subsections 810(4) and (5) apply, with any modifications that the circumstances require, to proceedings under this section. ** Sections 83.28 to 83.3 were allowed to sunset on 1 March 2007 and do no longuer form part of the law in Canada.*

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

United States "*Federal grand jury*"	FEDERAL GRAND JURY: The purpose of the federal grand jury is to determine whether or not an individual has committed an offence. It is an inquisitorial and investigative body that does not require probable cause or any other threshold of proof before summoning a witness. The grand jury need only believe that the person in question has information relevant to the matter being investigated. The rules governing the federal grand jury process are found in Chapter 215, Title 18, of the *United States Code*[59] and in Part III of the *Federal Rules of Criminal Procedures*. As stated above, the *USA Patriot Act* has introduced certain changes to the grand jury process. Prior to the enactment of the *Patriot Act*, information obtained through a grand jury inquiry was generally kept secret. Section 203(a) of the *Patriot Act* has altered this feature of the grand jury process in allowing information obtained during a grand jury hearing related to intelligence, counterintelligence or foreign intelligence to be released to a wide variety of federal officials. The relevant provision, as amended by the *Patriot Act*, is reproduced hereinafter. For a discussion of the federal grand jury process, please see in particular: *Briefing Book – Recent Developments in Anti-terrorism Law and Policy in the United Kingdom, United States, Australia and France*, Prepared for the Special Senate Committee on Anti-terrorism, Legal and Legislative Affairs Division, Parliamentary Information and Research Service, Library of Parliament (Canada), 5 August 2010; Jennifer WISPINSKI, *The USA Patriot Act and Canada's Anti-Terrorism Act: Key Differences in Legislative Approach*, Parliamentary Information and Research Service, Library of Parliament (Canada), 31 March 2008; and Sara BEALE and James FELMAN, "The Consequences of Enlisting Federal Grand Juries in the War on Terrorism: Assessing the Patriot Act's Changes in Grand Jury Secrecy", (2002: 25) *Harvard Journal of Law and Public Policy* at 699. ***Federal Rules of Criminal Procedures***[60]**: Rule 6. The Grand Jury** […] (e) Recording and Disclosing the Proceedings. (1) […] (2) Secrecy. (A) No obligation of secrecy may be imposed on any person except in accordance with Rule 6(e)(2)(B). (B) Unless these rules provide otherwise, the following persons must not disclose a matter occurring before the grand jury: (i) a grand juror; (ii) an interpreter; (iii) a court reporter; (iv) an operator of a recording device; (v) a person who transcribes recorded testimony; (vi) an attorney for the government; or (vii) a person to whom disclosure is made under Rule 6(e)(3)(A)(ii) or (iii). (3) Exceptions. (A) Disclosure of a grand-jury matter—other than the grand jury's deliberations or any grand juror's vote—may be made to: (i) an attorney for the government for use in performing that attorney's duty; (ii) any government personnel—including those of a state or state subdivision, Indian tribe, or foreign government—that an attorney for the government considers necessary to assist in performing that attorney's duty to enforce federal criminal law; or (iii) a person authorized by 18 U.S.C. § 3322. (B) A person to whom information is disclosed under Rule 6(e)(3)(A)(ii) may use that information only to assist an attorney for the government in performing that attorney's duty to enforce federal criminal law. An attorney for the government must promptly provide the court that impaneled the grand jury with the names of all persons to whom a disclosure has been made, and must certify that the attorney has advised those persons of their obligation of secrecy under this rule. (C) An attorney for the government may disclose any grand-jury matter to another federal grand jury. (D) An attorney for the government may disclose any grand-jury matter involving foreign intelligence, counterintelligence (as defined in 50 U.S.C. § 401a), or foreign intelligence information (as defined in Rule 6(e)(3)(D)(iii)) to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist the official receiving the information in the performance of that official's duties. An attorney for the government may also disclose any grand-jury matter involving, within the United States or elsewhere, a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage or terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by its agent, to any appropriate federal, state, state subdivision, Indian tribal, or foreign government official, for the purpose of preventing or responding to such threat or activities. (i) Any official who receives information under Rule 6(e)(3)(D) may use the information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Any state, state subdivision, Indian tribal, or foreign government official who receives information under Rule 6(e)(3)(D) may use the information only in a manner consistent with such guidelines as the Attorney General and the Director of National Intelligence shall jointly issue. (ii) Within a reasonable time after disclosure is made under Rule 6(e)(3)(D), an attorney for the government must file, under seal, a notice with the court in the district where the grand jury convened stating that such information was disclosed and the departments, agencies, or entities to which the disclosure was made. (iii) As used in Rule 6(e)(3)(D), the term "foreign intelligence information" means:

[59] *United States Code*: http://www.law.cornell.edu/uscode/ See also: http://uscode.house.gov/download/ascii.shtml
[60] *United States Federal Rules of Criminal Procedure*: http://www.law.cornell.edu/rules/frcrmp/

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(a) information, whether or not it concerns a United States person, that relates to the ability of the United States to protect against— • actual or potential attack or other grave hostile acts of a foreign power or its agent; • sabotage or international terrorism by a foreign power or its agent; or • clandestine intelligence activities by an intelligence service or network of a foreign power or by its agent; or (b) information, whether or not it concerns a United States person, with respect to a foreign power or foreign territory that relates to— • the national defense or the security of the United States; or • the conduct of the foreign affairs of the United States. (E) The court may authorize disclosure—at a time, in a manner, and subject to any other conditions that it directs—of a grand-jury matter: (i) preliminarily to or in connection with a judicial proceeding; (ii) at the request of a defendant who shows that a ground may exist to dismiss the indictment because of a matter that occurred before the grand jury; (iii) at the request of the government, when sought by a foreign court or prosecutor for use in an official criminal investigation; (iv) at the request of the government if it shows that the matter may disclose a violation of state or Indian tribal criminal law, as long as the disclosure is to an appropriate state, state-subdivision, or Indian tribal official for the purpose of enforcing that law; or (v) at the request of the government if it shows that the matter may disclose a violation of military criminal law under the Uniform Code of Military Justice, as long as the disclosure is to an appropriate military official for the purpose of enforcing that law. (F) A petition to disclose a grand-jury matter under Rule 6(e)(3)(E)(i) must be filed in the district where the grand jury convened. Unless the hearing is ex parte—as it may be when the government is the petitioner—the petitioner must serve the petition on, and the court must afford a reasonable opportunity to appear and be heard to: (i) an attorney for the government; (ii) the parties to the judicial proceeding; and (iii) any other person whom the court may designate. (G) If the petition to disclose arises out of a judicial proceeding in another district, the petitioned court must transfer the petition to the other court unless the petitioned court can reasonably determine whether disclosure is proper. If the petitioned court decides to transfer, it must send to the transferee court the material sought to be disclosed, if feasible, and a written evaluation of the need for continued grand-jury secrecy. The transferee court must afford those persons identified in Rule 6(e)(3)(F) a reasonable opportunity to appear and be heard.
"*Material witness arrest process*"	MATERIAL WITNESS ARREST PROCESS: US federal law enforcement officials can use the material witness arrest process to arrest a witness in order to secure his testimony in a criminal proceeding. The provisions governing the material witness arrest process are found in Chapter 207, Title 18, of the *United States Code* (*US Code*). A warrant is required before a person can be arrested pursuant to the material witness arrest process (section 3144). A person arrested under the material witness arrest process must be brought before a judge for a detention review as soon as possible. The judge will decide whether or not to release this person or to continue his or her detention (section 3142). There is a judicial presumption in favour of release, unless there is probable cause to believe the person has committed certain types of serious federal offences, one of which is the federal crime of terrorism (section 3142(a), (b), (e) and (f)). If the person is released, the judge may impose conditions on the release (section3142(c)). If the judge affirms the continued detention of the person, he or she may be held as long as his or her testimony is needed for criminal proceedings, which could mean detention until a trial is completed. As indicated previously, the material witness arrest process predates the enactment of the *USA Patriot Act*, but the events of 11 September 2001 appears to have changed how this investigative tool in being used. Since September 2001, approximately 70 individuals, primarily Muslim men, have been detained so as to facilitate the investigation of terrorism crimes. For additional information see: *Briefing Book—Recent Developments in Anti-terrorism Law and Policy in the United Kingdom, United States, Australia and France*, Prepared for the Special Senate Committee on Anti-terrorism, Legal and Legislative Affairs Division, Parliamentary Information and Research Service, Library of Parliament (Canada), 5 August 2010, at p. 5 and note 24; and Jennifer WISPINSKI, *The USA Patriot Act and Canada's Anti-Terrorism Act: Key Differences in Legislative Approach*, Parliamentary Information and Research Service, Library of Parliament (Canada), 31 March 2008. The most relevant provisions governing the material witness arrest process read as follows: ***United States Code*[61]:** **Sec. 3144. Release or detention of a material witness** If it appears from an affidavit filed by a party that the testimony of a person is material in a criminal proceeding, and if it is shown that it may become impracticable to secure the presence of the person by subpoena, a judicial officer may order the arrest of the person and treat the person in accordance with the provisions of section 3142 of this title. No material witness may be detained because of inability to comply with any condition of release if the testimony of such witness can adequately be secured by deposition, and if further detention is not necessary to prevent a failure of justice. Release of a material witness may be delayed for a reasonable period of time until the deposition of the witness can be taken pursuant to the Federal Rules of Criminal Procedure. **Sec. 3142. Release or detention of a defendant pending trial** (a) In General.— Upon the appearance before a judicial officer of a person charged with an offense, the judicial officer shall issue an order that, pending trial, the person be— (1) released on personal recognizance or upon execution of an unsecured appearance bond, under subsection (b) of this section;

[61] *United States Code*: http://www.law.cornell.edu/uscode/ See also: http://uscode.house.gov/download/ascii.shtml

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(2) released on a condition or combination of conditions under subsection (c) of this section;
(3) temporarily detained to permit revocation of conditional release, deportation, or exclusion under subsection (d) of this section; or
(4) detained under subsection (e) of this section.
(b) Release on Personal Recognizance or Unsecured Appearance Bond.— The judicial officer shall order the pretrial release of the person on personal recognizance, or upon execution of an unsecured appearance bond in an amount specified by the court, subject to the condition that the person not commit a Federal, State, or local crime during the period of release and subject to the condition that the person cooperate in the collection of a DNA sample from the person if the collection of such a sample is authorized pursuant to section 3 of the DNA Analysis Backlog Elimination Act of 2000 (42 U.S.C. 14135a), unless the judicial officer determines that such release will not reasonably assure the appearance of the person as required or will endanger the safety of any other person or the community.
(c) Release on Conditions.—
(1) If the judicial officer determines that the release described in subsection (b) of this section will not reasonably assure the appearance of the person as required or will endanger the safety of any other person or the community, such judicial officer shall order the pretrial release of the person—
(A) subject to the condition that the person not commit a Federal, State, or local crime during the period of release and subject to the condition that the person cooperate in the collection of a DNA sample from the person if the collection of such a sample is authorized pursuant to section 3 of the DNA Analysis Backlog Elimination Act of 2000 (42 U.S.C. 14135a); and
(B) subject to the least restrictive further condition, or combination of conditions, that such judicial officer determines will reasonably assure the appearance of the person as required and the safety of any other person and the community, which may include the condition that the person—
(i) remain in the custody of a designated person, who agrees to assume supervision and to report any violation of a release condition to the court, if the designated person is able reasonably to assure the judicial officer that the person will appear as required and will not pose a danger to the safety of any other person or the community;
(ii) maintain employment, or, if unemployed, actively seek employment;
(iii) maintain or commence an educational program;
(iv) abide by specified restrictions on personal associations, place of abode, or travel;
(v) avoid all contact with an alleged victim of the crime and with a potential witness who may testify concerning the offense;
(vi) report on a regular basis to a designated law enforcement agency, pretrial services agency, or other agency;
(vii) comply with a specified curfew;
(viii) refrain from possessing a firearm, destructive device, or other dangerous weapon;
(ix) refrain from excessive use of alcohol, or any use of a narcotic drug or other controlled substance, as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802), without a prescription by a licensed medical practitioner;
(x) undergo available medical, psychological, or psychiatric treatment, including treatment for drug or alcohol dependency, and remain in a specified institution if required for that purpose;
(xi) execute an agreement to forfeit upon failing to appear as required, property of a sufficient unencumbered value, including money, as is reasonably necessary to assure the appearance of the person as required, and shall provide the court with proof of ownership and the value of the property along with information regarding existing encumbrances as the judicial office may require;
(xii) execute a bail bond with solvent sureties; who will execute an agreement to forfeit in such amount as is reasonably necessary to assure appearance of the person as required and shall provide the court with information regarding the value of the assets and liabilities of the surety if other than an approved surety and the nature and extent of encumbrances against the surety's property; such surety shall have a net worth which shall have sufficient unencumbered value to pay the amount of the bail bond;
(xiii) return to custody for specified hours following release for employment, schooling, or other limited purposes; and
(xiv) satisfy any other condition that is reasonably necessary to assure the appearance of the person as required and to assure the safety of any other person and the community.
In any case that involves a minor victim under section 1201, 1591, 2241, 2242, 2244 (a)(1), 2245, 2251, 2251A, 2252 (a)(1), 2252 (a)(2), 2252 (a)(3), 2252A (a)(1), 2252A (a)(2), 2252A (a)(3), 2252A (a)(4), 2260, 2421, 2422, 2423, or 2425 of this title, or a failure to register offense under section 2250 of this title, any release order shall contain, at a minimum, a condition of electronic monitoring and each of the conditions specified at subparagraphs (iv), (v), (vi), (vii), and (viii).
(2) The judicial officer may not impose a financial condition that results in the pretrial detention of the person.
(3) The judicial officer may at any time amend the order to impose additional or different conditions of release.
(d) Temporary Detention To Permit Revocation of Conditional Release, Deportation, or Exclusion.— If the judicial officer determines that—
(1) such person—
(A) is, and was at the time the offense was committed, on—
(i) release pending trial for a felony under Federal, State, or local law;
(ii) release pending imposition or execution of sentence, appeal of sentence or conviction, or completion of sentence, for any offense under Federal, State, or local law; or
(iii) probation or parole for any offense under Federal, State, or local law; or
(B) is not a citizen of the United States or lawfully admitted for permanent residence, as defined in section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101 (a)(20)); and
(2) such person may flee or pose a danger to any other person or the community;
such judicial officer shall order the detention of such person, for a period of not more than ten days, excluding Saturdays, Sundays, and holidays, and direct the attorney for the Government to notify the appropriate court, probation or parole official, or State or local law enforcement official, or the appropriate official of the Immigration and Naturalization Service. If the official fails or declines to take such person into custody during that period, such person shall be treated in accordance with the other provisions of this section, notwithstanding the applicability of other provisions of law governing release pending trial or deportation or exclusion proceedings. If temporary detention is sought under paragraph (1)(B) of this subsection, such person has the burden of proving to

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

the court such person's United States citizenship or lawful admission for permanent residence.
(e) Detention.—
(1) If, after a hearing pursuant to the provisions of subsection (f) of this section, the judicial officer finds that no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of any other person and the community, such judicial officer shall order the detention of the person before trial.
(2) In a case described in subsection (f)(1) of this section, a rebuttable presumption arises that no condition or combination of conditions will reasonably assure the safety of any other person and the community if such judicial officer finds that—
(A) the person has been convicted of a Federal offense that is described in subsection (f)(1) of this section, or of a State or local offense that would have been an offense described in subsection (f)(1) of this section if a circumstance giving rise to Federal jurisdiction had existed;
(B) the offense described in subparagraph (A) was committed while the person was on release pending trial for a Federal, State, or local offense; and
(C) a period of not more than five years has elapsed since the date of conviction, or the release of the person from imprisonment, for the offense described in subparagraph (A), whichever is later.
(3) Subject to rebuttal by the person, it shall be presumed that no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of the community if the judicial officer finds that there is probable cause to believe that the person committed—
(A) an offense for which a maximum term of imprisonment of ten years or more is prescribed in the Controlled Substances Act (21 U.S.C. 801 et seq.), the Controlled Substances Import and Export Act (21 U.S.C. 951 et seq.), or chapter 705 of title 46;
(B) an offense under section 924 (c), 956 (a), or 2332b of this title;
(C) an offense listed in section 2332b (g)(5)(B) of title 18, United States Code, for which a maximum term of imprisonment of 10 years or more is prescribed;
(D) an offense under chapter 77 of this title for which a maximum term of imprisonment of 20 years or more is prescribed; or
(E) an offense involving a minor victim under section 1201, 1591, 2241, 2242, 2244 (a)(1), 2245, 2251, 2251A, 2252 (a)(1), 2252 (a)(2), 2252 (a)(3), 2252A (a)(1), 2252A (a)(2), 2252A (a)(3), 2252A (a)(4), 2260, 2421, 2422, 2423, or 2425 of this title.
(f) Detention Hearing.— The judicial officer shall hold a hearing to determine whether any condition or combination of conditions set forth in subsection (c) of this section will reasonably assure the appearance of such person as required and the safety of any other person and the community—
(1) upon motion of the attorney for the Government, in a case that involves—
(A) a crime of violence, a violation of section 1591, or an offense listed in section 2332b (g)(5)(B) for which a maximum term of imprisonment of 10 years or more is prescribed;
(B) an offense for which the maximum sentence is life imprisonment or death;
(C) an offense for which a maximum term of imprisonment of ten years or more is prescribed in the Controlled Substances Act (21 U.S.C. 801 et seq.), the Controlled Substances Import and Export Act (21 U.S.C. 951 et seq.), or chapter 705 of title 46;
(D) any felony if such person has been convicted of two or more offenses described in subparagraphs (A) through (C) of this paragraph, or two or more State or local offenses that would have been offenses described in subparagraphs (A) through (C) of this paragraph if a circumstance giving rise to Federal jurisdiction had existed, or a combination of such offenses; or
(E) any felony that is not otherwise a crime of violence that involves a minor victim or that involves the possession or use of a firearm or destructive device (as those terms are defined in section 921), or any other dangerous weapon, or involves a failure to register under section 2250 of title 18, United States Code; or
(2) upon motion of the attorney for the Government or upon the judicial officer's own motion in a case, that involves—
(A) a serious risk that such person will flee; or
(B) a serious risk that such person will obstruct or attempt to obstruct justice, or threaten, injure, or intimidate, or attempt to threaten, injure, or intimidate, a prospective witness or juror.
The hearing shall be held immediately upon the person's first appearance before the judicial officer unless that person, or the attorney for the Government, seeks a continuance. Except for good cause, a continuance on motion of such person may not exceed five days (not including any intermediate Saturday, Sunday, or legal holiday), and a continuance on motion of the attorney for the Government may not exceed three days (not including any intermediate Saturday, Sunday, or legal holiday). During a continuance, such person shall be detained, and the judicial officer, on motion of the attorney for the Government or sua sponte, may order that, while in custody, a person who appears to be a narcotics addict receive a medical examination to determine whether such person is an addict. At the hearing, such person has the right to be represented by counsel, and, if financially unable to obtain adequate representation, to have counsel appointed. The person shall be afforded an opportunity to testify, to present witnesses, to cross-examine witnesses who appear at the hearing, and to present information by proffer or otherwise. The rules concerning admissibility of evidence in criminal trials do not apply to the presentation and consideration of information at the hearing. The facts the judicial officer uses to support a finding pursuant to subsection (e) that no condition or combination of conditions will reasonably assure the safety of any other person and the community shall be supported by clear and convincing evidence. The person may be detained pending completion of the hearing. The hearing may be reopened, before or after a determination by the judicial officer, at any time before trial if the judicial officer finds that information exists that was not known to the movant at the time of the hearing and that has a material bearing on the issue whether there are conditions of release that will reasonably assure the appearance of such person as required and the safety of any other person and the community.
(g) Factors To Be Considered.— The judicial officer shall, in determining whether there are conditions of release that will reasonably assure the appearance of the person as required and the safety of any other person and the community, take into account the available information concerning—
(1) the nature and circumstances of the offense charged, including whether the offense is a crime of violence, a violation of section 1591, a Federal crime of terrorism, or involves a minor victim or a controlled substance, firearm, explosive, or destructive device;
(2) the weight of the evidence against the person;
(3) the history and characteristics of the person, including—
(A) the person's character, physical and mental condition, family ties, employment, financial resources, length of residence in the community, community ties, past conduct, history relating to drug

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	or alcohol abuse, criminal history, and record concerning appearance at court proceedings; and (B) whether, at the time of the current offense or arrest, the person was on probation, on parole, or on other release pending trial, sentencing, appeal, or completion of sentence for an offense under Federal, State, or local law; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the person's release. In considering the conditions of release described in subsection (c)(1)(B)(xi) or (c)(1)(B)(xii) of this section, the judicial officer may upon his own motion, or shall upon the motion of the Government, conduct an inquiry into the source of the property to be designated for potential forfeiture or offered as collateral to secure a bond, and shall decline to accept the designation, or the use as collateral, of property that, because of its source, will not reasonably assure the appearance of the person as required. (h) Contents of Release Order.— In a release order issued under subsection (b) or (c) of this section, the judicial officer shall— (1) include a written statement that sets forth all the conditions to which the release is subject, in a manner sufficiently clear and specific to serve as a guide for the person's conduct; and (2) advise the person of— (A) the penalties for violating a condition of release, including the penalties for committing an offense while on pretrial release; (B) the consequences of violating a condition of release, including the immediate issuance of a warrant for the person's arrest; and (C) sections 1503 of this title (relating to intimidation of witnesses, jurors, and officers of the court), 1510 (relating to obstruction of criminal investigations), 1512 (tampering with a witness, victim, or an informant), and 1513 (retaliating against a witness, victim, or an informant). (i) Contents of Detention Order.— In a detention order issued under subsection (e) of this section, the judicial officer shall— (1) include written findings of fact and a written statement of the reasons for the detention; (2) direct that the person be committed to the custody of the Attorney General for confinement in a corrections facility separate, to the extent practicable, from persons awaiting or serving sentences or being held in custody pending appeal; (3) direct that the person be afforded reasonable opportunity for private consultation with counsel; and (4) direct that, on order of a court of the United States or on request of an attorney for the Government, the person in charge of the corrections facility in which the person is confined deliver the person to a United States marshal for the purpose of an appearance in connection with a court proceeding. The judicial officer may, by subsequent order, permit the temporary release of the person, in the custody of a United States marshal or another appropriate person, to the extent that the judicial officer determines such release to be necessary for preparation of the person's defense or for another compelling reason. (j) Presumption of Innocence.— Nothing in this section shall be construed as modifying or limiting the presumption of innocence.
"*FISA surveillance orders*"	FISA SURVEILLANCE ORDERS: Section 218 of the *USA Patriot Act* and section 104 of the *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008* allow federal officials to apply for surveillance orders under the *Foreign Intelligence Surveillance Act* (FISA) when gathering foreign intelligence is "a significant" reason for the order rather than "the" reason, which was the case prior to the enactment of the *USA Patriot Act* (see section 1804(a)(7)(B) of the *US Code* hereinafter). This means that FISA surveillance orders could be used in criminal investigations, as long as they have a foreign intelligence aspect to them. As a general matter, the test one has to meet in order to get a FISA order is less stringent than the test one has to meet to obtain an order under Title III of the *US Code*, which is the type of surveillance order usually required when one is investigating a serious crime. The FISA is contained in Chapter 36, Title 50 of the *US Code*. **Sec. 1804. Applications for court orders** (a) Submission by Federal officer; approval of Attorney General; contents Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include— (1) the identity of the Federal officer making the application; (2) the identity, if known, or a description of the specific target of the electronic surveillance; (3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that— (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power; (4) a statement of the proposed minimization procedures; (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance; (6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official— (A) that the certifying official deems the information sought to be foreign intelligence information; (B) that a significant purpose of the surveillance is to obtain foreign intelligence information; (C) that such information cannot reasonably be obtained by normal investigative techniques; (D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801 (e) of this title; and (E) including a statement of the basis for the certification that—

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(i) the information sought is the type of foreign intelligence information designated; and (ii) such information cannot reasonably be obtained by normal investigative techniques; (7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance; (8) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application; and (9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter. (b) Additional affidavits or certifications The Attorney General may require any other affidavit or certification from any other officer in connection with the application. (c) Additional information The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title. (d) Personal review by Attorney General (1) (A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) of this section an application under that subsection for a target described in section 1801 (b)(2) of this title. (B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph. (C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request. (2) (A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) of this section for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination. (B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) of this section for purposes of making the application under this section. (C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.
"*Roving FISA orders*"	ROVING FISA ORDERS: Section 206 of the *USA Patriot Act* and section 105 of the *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008* allow intelligence officials to obtain a roving order to target a person rather than a specific phone. Consequently, the officials need not obtain anymore a separate order for every telephone or device they wish to tap; they can obtain a global order permitting them to tap multiple devices belonging to a single individual. In accordance with the amended *Foreign Intelligence Surveillance Act* (FISA), found in Chapter 36, Title 50 of the *United States Code*, to obtain a roving FISA order, the court must be satisfied that the target is a "foreign power" (see the definition in section 1801 of the *US Code*) and that the actions of the target may have the effect of thwarting surveillance. **Sec. 1805. Issuance of order** (a) Necessary findings Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that— (1) the application has been made by a Federal officer and approved by the Attorney General; (2) on the basis of the facts submitted by the applicant there is probable cause to believe that— (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power; (3) the proposed minimization procedures meet the definition of minimization procedures under section 1801 (h) of this title; and (4) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804 (a)(7)(E) of this title and any other information furnished under section 1804 (d) of this title.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(b) Determination of probable cause
In determining whether or not probable cause exists for purposes of an order under subsection (a)(2) of this section, a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.
(c) Specifications and directions of orders
(1) Specifications
An order approving an electronic surveillance under this section shall specify—
(A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 1804 (a)(3) of this title;
(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;
(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and
(E) the period of time during which the electronic surveillance is approved.
(2) Directions
An order approving an electronic surveillance under this section shall direct—
(A) that the minimization procedures be followed;
(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;
(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and
(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.
(3) Special directions for certain orders
An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of—
(A) the nature and location of each new facility or place at which the electronic surveillance is directed;
(B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;
(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and
(D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.
(d) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated
(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that
(A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801 (a)(1), (2), or (3) of this title, for the period specified in the application or for one year, whichever is less, and
(B) an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.
(2) Extensions of an order issued under this subchapter may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that
(A) an extension of an order under this chapter for a surveillance targeted against a foreign power, as defined in paragraph (5), (6), or (7) of section 1801 (a) of this title, or against a foreign power as defined in section 1801 (a)(4) of this title that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and
(B) an extension of an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed 1 year.
(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.
(e) Emergency orders
(1) Notwithstanding any other provision of this subchapter, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General—
(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;
(B) reasonably determines that the factual basis for the issuance of an order under this subchapter to approve such electronic surveillance exists;
(C) informs, either personally or through a designee, a judge having jurisdiction under section 1803 of this title at the time of such authorization that the decision has been made to employ

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	emergency electronic surveillance; and (D) makes an application in accordance with this subchapter to a judge having jurisdiction under section 1803 of this title as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance. (2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed. (3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest. (4) A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title. (5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. (6) The Attorney General shall assess compliance with the requirements of paragraph (5). (f) Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel Notwithstanding any other provision of this subchapter, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to— (1) test the capability of electronic equipment, if— (A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance; (B) the test is limited in extent and duration to that necessary to determine the capability of the equipment; (C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and: (D) Provided, That the test may exceed ninety days only with the prior approval of the Attorney General; (2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if— (A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance; (B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and (C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, or section 605 of title 47, or to protect information from unauthorized surveillance; or (3) train intelligence personnel in the use of electronic surveillance equipment, if— (A) it is not reasonable to— (i) obtain the consent of the persons incidentally subjected to the surveillance; (ii) train persons in the course of surveillances otherwise authorized by this subchapter; or (iii) train persons in the use of such equipment without engaging in electronic surveillance; (B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and (C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible. (g) Retention of certifications, applications and orders Certifications made by the Attorney General pursuant to section 1802 (a) of this title and applications made and orders granted under this subchapter shall be retained for a period of at least ten years from the date of the certification or application. (h) Bar to legal action No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this chapter for electronic surveillance or physical search. (i) Pen registers and trap and trace devices In any case in which the Government makes an application to a judge under this subchapter to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 1842 (d)(2) of this title.
"*Interception of wire, oral, or electronic communications*"	OTHER INVESTIGATIVE POWERS RELATED TO TERRORISM OFFENCES FOUND IN THE *US CODE* ARE FOR INSTANCE: **Sec. 2516. Authorization for interception of wire, oral, or electronic communications** (1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Disclosure and use of intercepted wire, oral, or electronic communications*"	judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of— […] (q) any criminal violation of section 229 (relating to chemical weapons) or section 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h [2] 2339, 2339A, 2339B, 2339C, or 2339D of this title (relating to terrorism); […] **Sec. 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications** […] (6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. […] THIS PROVISION IS TO BE READ IN CONJUNCTION WITH: **Sec. 2510. Definitions** As used in this chapter— (19) "foreign intelligence information", for purposes of section 2517 (6) of this title, means— (A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against— (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to— (i) the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States;
"*Required disclosure of customers communications or records*"	**Sec. 2703. Required disclosure of customer communications or records** […] (c) Records Concerning Electronic Communication Service or Remote Computing Service.— […] (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the— (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1). […]
"*Voluntary disclosure of customers communications or records*"	**Sec. 2702. Voluntary disclosure of customer communications or records** (a) Prohibitions.— Except as provided in subsection (b) or (c)— (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service— (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity. (b) Exceptions for disclosure of communications.— A provider described in subsection (a) may divulge the contents of a communication— (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; (2) as otherwise authorized in section 2517, 2511 (2)(a), or 2703 of this title; (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service; (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; (7) to a law enforcement agency— (A) if the contents— (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; or [(B) Repealed.] (8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency. (c) Exceptions for Disclosure of Customer Records.— A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))— (1) as otherwise authorized in section 2703; (2) with the lawful consent of the customer or subscriber; (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; (4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency; (5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or (6) to any person other than a governmental entity. (d) Reporting of Emergency Disclosures.— On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing— (1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and (2) a summary of the basis for disclosure in those instances where— (A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and (B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.
"*Powers of search and seizure*"	**Sec. 3103a. Additional grounds for issuing warrant** (a) In General.— In addition to the grounds for issuing a warrant in section 3103 of this title, a warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States. (b) Delay.— With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if— (1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial) [1] ; (2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and (3) the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay. THIS PROVISION IS TO BE READ IN CONJUNCTION WITH: **Sec. 2705. Delayed notice** (a) Delay of Notification.— […]

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(2) An adverse result for the purposes of paragraph (1) of this subsection is— (A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial. […]
United Kingdom "*Terrorist investigation (definition)*" "*Police cordons*" "*Arrest without warrant*"	***Terrorism Act 2000***[62]**:** **Sec. 32 Terrorist investigation** In this Act "terrorist investigation" means an investigation of— (a) the commission, preparation or instigation of acts of terrorism, (b) an act which appears to have been done for the purposes of terrorism, (c) the resources of a proscribed organisation, (d) the possibility of making an order under section 3(3), or (e) the commission, preparation or instigation of an offence under this Act or under Part 1 of the Terrorism Act 2006 other than an offence under section 1 or 2 of that Act]. **Sec. 36 Police powers** (1) A constable in uniform may— (a) order a person in a cordoned area to leave it immediately; (b) order a person immediately to leave premises which are wholly or partly in or adjacent to a cordoned area; (c) order the driver or person in charge of a vehicle in a cordoned area to move it from the area immediately; (d) arrange for the removal of a vehicle from a cordoned area; (e) arrange for the movement of a vehicle within a cordoned area; (f) prohibit or restrict access to a cordoned area by pedestrians or vehicles. (2) A person commits an offence if he fails to comply with an order, prohibition or restriction imposed by virtue of subsection (1). (3) It is a defence for a person charged with an offence under subsection (2) to prove that he had a reasonable excuse for his failure. (4) A person guilty of an offence under subsection (2) shall be liable on summary conviction to— (a) imprisonment for a term not exceeding three months, (b) a fine not exceeding level 4 on the standard scale, or (c) both. ***Sec.* 41 Arrest without warrant*** (1) A constable may arrest without a warrant a person whom he reasonably suspects to be a terrorist. (2) Where a person is arrested under this section the provisions of Schedule 8 (detention: treatment, review and extension) shall apply. (3) Subject to subsections (4) to (7), a person detained under this section shall (unless detained under any other power) be released not later than the end of the period of 48 hours beginning— (a) with the time of his arrest under this section, or (b) if he was being detained under Schedule 7 when he was arrested under this section, with the time when his examination under that Schedule began. (4) If on a review of a person's detention under Part II of Schedule 8 the review officer does not authorise continued detention, the person shall (unless detained in accordance with subsection (5) or (6) or under any other power) be released. (5) Where a police officer intends to make an application for a warrant under paragraph 29 of Schedule 8 extending a person's detention, the person may be detained pending the making of the application. (6) Where an application has been made under paragraph 29 or 36 of Schedule 8 in respect of a person's detention, he may be detained pending the conclusion of proceedings on the application. (7) Where an application under paragraph 29 or 36 of Schedule 8 is granted in respect of a person's detention, he may be detained, subject to paragraph 37 of that Schedule, during the period specified in the warrant. (8) The refusal of an application in respect of a person's detention under paragraph 29 or 36 of Schedule 8 shall not prevent his continued detention in accordance with this section. (9) A person who has the powers of a constable in one Part of the United Kingdom may exercise the power under subsection (1) in any Part of the United Kingdom.

[62] UK *Terrorism Act 2000* (as amended by the *Terrorism Act 2006* and the *Criminal Justice Act 2003*): http://www.legislation.gov.uk/ukpga/2000/11/contents

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	** With respect to section 41 and Schedule 8, please refer to Chart e.2 under the Title (e) of the research,* infra*, relating to UK anti-terrorism legislation proposed but not yet enacted.*
"*Search of premises*"	**Sec. 42 Search of premises** (1) A justice of the peace may on the application of a constable issue a warrant in relation to specified premises if he is satisfied that there are reasonable grounds for suspecting that a person whom the constable reasonably suspects to be a person falling within section 40(1)(b) is to be found there. (2) A warrant under this section shall authorise any constable to enter and search the specified premises for the purpose of arresting the person referred to in subsection (1) under section 41. (3) In the application of subsection (1) to Scotland— (a) "justice of the peace" includes the sheriff, and (b) the justice of the peace or sheriff can be satisfied as mentioned in that subsection only by having heard evidence on oath.
"*Search of persons*"	**Sec. 43 Search of persons** (1) A constable may stop and search a person whom he reasonably suspects to be a terrorist to discover whether he has in his possession anything which may constitute evidence that he is a terrorist. (2) A constable may search a person arrested under section 41 to discover whether he has in his possession anything which may constitute evidence that he is a terrorist. (3) A search of a person under this section must be carried out by someone of the same sex. (4) A constable may seize and retain anything which he discovers in the course of a search of a person under subsection (1) or (2) and which he reasonably suspects may constitute evidence that the person is a terrorist. (5) A person who has the powers of a constable in one Part of the United Kingdom may exercise a power under this section in any Part of the United Kingdom.
"*Stop and search (vehicles and persons)*"	**Sec. 44 Authorisations**[**] (1) An authorisation under this subsection authorises any constable in uniform to stop a vehicle in an area or at a place specified in the authorisation and to search— (a) the vehicle; (b) the driver of the vehicle; (c) a passenger in the vehicle; (d) anything in or on the vehicle or carried by the driver or a passenger. (2) An authorisation under this subsection authorises any constable in uniform to stop a pedestrian in an area or at a place specified in the authorisation and to search— (a) the pedestrian; (b) anything carried by him. (3) An authorisation under subsection (1) or (2) may be given only if the person giving it considers it expedient for the prevention of acts of terrorism. (4) An authorisation may be given— (a) where the specified area or place is the whole or part of a police area outside Northern Ireland other than one mentioned in paragraph (b) or (c), by a police officer for the area who is of at least the rank of assistant chief constable; (b) where the specified area or place is the whole or part of the metropolitan police district, by a police officer for the district who is of at least the rank of commander of the metropolitan police; (c) where the specified area or place is the whole or part of the City of London, by a police officer for the City who is of at least the rank of commander in the City of London police force; (d) where the specified area or place is the whole or part of Northern Ireland, by a member of the Royal Ulster Constabulary who is of at least the rank of assistant chief constable. (4ZA) The power of a person mentioned in subsection (4) to give an authorisation specifying an area or place so mentioned includes power to give such an authorisation specifying such an area or place together with— (a) the internal waters adjacent to that area or place; or (b) such area of those internal waters as is specified in the authorisation. (4A) In a case (within subsection (4)(a), (b) or (c) in which the specified area or place is in a place described in section 34(1A), an authorisation may also be given by a member of the British Transport Police Force who is of at least the rank of assistant chief constable. (4B) In a case in which the specified area or place is a place to which section 2(2) of the Ministry of Defence Police Act 1987 applies, an authorisation may also be given by a member of the Ministry of Defence Police who is of at least the rank of assistant chief constable. (4BA) In a case in which the specified area or place is a place in which members of the Civil Nuclear Constabulary have the powers and privileges of a constable, an authorisation may also be given by a member of that Constabulary who is of at least the rank of assistant chief constable. (4C) But an authorisation may not be given by— (a) a member of the British Transport Police Force, (b) a member of the Ministry of Defence Police, or (c) a member of the Civil Nuclear Constabulary, in any other case.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(5) If an authorisation is given orally, the person giving it shall confirm it in writing as soon as is reasonably practicable.
(5A) In this section—
"driver", in relation to an aircraft, hovercraft or vessel, means the captain, pilot or other person with control of the aircraft, hovercraft or vessel or any member of its crew and, in relation to a train, includes any member of its crew;
"internal waters" means waters in the United Kingdom that are not comprised in any police area.

Sec. 45 Exercise of power**
(1) The power conferred by an authorisation under section 44(1) or (2)—
(a) may be exercised only for the purpose of searching for articles of a kind which could be used in connection with terrorism, and
(b) may be exercised whether or not the constable has grounds for suspecting the presence of articles of that kind.
(2) A constable may seize and retain an article which he discovers in the course of a search by virtue of section 44(1) or (2) and which he reasonably suspects is intended to be used in connection with terrorism.
(3) A constable exercising the power conferred by an authorisation may not require a person to remove any clothing in public except for headgear, footwear, an outer coat, a jacket or gloves.
(4) Where a constable proposes to search a person or vehicle by virtue of section 44(1) or (2) he may detain the person or vehicle for such time as is reasonably required to permit the search to be carried out at or near the place where the person or vehicle is stopped.
(5) Where—
(a) a vehicle or pedestrian is stopped by virtue of section 44(1) or (2), and
(b) the driver of the vehicle or the pedestrian applies for a written statement that the vehicle was stopped, or that he was stopped, by virtue of section 44(1) or (2),
the written statement shall be provided.
(6) An application under subsection (5) must be made within the period of 12 months beginning with the date on which the vehicle or pedestrian was stopped.
(7) In this section "driver" has the same meaning as in section 44.

Sec. 46 Duration of authorisation**
(1) An authorisation under section 44 has effect, subject to subsections (2) to (7), during the period—
(a) beginning at the time when the authorisation is given, and
(b) ending with a date or at a time specified in the authorisation.
(2) The date or time specified under subsection (1)(b) must not occur after the end of the period of 28 days beginning with the day on which the authorisation is given.
(2A) An authorisation under section 44(4BA) does not have effect except in relation to times when the specified area or place is a place where members of the Civil Nuclear Constabulary have the powers and privileges of a constable.
(3) The person who gives an authorisation shall inform the Secretary of State as soon as is reasonably practicable.
(4) If an authorisation is not confirmed by the Secretary of State before the end of the period of 48 hours beginning with the time when it is given—
(a) it shall cease to have effect at the end of that period, but
(b) its ceasing to have effect shall not affect the lawfulness of anything done in reliance on it before the end of that period.
(5) Where the Secretary of State confirms an authorisation he may substitute an earlier date or time for the date or time specified under subsection (1)(b).
(6) The Secretary of State may cancel an authorisation with effect from a specified time.
(7) An authorisation may be renewed in writing by the person who gave it or by a person who could have given it; and subsections (1) to (6) shall apply as if a new authorisation were given on each occasion on which the authorisation is renewed.

Sec. 47 Offences**
(1) A person commits an offence if he—
(a) fails to stop a vehicle when required to do so by a constable in the exercise of the power conferred by an authorisation under section 44(1);
(b) fails to stop when required to do so by a constable in the exercise of the power conferred by an authorisation under section 44(2);
(c) wilfully obstructs a constable in the exercise of the power conferred by an authorisation under section 44(1) or (2).
(2) A person guilty of an offence under this section shall be liable on summary conviction to—
(a) imprisonment for a term not exceeding six months,
(b) a fine not exceeding level 5 on the standard scale, or
(c) both.

** *The European Court of Human Right has ruled that the stop and search power contained in sections 44 to 47 of the* Terrorism Act 2000 *violated Article 8 (privacy and family life) of the* European Convention on Human Rights *(*ECHR*). In order to put the stop and search powers into line with the* ECHR*, the UK Parliament enacted the* Terrorism Act 2000 (Remedial Order) 2011*, which entered into force on 18 March 2011 (i.e. after 1 February 2011). The remedial order replaces sections 44 to 47 of the* Terrorism Act 2000 *with a more targeted and proportionate power. The*

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Prohibition of the parking of vehicles*"	*provisions of the* Remedial Order *will cease to have effect on the coming into force of the similar provisions provided in the* Protection of Freedoms Bill *that is currently being taken through the UK Parliament. For greater details, please refer to the Title (e) of the research,* infra. **Sec. 48 Authorisations** (1) An authorisation under this section authorises any constable in uniform to prohibit or restrict the parking of vehicles on a road specified in the authorisation. (2) An authorisation may be given only if the person giving it considers it expedient for the prevention of acts of terrorism. (3) An authorisation may be given— (a) where the road specified is outside Northern Ireland and is wholly or partly within a police area other than one mentioned in paragraphs (b) or (c), by a police officer for the area who is of at least the rank of assistant chief constable; (b) where the road specified is wholly or partly in the metropolitan police district, by a police officer for the district who is of at least the rank of commander of the metropolitan police; (c) where the road specified is wholly or partly in the City of London, by a police officer for the City who is of at least the rank of commander in the City of London police force; (d) where the road specified is in Northern Ireland, by a member of the Royal Ulster Constabulary who is of at least the rank of assistant chief constable. (4) If an authorisation is given orally, the person giving it shall confirm it in writing as soon as is reasonably practicable. [*Please also refer to* Terrorism Act 2000*, sections 49 to 51 on Execution of power, Duration of authorization, and related Offences*].
Australia "*Requirement to provide name*" "*Stopping and searching*"	***Crimes Act 1914***[63]**:** POWERS **Sec. 3UC Requirement to provide name etc.** (1) A police officer may request the person to provide the officer with the following details: (a) the person's name; (b) the person's residential address; (c) the person's reason for being in that particular Commonwealth place; (d) evidence of the person's identity. (2) If a police officer: (a) makes a request under subsection (1); and (b) informs the person: (i) of the officer's authority to make the request; and (ii) that it may be an offence not to comply with the request; the person commits an offence if: (c) the person fails to comply with the request; or (d) the person gives a name or address that is false in a material particular. Penalty: 20 penalty units. (3) Subsection (2) does not apply if the person has a reasonable excuse. **Sec. 3UD Stopping and searching** (1) A police officer may: (a) stop and detain the person for the purpose of conducting a search under paragraph (b); and (b) conduct one of the following searches for a terrorism related item: (i) an ordinary search or a frisk search of the person; (ii) a search of any thing that is, or that the officer suspects on reasonable grounds to be, under the person's immediate control; (iii) a search of any vehicle that is operated or occupied by the person; (iv) a search of any thing that the person has, or that the officer suspects on reasonable grounds that the person has, brought into the Commonwealth place. Conditions relating to conduct of search of person (2) A police officer who conducts a search of a person under this section must not use more force, or subject the person to greater indignity, than is reasonable and necessary in order to conduct the search.

[63] Australia *Crimes Act 1914*: http://www.comlaw.gov.au/Details/C2011C00233

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Seizure of terrorism related items*" "*Emergency entry to premises without warrant*"	(3) A person must not be detained under this section for longer than is reasonably necessary for a search to be conducted under this section. Other conditions relating to conduct of search of person or thing (4) In searching a thing (including a vehicle) under subsection (1), a police officer may use such force as is reasonable and necessary in the circumstances, but must not damage the thing by forcing it, or a part of it, open unless: (a) the person has been given a reasonable opportunity to open the thing or part of it; or (b) it is not possible to give that opportunity. **Sec. 3UE Seizure of terrorism related items and serious offence related items** If a police officer: (a) conducts a search under section 3UD; and (b) finds, in the course of the search, a thing that is: (i) a terrorism related item; or (ii) a serious offence related item; the officer may seize the thing. **Sec. 3UEA Emergency entry to premises without warrant** (1) A police officer may enter premises in accordance with this section if the police officer suspects, on reasonable grounds, that: (a) it is necessary to exercise a power under subsection (2) in order to prevent a thing that is on the premises from being used in connection with a terrorism offence; and (b) it is necessary to exercise the power without the authority of a search warrant because there is a serious and imminent threat to a person's life, health or safety. (2) The police officer may: (a) search the premises for the thing; and (b) seize the thing if he or she finds it there. (3) If, in the course of searching for the thing, the police officer finds another thing that the police officer suspects, on reasonable grounds, to be relevant to an indictable offence or a summary offence, the police officer may secure the premises pending the obtaining of a warrant under Part IAA in relation to the premises. (4) Premises must not be secured under subsection (3) for longer than is reasonably necessary to obtain the warrant. (5) In the course of searching for the thing, the police officer may also seize any other thing, or do anything to make the premises safe, if the police officer suspects, on reasonable grounds, that it is necessary to do so: (a) in order to protect a person's life, health or safety; and (b) without the authority of a search warrant because the circumstances are serious and urgent. (6) In exercising powers under this section: (a) the police officer may use such assistance; and (b) the police officer, or a person who is also a police officer and who is assisting the police officer, may use such force against persons and things; and (c) a person (other than a police officer) who is authorised by the police officer to assist the police officer may use such force against things; as is necessary and reasonable in the circumstances. Notification (7) If one or more police officers have entered premises in accordance with this section, a police officer must, within 24 hours after the entry: (a) notify the occupier of the premises that the entry has taken place; or (b) if it is not practicable so to notify the occupier—leave a written notice of the entry at the premises.
"*Applications for declarations of a security zone*"	PRESCRIBED SECURITY ZONES **Sec. 3UI Applications for declarations** A police officer may apply to the Minister for a declaration that a Commonwealth place be declared as a prescribed security zone. **Sec. 3UJ Minister may make declarations** Declaration (1) The Minister may declare, in writing, a Commonwealth place to be a prescribed security zone if he or she considers that a declaration would assist: (a) in preventing a terrorist act occurring; or (b) in responding to a terrorist act that has occurred. Declaration has effect (2) A declaration under this section has effect accordingly.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	Duration of declaration (3) A declaration ceases to have effect at the end of 28 days after it is made, unless the declaration is revoked by the Minister before then. Revocation of declaration (4) The Minister must revoke a declaration, in writing, if he or she is satisfied that: (a) in the case of a declaration made on the ground mentioned in paragraph (1)(a)—there is no longer a terrorism threat that justifies the declaration being continued; or (b) in the case of a declaration made on the ground mentioned in paragraph (1)(b)—the declaration is no longer required. Gazettal and publication of declaration (5) If a declaration of a Commonwealth place as a prescribed security zone under this section is made or revoked, the Minister must arrange for: (a) a statement to be prepared that: (i) states that the declaration has been made or revoked, as the case may be; and (ii) identifies the prescribed security zone; and (b) the statement to be: (i) broadcast by a television or radio station so as to be capable of being received within the place; and (ii) published in the Gazette; and (iii) published on the internet. Effect of failure to publish (6) A failure to comply with subsection (5) does not make the declaration or its revocation ineffective to any extent. Declaration or revocation not legislative instruments (7) A declaration or revocation made under this section is not a legislative instrument. POWER TO OBTAIN INFORMATION AND DOCUMENTS
"*Power to request information or documents from operators of aircraft or ships*"	**Sec. 3ZQM Power to request information or documents about terrorist acts from operators of aircraft or ships** (1) This section applies if an authorised AFP officer believes on reasonable grounds that an operator of an aircraft or ship has information or documents (including in electronic form) that are relevant to a matter that relates to the doing of a terrorist act (whether or not a terrorist act has occurred or will occur). (2) The officer may: (a) ask the operator questions relating to the aircraft or ship, or its cargo, crew, passengers, stores or voyage, that are relevant to the matter; or (b) request the operator to produce documents relating to the aircraft or ship, or its cargo, crew, passengers, stores or voyage: (i) that are relevant to the matter; and (ii) that are in the possession or under the control of the operator. (3) A person who is asked a question or requested to produce a document under subsection (2) must answer the question or produce the document as soon as practicable. Offence (4) A person commits an offence if: (a) the person is an operator of an aircraft or ship; and (b) the person is asked a question or requested to produce a document under subsection (2); and (c) the person fails to answer the question or produce the document. Penalty: 60 penalty units. (5) Subsection (4) is an offence of strict liability. (6) It is a defence to a prosecution for an offence against subsection (4) if the person charged had a reasonable excuse for: (a) failing to answer the question; or (b) failing to produce the document. Definitions (7) In this section: operator has the meaning given by section 4 of the Customs Act 1901.
"*Power to obtain documents relating to terrorism offences*"	**Sec. 3ZQN Power to obtain documents relating to serious terrorism offences** (1) This section applies if an authorised AFP officer considers on reasonable grounds that a person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious terrorism offence. (2) The officer may give the person a written notice requiring the person to produce documents that: (a) relate to one or more of the matters set out in section 3ZQP, as specified in the notice; and (b) are in the possession or under the control of the person.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(3) The notice must: (a) specify the name of the person to whom the notice is given; and (b) specify the matters to which the documents to be produced relate; and (c) specify the manner in which the documents are to be produced; and (d) specify the place at which the documents are to be produced; and (e) state that the person must comply with the notice as soon as practicable; and (f) set out the effect of section 3ZQS (offence for failure to comply); and (g) if the notice specifies that information about the notice must not be disclosed—set out the effect of section 3ZQT (offence for disclosing existence or nature of a notice). **Sec. 3ZQP Matters to which documents must relate** A document to be produced under a notice under section 3ZQN or 3ZQO must relate to one or more of the following matters: (a) determining whether an account is held by a specified person with a specified financial institution, and details relating to the account (including details of any related accounts); (b) determining whether a specified person is a signatory to an account with a specified financial institution, and details relating to the account (including details of any related accounts); (c) determining whether a transaction has been conducted by a specified financial institution on behalf of a specified person, and details relating to the transaction (including details relating to other parties to the transaction); (d) determining whether a specified person travelled or will travel between specified dates or specified locations, and details relating to the travel (including details relating to other persons travelling with the specified person); (e) determining whether assets have been transferred to or from a specified person between specified dates, and details relating to the transfers (including details relating to the names of any other persons to or from whom the assets were transferred); (f) determining whether an account is held by a specified person in respect of a specified utility (such as gas, water or electricity), and details relating to the account (including the names of any other persons who also hold the account); (g) determining who holds an account in respect of a specified utility (such as gas, water or electricity) at a specified place, and details relating to the account; (h) determining whether a telephone account is held by a specified person, and details relating to the account (including: (i) details in respect of calls made to or from the relevant telephone number; or (ii) the times at which such calls were made or received; or (iii) the lengths of such calls; or (iv) the telephone numbers to which such calls were made and from which such calls were received); (i) determining who holds a specified telephone account, and details relating to the account (including details mentioned in paragraph (h)); (j) determining whether a specified person resides at a specified place; (k) determining who resides at a specified place. **Sec. 3ZQR Documents must be produced** (1) A person is not excused from producing a document under section 3ZQN or 3ZQO on the ground that to do so: (a) would contravene any other law; or (b) might tend to incriminate the person or otherwise expose the person to a penalty or other liability; or (c) would disclose material that is protected against disclosure by legal professional privilege or any other duty of confidence; or (d) would be otherwise contrary to the public interest. (2) However, neither: (a) the production of the document; nor (b) any information, document or thing obtained as a direct or indirect consequence of producing the document; is admissible in evidence against the person in proceedings other than proceedings for an offence against section 137.1, 137.2 or 149.1 of the Criminal Code that relates to this Act. (3) A person is not liable to any penalty by reason of his or her producing a document when required to do so under section 3ZQN or 3ZQO. (4) The fact that a person is not excused under subsection (1) from producing a document does not otherwise affect a claim of legal professional privilege that anyone may make in relation to that document. INVESTIGATION OF TERRORISM OFFENCES
"*Period of investigation if arrested for a terrorism offence*"	**Sec. 23DB Period of investigation if arrested for a terrorism offence** (1) If a person is arrested for a terrorism offence, the following provisions apply. (2) The person may, while arrested for the terrorism offence, be detained for the purpose of investigating either or both of the following: (a) whether the person committed the offence;

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(b) whether the person committed another Commonwealth offence that an investigating official reasonably suspects that the person has committed.
(3) Subsection (2) ceases to apply at the end of the investigation period, but that cessation does not affect any other power to detain the person.
(4) If the person is not released within the investigation period, the person must be brought before a judicial officer within the investigation period or, if it is not practicable to do so within the investigation period, as soon as practicable after the end of the investigation period.
(5) For the purposes of this section, but subject to subsections (7) and (9), the investigation period begins when the person is arrested, and ends at a later time that is reasonable, having regard to all the circumstances, but does not extend beyond:
(a) if the person is or appears to be under 18, an Aboriginal person or a Torres Strait Islander—2 hours; or
(b) in any other case—4 hours;
after the arrest, unless the period is extended under section 23DF.
(6) In ascertaining any period of time for the purposes of this section, regard shall be had to the number and complexity of matters being investigated.
(7) If the person has been arrested more than once within any period of 48 hours, the investigation period for each arrest other than the first is reduced by so much of any of the following periods as occurred within that 48 hours:
(a) any earlier investigation period or periods under this section;
(b) any earlier investigation period or periods under section 23C.
(8) However, in relation to each first arrest, disregard subsection (7) for any later arrest if:
(a) the later arrest is for a Commonwealth offence:
(i) that was committed after the end of the person's period of detention under this Part for the first arrest; or
(ii) that arose in different circumstances to those in which any Commonwealth offence to which the first arrest relates arose, and for which new evidence has been found since the first arrest; and
(b) the person's questioning associated with the later arrest does not relate to:
(i) a Commonwealth offence to which the first arrest relates; or
(ii) the circumstances in which such an offence was committed.
(9) In ascertaining any period of time for the purposes of subsection (5) or (7), disregard any reasonable time during which the questioning of the person is suspended, or delayed, for one or more of the following reasons:
(a) to allow the person to be conveyed from the place at which the person is arrested to the nearest premises at which the investigating official has access to facilities for complying with this Part;
(b) to allow the person, or someone else on the person's behalf, to communicate with a legal practitioner, friend, relative, parent, guardian, interpreter or other person as provided by this Part;
(c) to allow such a legal practitioner, friend, relative, parent, guardian, interpreter or other person to arrive at the place where the questioning is to take place;
(d) to allow the person to receive medical attention;
(e) because of the person's intoxication;
(f) to allow for an identification parade to be arranged and conducted;
(g) to allow the making of an application under section 3ZQB or the carrying out of a prescribed procedure within the meaning of Division 4A of Part IAA;
(h) to allow the making and disposing of an application under section 23DC, 23DE, 23WU or 23XB;
(i) to allow a constable to inform the person of matters specified in section 23WJ;
(j) to allow the person to rest or recuperate;
(k) to allow a forensic procedure to be carried out on the person by order of a magistrate under Division 5 of Part ID;
(l) because section 23XGD applies and the time is to be disregarded in working out a period of time for the purposes of that section;
(m) subject to subsection (11), because the time is within a period specified under section 23DD, so long as the suspension or delay in the questioning of the person is reasonable.
(10) To avoid doubt:
(a) subsection (9) does not prevent the person being questioned during a time covered by a paragraph of subsection (9), but if the person is questioned during such a time, the time is not to be disregarded; and
(b) a period specified under section 23DD is not extended by any time covered by a paragraph of subsection (9).
Limit on time that may be disregarded under paragraph (9)(m)
(11) No more than 7 days may be disregarded under paragraph (9)(m) in relation to an arrest. However:
(a) if the person has been arrested more than once within any period of 48 hours, the 7 day period for each arrest other than the first arrest is reduced by any period or periods specified under section 23DD in relation to any earlier arrest; and
(b) subsection (8) applies as if the reference in that subsection to subsection (7) were a reference to this subsection.
Evidentiary provision
(12) In any proceedings, the burden lies on the prosecution to prove that:
(a) the person was brought before a judicial officer as soon as practicable; or
(b) any particular time was covered by a provision of subsection (9).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Disregard of suspension or delay of questioning*"	**Sec. 23DC Time during which suspension or delay of questioning may be disregarded—application** (1) This section applies if: (a) a person is arrested for a terrorism offence; and (b) an investigation is being conducted into whether the person committed that terrorism offence or another terrorism offence. Application for specification of period (2) At or before the end of the investigation period, an investigating official (within the meaning of paragraph (a) or (b) of the definition of that expression) may apply, in writing, to a magistrate for a period to be specified for the purpose of paragraph 23DB(9)(m). (3) The application must not be made unless the application is authorised, in writing, by an authorising officer. (4) Subject to subsection (5), the application must include statements of all of the following: (a) whether it appears to the investigating official that the person is under 18; (b) whether it appears to the investigating official that the person is an Aboriginal person or a Torres Strait Islander; (c) the outcome of any previous application under this section in relation to: (i) the person and the arrest; and (ii) if the person was arrested at any time during the period of 48 hours before the arrest—the person and the earlier arrest or arrests; (d) the total amount of time that has been disregarded under subsection 23DB(9) in ascertaining the investigation period in relation to: (i) the person and the arrest; and (ii) if the person was arrested at any time during the period of 48 hours before the arrest—the person and the earlier arrest or arrests; (e) the reasons why the investigating official believes the period should be specified, which may, for example, be or include one or more of the following: (i) the need to collate and analyse information relevant to the investigation from sources other than the questioning of the person (including, for example, information obtained from a place outside Australia); (ii) the need to allow authorities in or outside Australia (other than authorities in an organisation of which the investigating official is part) time to collect information relevant to the investigation on the request of the investigating official; (iii) the fact that the investigating official has requested the collection of information relevant to the investigation from a place outside Australia that is in a time zone different from the investigating official's time zone; (iv) the fact that translation is necessary to allow the investigating official to seek information from a place outside Australia and/or be provided with such information in a language that the official can readily understand; (f) the period that the investigating official believes should be specified. (5) Subsection (4) does not require any information to be included in the application if disclosure of that information is likely: (a) to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004); or (b) to be protected by public interest immunity; or (c) to put at risk ongoing operations by law enforcement agencies or intelligence agencies; or (d) to put at risk the safety of the community, law enforcement officers or intelligence officers. (6) Before the application is considered by the magistrate, the investigating official must: (a) provide a copy of the application to the person or to his or her legal representative; and (b) inform the person that he or she, or his or her legal representative, may make representations to the magistrate about the application. (7) If the application contains any information of a kind mentioned in subsection (5), the investigating official may remove it from the copy of the application that is provided to the person or to his or her legal representative. (8) The person, or his or her legal representative, may make representations to the magistrate about the application. **Sec. 23DD Time during which suspension or delay of questioning may be disregarded—time specified by magistrate** (1) This section applies if: (a) a person is arrested for a terrorism offence; and (b) an application has been made under subsection 23DC(2) to a magistrate in respect of the person. Specification of period (2) The magistrate may, by signed instrument, specify a period starting at the time the instrument is signed, if satisfied that: (a) it is appropriate to do so, having regard to: (i) the application; and (ii) the representations (if any) made by the person, or his or her legal representative, about the application; and (iii) any other relevant matters; and (b) the offence is a terrorism offence; and (c) detention of the person is necessary to preserve or obtain evidence or to complete the investigation into the offence or into another terrorism offence; and

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(d) the investigation into the offence is being conducted properly and without delay; and (e) the application has been authorised by an authorising officer; and (f) the person, or his or her legal representative, has been given the opportunity to make representations about the application. Instrument specifying period (3) Subject to subsection (4), the instrument must: (a) specify the period as a number (which may be less than one) of hours; and (b) set out the day and time when it was signed; and (c) set out the reasons for specifying the period. (4) Subsection (3) does not require any information to be included in the instrument if disclosure of that information is likely: (a) to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004); or (b) to be protected by public interest immunity; or (c) to put at risk ongoing operations by law enforcement agencies or intelligence agencies; or (d) to put at risk the safety of the community, law enforcement officers or intelligence officers. (5) The magistrate must: (a) give the investigating official a copy of the instrument as soon as practicable after signing it; and (b) if the instrument was made as a result of an application made by telex, fax or other electronic means—inform the investigating official of the matters included in the instrument. (6) The investigating official must: (a) as soon as practicable after receiving a copy of the instrument under paragraph (5)(a), give the person, or his or her legal representative, a copy of it; and (b) if the instrument was made as a result of an application made by telex, fax or other electronic means—inform the person, or his or her legal representative, of the matters included in the instrument as soon as practicable after being informed of them under paragraph (5)(b).
"*Application for extension of investigation period*"	**Sec. 23DE Application may be made for extension of investigation period** (1) If a person is arrested for a terrorism offence, an investigating official (within the meaning of paragraph (a) or (b) of the definition of that expression) may, at or before the end of the investigation period, apply, in writing, to a magistrate for an extension of the investigation period. (2) The application must not be made unless the application is authorised, in writing, by an authorising officer. (3) Subject to subsection (4), the application must include statements of all of the following: (a) whether it appears to the investigating official that the person is under 18; (b) whether it appears to the investigating official that the person is an Aboriginal person or a Torres Strait Islander; (c) the outcome of any previous application under this section in relation to the person and the investigation period; (d) the period (if any) by which the investigation period has been reduced under subsection 23DB(7); (e) the total amount of time (if any) that has been disregarded under subsection 23DB(9) in ascertaining the investigation period; (f) the maximum amount of time by which the investigation period could be extended; (g) the reasons why the investigating official believes the investigation period should be extended; (h) the period by which the investigating official believes the investigation period should be extended. (4) Subsection (3) does not require any information to be included in the application if disclosure of that information is likely: (a) to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004); or (b) to be protected by public interest immunity; or (c) to put at risk ongoing operations by law enforcement agencies or intelligence agencies; or (d) to put at risk the safety of the community, law enforcement officers or intelligence officers. (5) Before the application is considered by the magistrate, the investigating official must: (a) provide a copy of the application to the person or to his or her legal representative; and (b) inform the person that he or she, or his or her legal representative, may make representations to the magistrate about the application. (6) If the application contains any information of a kind mentioned in subsection (4), the investigating official may remove it from the copy of the application that is provided to the person or to his or her legal representative. (7) The person, or his or her legal representative, may make representations to the magistrate about the application. **Sec. 23DF Magistrate may extend investigation period** (1) This section applies if: (a) a person is arrested for a terrorism offence; and (b) an application has been made under subsection 23DE(1) to a magistrate in respect of the person. Extension of investigation period

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(2) Subject to subsection (3), the magistrate may extend the investigation period, by signed written instrument, if satisfied that: (a) the offence is a terrorism offence; and (b) further detention of the person is necessary to: (i) preserve or obtain evidence related to the offence or to another terrorism offence; or (ii) complete the investigation into the offence or into another terrorism offence; and (c) the investigation into the offence is being conducted properly and without delay; and (d) the application has been authorised by an authorising officer; and (e) the person, or his or her legal representative, has been given the opportunity to make representations about the application. (3) Subject to subsection (4), the instrument must set out: (a) the day and time when the extension was granted; and (b) the reasons for granting the extension; and (c) the terms of the extension. (4) Subsection (3) does not require any information to be included in the instrument if disclosure of that information is likely: (a) to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004); or (b) to be protected by public interest immunity; or (c) to put at risk ongoing operations by law enforcement agencies or intelligence agencies; or (d) to put at risk the safety of the community, law enforcement officers or intelligence officers. (5) The magistrate must: (a) give the investigating official a copy of the instrument as soon as practicable after signing it; and (b) if the instrument was made as a result of an application made by telex, fax or other electronic means—inform the investigating official of the matters included in the instrument. (6) The investigating official must: (a) as soon as practicable after receiving a copy of the instrument under paragraph (5)(a), give the person, or his or her legal representative, a copy of it; and (b) if the instrument was made as a result of an application made by telex, fax or other electronic means—inform the person, or his or her legal representative, of the matters included in the instrument as soon as practicable after being informed of them under paragraph (5)(b). (7) The investigation period may be extended any number of times, but the total of the periods of extension cannot be more than 20 hours.
New Zealand "*Application by police for warrant to intercept private communication relating to terrorist offences*"	***Crimes Act 1961***[64]: **Sec. 312CC Application by police for warrant to intercept private communications relating to terrorist offences** (1) An application may be made to a Judge of the High Court for a warrant for any member of the police to intercept a private communication by means of an interception device if there are reasonable grounds for believing— (a) that a terrorist offence has been committed, or is being committed, or is about to be committed; and (b) if the offence has yet to be committed, that the use of an interception device to intercept private communications is likely to prevent its commission; and (c) that it is unlikely that without the granting of such a warrant the police investigation of the case can be brought to a successful conclusion or, as the case may be, the commission of the offence can be prevented. (2) The application must be made by a commissioned officer of the police, in writing and on oath, and must set out the following particulars: (a) a statement of the facts relied on to show that there are reasonable grounds for believing— (i) that a terrorist offence has been committed, or is being committed, or is about to be committed; and (ii) if the offence has yet to be committed, that the use of an interception device to intercept private communications is likely to prevent its commission; and (b) a description of how it is proposed to intercept private communications; and (c) either,— (i) if they are known, the name and address of the suspect the interception of whose private communications there are reasonable grounds for believing will assist the police investigation of the case or (as the case may be) prevent the commission of a terrorist offence; or (ii) if the name and address of the suspect are not known, a general description of the premises or place in respect of which it is proposed to intercept private communications, being premises or a place believed to be used for any purpose by a person— (A) who it is believed has committed, or is committing, or is about to commit, a terrorist offence; or (B) who it is believed was involved, or is involved, or will be involved, in the commission of the offence; and (d) a statement of the period for which the warrant is requested; and

[64] NZ *Crimes Act 1961*: http://www.legislation.govt.nz/act/public/1961/0043/latest/whole.html?search=ts_act_crimes+act_resel&p=1#dlm327382

000462

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(e) whichever of the following is applicable: (i) both— (A) a general description of the investigative procedures and techniques that have been tried, but have failed to enable the police to conclude their investigation of the case successfully or (as the case may be) failed to help prevent the commission of the offence; and (B) a statement of why those procedures and techniques have failed: (ii) a statement of why it appears that investigative procedures and techniques other than the interception of private communications— (A) are unlikely to enable the police to conclude their investigation of the case successfully or (as the case may be) to help prevent the commission of the offence, or (B) are likely to be too dangerous to adopt in the particular case: (iii) a statement of why the case is considered so urgent that it would be impracticable for the police to carry out their investigation using only investigative procedures and techniques other than the interception of private communications. **Sec. 312CD Matters of which Judge must be satisfied in respect of applications relating to terrorist offences** (1) A Judge may grant an interception warrant on an application under section 312CC if satisfied that it is in the best interests of the administration of justice to do so, and— (a) that there are reasonable grounds for believing,— (i) that a terrorist offence has been committed, or is being committed, or is about to be committed; and (ii) if the offence has yet to be committed, that the use of an interception device to intercept private communications is likely to prevent its commission; and (b) that there are reasonable grounds for believing— (i) that evidence relevant to the investigation of the case will be obtained through the use of an interception device to intercept private communications; or (ii) if the offence has yet to be committed, that evidence relevant to the prevention of the offence will be obtained through the use of an interception device to intercept private communications; and (c) whichever of the following is applicable: (i) that investigative procedures and techniques other than the interception of private communications have been tried, but have failed to enable the police to conclude their investigation of the case successfully or (as the case may be) failed to help prevent the commission of the offence; and (ii) that investigative procedures and techniques other than the interception of private communications— (A) are unlikely to enable the police to conclude their investigation of the case successfully or (as the case may be) to help prevent the commission of the offence, or (B) are likely to be too dangerous to adopt in the particular case: (iii) that the case is so urgent that it would be impracticable for the police to carry out their investigation using only investigative procedures and techniques other than the interception of private communications; and (d) that the private communications proposed to be intercepted are not likely to be privileged in proceedings in a court of law by virtue of Part 3 of the Evidence Amendment Act (No 2) 1980 or of any rule of law that confers privilege on communications of a professional character between a barrister or solicitor and a client. (2) In determining whether or not the granting of an interception warrant under subsection (1) is in the best interests of the administration of justice, the Judge must consider the extent to which the privacy of any person or persons would be likely to be interfered with by the interception of private communications under it. "(3) Subsection (2) does not limit subsection (1).
"*Assistance request to access computer data*"	***Summary Proceedings Act 1957***[65]**:** **Sec. 198B Person with knowledge of computer or computer network to assist access** (1) A constable executing a search warrant may require a specified person to provide information or assistance that is reasonable and necessary to allow the constable to access data held in, or accessible from, a computer that is on premises named in the warrant. (2) A specified person is a person who— (a) is the owner or lessee of the computer, or is in possession or control of the computer, or is an employee of any of the above; and (b) has relevant knowledge of— (i) the computer or a computer network of which the computer forms a part; or (ii) measures applied to protect data held in, or accessible from, the computer. (3) A person may not be required under subsection (1) to give any information tending to incriminate the person. (4) Subsection (3) does not prevent a constable from requiring a person to provide information that— (a) is reasonable and necessary to allow the constable to access data held in, or accessible from, a computer that— (i) is on premises named in the warrant concerned; and (ii) contains or may contain information tending to incriminate the person; but

[65] NZ *Summary Proceedings Act 1957*: http://www.legislation.govt.nz/act/public/1957/0087/latest/DLM310743.html?search=ts_act_accident+compensation+act_res+el&p=1
[66] *New Zealand Security Intelligence Service Act 1969* (as modified by *New Zealand Security Intelligence Service Amendment Act 2003*): http://www.legislation.govt.nz/act/public/1969/0024/latest/whole.html#DLM391673

000463

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Tracking device warrant*"	(b) does not itself tend to incriminate the person. (5) Subsection (3) does not prevent a constable from requiring a person to provide assistance that is reasonable and necessary to allow the constable to access data held in, or accessible from, a computer that— (a) is on premises named in the warrant concerned; and (b) contains or may contain information tending to incriminate the person. (6) Every person commits an offence and is liable on summary conviction to a term of imprisonment not exceeding 3 months or a fine not exceeding $2,000 who fails to assist a constable when requested to do so under subsection (1). **Sec. 200B Application for tracking device warrant** (1) An authorised officer may apply to a High Court Judge or a District Court Judge for a tracking device warrant. (2) The application may not be made unless the officer believes— (a) that there are reasonable grounds to suspect that an offence has been, is being, or will be committed; and (b) that information that is relevant to the commission of the offence (whether or not including the whereabouts of any person) can be obtained through the use of a tracking device; and (c) that it is in the public interest to issue a warrant, taking into account the seriousness of the offence, the degree to which privacy or property rights are likely to be intruded upon, the usefulness of the information likely to be obtained, and whether it is reasonably practicable for the information to be obtained in another way. (3) The application must be made in writing and on oath and must set out the following particulars: (a) the facts relied on to show that the requirements in subsection (2) are met; and (b) any information that is necessary so that the Judge may assess the degree to which privacy or property rights are likely to be intruded on; and (c) the period for which a warrant is requested; and (d) the name of the parent agency. **Sec. 200C Issue of tracking device warrant** (1) On an application under section 200B, a High Court Judge or a District Court Judge may issue a warrant under this section if he or she is satisfied that the matters specified in section 200B(2)(a) to (c) are met and may impose any terms and conditions that the Judge sees fit. (2) The warrant must be directed to an authorised officer by name or generally to every authorised officer of the parent agency concerned, and must— (a) state the offence or offences in respect of which it is issued; and (b) state a period (not exceeding 60 days) for which it is valid; and (c) state the terms and conditions (if any) subject to which it is issued; and (d) describe or specify the thing in or on which a tracking device may be installed. (3) Further tracking device warrants may be issued in respect of the same thing, or in respect of information relevant to the commission of the same offence. **Sec. 200D Effect of tracking device warrant** (1) A tracking device warrant authorises the authorised officer or officers to whom it is directed— (a) to install, maintain, or remove a tracking device in or on the thing specified; and (b) to monitor the device or have it monitored. (2) If it is necessary to do so to install, maintain, remove, or monitor a tracking device, a tracking device warrant authorises one or more authorised officers to do any of the following things at any time, using any necessary force: (a) enter on to any premises specified in the warrant: (b) break open or interfere with any thing: (c) temporarily remove anything from anyplace where it is found and to return the thing to that place. **Sec. 200E Expiry of warrant** (1) Unless renewed under section 200F, a tracking device warrant expires at the end of the period stated in it. (2) If a tracking device remains in place after the expiry of the warrant authorising its installation, the authorised officer concerned must apply to a District Court Judge or a High Court Judge for a warrant under section 200I to remove the device; and the Judge may issue a warrant to remove the device subject to any terms and conditions the Judge sees fit. (3) A tracking device that remains in place after the expiry of the warrant authorising its installation must not be monitored; but its remaining in place does not constitute a trespass **Sec. 200F Renewal of warrant** (1) Any authorised officer may apply for the renewal of a tracking device warrant that has not expired. (2) The application must be made— (a) to a District Court Judge, if the warrant was issued by a District Court Judge; and

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(b) to a High Court Judge, if the warrant was issued by a High Court Judge. (3) The application must be made in writing and on oath. (4) A Judge may grant the application and renew the warrant if he or she is satisfied, at the time the application is made, of the matters specified in section 200B(2)(a) to (c). (5) The warrant may be renewed under this section for a period of not more than 60 days. (6) The period for which the warrant is renewed must be written on the warrant, and (unless renewed again) the warrant expires at the end of that period. (7) The warrant may be renewed more than once. (8) If (whether initially or on renewal or further renewal) the warrant was directed to an authorised officer by name, the Judge may amend it so that is directed, by name, to some other authorised officer of the parent agency.
"*Use of tracking device without warrant*"	**Sec. 200G Use of tracking device without warrant** (1) An authorised officer may install, monitor, and maintain a tracking device in or on any thing if— (a) it is not in all the circumstances reasonably practicable to obtain a tracking device warrant; and (b) the officer believes on reasonable grounds that a Judge would issue a tracking device warrant if time permitted. (2) The officer may remove the tracking device within 72 hours of its installation. (3) If it is necessary to do so to install, monitor, maintain, or remove the device, the officer concerned may at any time do any of the following things, using any necessary force: (a) enter any premises: (b) break open or interfere with any thing: (c) temporarily remove anything from anyplace where it is found and return the thing to that place. (4) A tracking device installed under subsection (1) that remains in place more than 72 hours after being installed must not be monitored; but its remaining in place does not constitute a trespass. (5) Subsection (4) does not prevent the monitoring (or the maintenance or removal) of a tracking device if a tracking device warrant for it is in force. (6) Unless the device has already been removed, the officer must within 72 hours of installing it— (a) apply for a tracking device warrant for it; or (b) apply to a Judge for a warrant under section 200I to remove it; or (c) if the officer wants to leave it in place without monitoring it, apply to a Judge for directions. (7) Within 72 hours of being refused a tracking device warrant, the officer must either— (a) apply to a Judge for a warrant under section 200I to remove the device; or (b) if the officer wants to leave the device in place without monitoring it, apply to a Judge for directions. (8) An authorised officer who acts in the exercise or intended exercise of a power conferred by this section is not under any civil or criminal liability in respect of the officer's actions (whether on the ground of lack of jurisdiction or mistake of law or fact, or on any other ground) unless the officer acts in bad faith or without reasonable care.
"*Reports*"	**Sec. 200H Reports** (1) There must be lodged with every application under paragraph (b) or paragraph (c) of section 200G(6) or under section 200G(7) a written report on the installation of the tracking device concerned, and the circumstances in which it came to be installed. (2) If a tracking device installed under section 200G is removed within 72 hours of being installed, an authorised officer of the parent agency concerned must lodge in a District Court or the High Court a written report on its installation, and the circumstances in which it came to be installed. (3) The Registrar of a court in which a report under subsection (1) or subsection (2) is lodged must promptly bring it to the notice of a Judge of the court. (4) If the Judge considers that the circumstances warrant it, the Judge may refer a copy of the report to the chief executive of the parent agency of the authorised officer who installed the device, with any recommendations the Judge thinks fit. (5) The Judge may also refer a copy of the report to the Minister for the time being responsible for the agency.
"*Removal of tracking device*"	**Sec. 200I Warrant for removal of tracking device** (1) A District Court Judge or High Court Judge may issue a warrant for the removal of a tracking device, subject to any terms and conditions the Judge sees fit. (2) A warrant under this section must be directed to an authorised officer by name or generally to every authorised officer of the parent agency concerned. (3) A warrant under this section authorises the authorised officer or officers to whom it is directed to remove the tracking device concerned and, in so doing, to do any of the following at any time if necessary, using any necessary force: (a) enter any premises specified in the warrant: (b) break open or interfere with any thing: (c) temporarily remove any thing from any place where it is found and to return the thing to that place. (4) A warrant under this section expires on the earlier of the following: (a) the date 30 days after the day on which it is issued: (b) a date specified when it is issued by the Judge who issues it.

000465

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Interception warrant*"	[*Please see also sections 200J to 200P of the* Summary Proceedings Act 1957]. ***New Zealand Security Intelligence Service Act 1969***[66]**:** **Sec. 2 Interpretation** (1) In this Act, unless the context otherwise requires,— security means— […] (d) the prevention of any terrorist act and of any activity relating to the carrying out or facilitating of any terrorist act. […] **Sec. 4A Issue of interception warrant** (1) The Minister and the Commissioner may jointly issue a domestic interception warrant, authorising a person to intercept or seize any communication, document, or thing not otherwise lawfully obtainable by the person, if the Minister and the Commissioner are both satisfied on evidence on oath given by the applicant for the warrant that the conditions specified in subsection (3) apply to the proposed warrant. (2) The Minister may issue a foreign interception warrant authorising a person to intercept or seize any communication, document, or thing not otherwise lawfully obtainable by the person, if the Minister is satisfied on evidence on oath given by the applicant for the warrant that— (a) the conditions specified in subsection (3) apply to the proposed warrant; and (b) there are reasonable grounds for believing— (i) that no New Zealand citizen or permanent resident is to be identified by the proposed warrant as a person whose communications may be intercepted; and (ii) that any place to be specified in the proposed warrant is occupied by a foreign organisation or a foreign person. (3) The conditions referred to in subsections (1) and (2) are that— (a) the interception or seizure to be authorised by the proposed warrant is necessary— (i) for the detection of activities prejudicial to security; or (ii) for the purpose of gathering foreign intelligence information essential to security; and (b) the value of the information sought to be obtained under the proposed warrant justifies the particular interception or seizure; and (c) the information is not likely to be obtained by any other means; and (d) any communication sought to be intercepted or seized under the proposed warrant is not privileged in proceedings in a court of law under— (i) any of sections 31 to 33 of the Evidence Amendment Act (No 2) 1980; or (ii) any rule of law that confers privilege on communications of a professional nature between a lawyer and his or her client. (4) An interception warrant may be issued only on an application made in writing by the Director or by the person for the time being acting as the Director. (5) Before issuing an interception warrant in respect of any matter specified in paragraph (b) of the definition of the term security in section 2(1), the Minister must consult the Minister of Foreign Affairs and Trade about the proposed warrant. (6) Every person who, by any interception warrant issued under subsection (1) of this section, is authorised to intercept or seize any communication, document, or thing, or is requested to give any assistance in making the interception or seizure, is justified in making the interception or seizure, and in taking any reasonable action necessarily involved in making or assisting to make or attempting to make the interception or seizure, in accordance with the terms and conditions of the warrant; and (a) no civil or criminal proceedings shall lie against him by reason of his so doing; and (b) the issue of the warrant shall not be subject to judicial review under Part 1 of the Judicature Amendment Act 1972 or otherwise. (7) Where it is necessary to prove in any proceedings in any Court that any person was acting at any time pursuant to an interception warrant, it shall not be necessary to produce the warrant to the Court, but a certificate by the Attorney-General as to any matters specified in the warrant shall be conclusive evidence as to all such matters so certified. (8) Subsection (6) of this section is in addition to and not in derogation of any other enactment relating to the execution of warrants. (9) This section shall have effect notwithstanding anything to the contrary in any other Act. (10) The expiry of an interception warrant does not prevent an application under subsection (1) in respect of the same subject matter. [*Please see also sections 4B to 4I of the New Zealand Security Intelligence Service Act 1969*].

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

France "*Seizures and searches without the agreement of the person concerned*" "*Identity checks on transnational trains*"	***Code de procédure pénale*** **(French Code of Penal Procedure)**[67] **Art. 76** Les perquisitions, visites domiciliaires et saisies de pièces à conviction ou de biens dont la confiscation est prévue à l'article 131-21 du code pénal ne peuvent être effectuées sans l'assentiment exprès de la personne chez laquelle l'opération a lieu. Cet assentiment doit faire l'objet d'une déclaration écrite de la main de l'intéressé ou, si celui-ci ne sait écrire, il en est fait mention au procès verbal ainsi que de son assentiment. Les dispositions prévues par les articles 56 et 59 (premier alinéa) du présent code sont applicables. Si les nécessités de l'enquête relative à un crime ou à un délit puni d'une peine d'emprisonnement d'une durée égale ou supérieure à cinq ans l'exigent ou si la recherche de biens dont la confiscation est prévue à l' article 131-21 du code pénal le justifie, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, décider, par une décision écrite et motivée, que les opérations prévues au présent article seront effectuées sans l'assentiment de la personne chez qui elles ont lieu. A peine de nullité, la décision du juge des libertés et de la détention précise la qualification de l'infraction dont la preuve est recherchée ainsi que l'adresse des lieux dans lesquels ces opérations peuvent être effectuées ; cette décision est motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires. Les opérations sont effectuées sous le contrôle du magistrat qui les a autorisées, et qui peut se déplacer sur les lieux pour veiller au respect des dispositions légales. Ces opérations ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans la décision du juge des libertés et de la détention ou la saisie des biens dont la confiscation est prévue à l'article 131-21 du code pénal. Toutefois, le fait que ces opérations révèlent des infractions autres que celles visées dans la décision ne constitue pas une cause de nullité des procédures incidentes. Pour l'application des dispositions de l'alinéa précédent, est compétent le juge des libertés et de la détention du tribunal de grande instance dont le procureur de la République dirige l'enquête, quelle que soit la juridiction dans le ressort de laquelle la perquisition doit avoir lieu. Le juge des libertés et de la détention peut alors se déplacer sur les lieux quelle que soit leur localisation sur le territoire national. Le procureur de la République peut également saisir le juge des libertés et de la détention du tribunal de grande instance dans le ressort duquel la perquisition doit avoir lieu, par l'intermédiaire du procureur de la République de cette juridiction. **Art. 78-2** Les officiers de police judiciaire et, sur l'ordre et sous la responsabilité de ceux-ci, les agents de police judiciaire et agents de police judiciaire adjoints mentionnés aux articles 20 et 21-1° peuvent inviter à justifier, par tout moyen, de son identité toute personne à l'égard de laquelle existe une ou plusieurs raisons plausibles de soupçonner : - qu'elle a commis ou tenté de commettre une infraction ; - ou qu'elle se prépare à commettre un crime ou un délit ; - ou qu'elle est susceptible de fournir des renseignements utiles à l'enquête en cas de crime ou de délit ; - ou qu'elle fait l'objet de recherches ordonnées par une autorité judiciaire. Sur réquisitions écrites du procureur de la République aux fins de recherche et de poursuite d'infractions qu'il précise, l'identité de toute personne peut être également contrôlée, selon les mêmes modalités, dans les lieux et pour une période de temps déterminés par ce magistrat. Le fait que le contrôle d'identité révèle des infractions autres que celles visées dans les réquisitions du procureur de la République ne constitue pas une cause de nullité des procédures incidentes. L'identité de toute personne, quel que soit son comportement, peut également être contrôlée, selon les modalités prévues au premier alinéa, pour prévenir une atteinte à l'ordre public, notamment à la sécurité des personnes ou des biens. Dans une zone comprise entre la frontière terrestre de la France avec les Etats parties à la convention signée à Schengen le 19 juin 1990 et une ligne tracée à 20 kilomètres en deçà, (Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 93-323 DC du 5 août 1993) ainsi que dans les zones accessibles au public des ports, aéroports et gares ferroviaires ou routières ouverts au trafic international et désignés par arrêté, pour la prévention et la recherche des infractions liées à la criminalité transfrontalière, (Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 93-323 DC du 5 août 1993) l'identité de toute personne peut également être contrôlée, selon les modalités prévues au premier alinéa, en vue de vérifier le respect des obligations de détention, de port et de présentation des titres et documents prévues par la loi. Lorsque ce contrôle a lieu à bord d'un train effectuant une liaison internationale, il peut être opéré sur la portion du trajet entre la frontière et le premier arrêt qui se situe au-delà des vingt kilomètres de la frontière. Toutefois, sur celles des lignes ferroviaires effectuant une liaison internationale et présentant des caractéristiques particulières de desserte, le contrôle peut également être opéré entre cet arrêt et un arrêt situé dans la limite des cinquante kilomètres suivants. Ces lignes et ces arrêts sont désignés par arrêté ministériel (1). Lorsqu'il existe une section autoroutière démarrant dans la zone mentionnée à la première phrase du présent alinéa (1) et que le premier péage autoroutier se situe au-delà de la ligne des 20 kilomètres, le contrôle peut en outre avoir lieu jusqu'à ce premier péage sur les aires de stationnement ainsi que sur le lieu de ce péage et les aires de stationnement attenantes. Les péages concernés par cette disposition sont désignés par arrêté. Le fait que le contrôle d'identité révèle une infraction autre que celle de non-respect des obligations susvisées ne constitue pas une cause de nullité des procédures incidentes. Pour l'application du présent alinéa, le contrôle des obligations de détention, de port et de présentation des titres et documents prévus par la loi ne peut être pratiqué que pour une durée n'excédant pas six heures consécutives dans un même lieu et ne peut consister en un contrôle systématique des personnes présentes ou circulant dans les zones ou lieux mentionnés au même alinéa. Dans une zone comprise entre les frontières terrestres ou le littoral du département de la Guyane et une ligne tracée à vingt kilomètres en-deçà, et sur une ligne tracée à cinq kilomètres de part et d'autre, ainsi que sur la route nationale 2 sur le territoire de la commune de Régina, l'identité de toute personne peut être contrôlée, selon les modalités prévues au premier alinéa, en vue de vérifier le respect des obligations de détention, de port et de présentation des titres et documents prévus par la loi.

[67] *Code français de procédure pénale* (French Code of Penal Procedure): http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154 (in French).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Vehicle inspections*"	Pendant cinq ans à compter de la publication de la loi n° 2006-911 du 24 juillet 2006 relative à l'immigration et à l'intégration, l'identité de toute personne peut également être contrôlée, selon les modalités prévues au premier alinéa du présent article, en vue de vérifier le respect des obligations de détention, de port et de présentation des titres et documents prévus par la loi : 1° En Guadeloupe, dans une zone comprise entre le littoral et une ligne tracée à un kilomètre en deçà, ainsi que dans une zone d'un kilomètre de part et d'autre, d'une part, de la route nationale 1 sur le territoire des communes de Basse-Terre, Gourbeyre et Trois-Rivières et, d'autre part, de la route nationale 4 sur le territoire des communes du Gosier et de Sainte-Anne et Saint-François ; 2° A Mayotte, dans une zone comprise entre le littoral et une ligne tracée à un kilomètre en deçà ; 3° A Saint-Martin, dans une zone comprise entre le littoral et une ligne tracée à un kilomètre en deçà ; 4° A Saint-Barthélemy, dans une zone comprise entre le littoral et une ligne tracée à un kilomètre en deçà.
"*Surveillance throughout the national territory of suspected of terrorist acts*"	**Art. 78-2-2** Sur réquisitions écrites du procureur de la République aux fins de recherche et de poursuite des actes de terrorisme visés par les articles 421-1 à 421-6 du code pénal, des infractions en matière de prolifération des armes de destruction massive et de leurs vecteurs visées aux 1° et 2° du I de l'article L. 1333-9, à l'article L. 1333-11, au II des articles L. 1333-13-3 et L. 1333-13-4 et aux articles L. 1333-13-5, L. 2339-14, L. 2339-15, L. 2341-1, L. 2341-2, L. 2341-4, L. 2342-59 et L. 2342-60 du code de la défense, d'armes et d'explosifs visées par les articles L. 2339-8, L. 2339-9 et L. 2353-4 du code de la défense, des infractions de vol visées par les articles 311-3 à 311-11 du code pénal, de recel visées par les articles 321-1 et 321-2 du même code ou des faits de trafic de stupéfiants visés par les articles 222-34 à 222-38 dudit code, les officiers de police judiciaire, assistés, le cas échéant, des agents de police judiciaire et des agents de police judiciaire adjoints mentionnés aux 1°,1° bis et 1° ter de l'article 21 peuvent, dans les lieux et pour la période de temps que ce magistrat détermine et qui ne peut excéder vingt-quatre heures, renouvelables sur décision expresse et motivée selon la même procédure, procéder non seulement aux contrôles d'identité prévus au sixième alinéa de l'article 78-2 mais aussi à la visite des véhicules circulant, arrêtés ou stationnant sur la voie publique ou dans des lieux accessibles au public. Pour l'application des dispositions du présent article, les véhicules en circulation ne peuvent être immobilisés que le temps strictement nécessaire au déroulement de la visite qui doit avoir lieu en présence du conducteur. Lorsqu'elle porte sur un véhicule à l'arrêt ou en stationnement, la visite se déroule en présence du conducteur ou du propriétaire du véhicule ou, à défaut, d'une personne requise à cet effet par l'officier ou l'agent de police judiciaire et qui ne relève pas de son autorité administrative. La présence d'une personne extérieure n'est toutefois pas requise si la visite comporte des risques graves pour la sécurité des personnes et des biens. En cas de découverte d'une infraction ou si le conducteur ou le propriétaire du véhicule le demande ainsi que dans le cas où la visite se déroule en leur absence, il est établi un procès-verbal mentionnant le lieu et les dates et heures du début et de la fin de ces opérations. Un exemplaire en est remis à l'intéressé et un autre est transmis sans délai au procureur de la République. Toutefois, la visite des véhicules spécialement aménagés à usage d'habitation et effectivement utilisés comme résidence ne peut être faite que conformément aux dispositions relatives aux perquisitions et visites domiciliaires. Le fait que ces opérations révèlent des infractions autres que celles visées dans les réquisitions du procureur de la République ne constitue pas une cause de nullité des procédures incidentes.
"*Infiltration operations authorized by state prosecutors or investigating judges*"	**Art. 706-80** Les officiers de police judiciaire et, sous leur autorité, les agents de police judiciaire, après en avoir informé le procureur de la République et sauf opposition de ce magistrat, peuvent étendre à l'ensemble du territoire national la surveillance de personnes contre lesquelles il existe une ou plusieurs raisons plausibles de les soupçonner d'avoir commis l'un des crimes et délits entrant dans le champ d'application des articles 706-73 ou 706-74 ou la surveillance de l'acheminement ou du transport des objets, biens ou produits tirés de la commission de ces infractions ou servant à les commettre. L'information préalable à l'extension de compétence prévue par le premier alinéa doit être donnée, par tout moyen, au procureur de la République près le tribunal de grande instance dans le ressort duquel les opérations de surveillance sont susceptibles de débuter ou, le cas échéant, au procureur de la République saisi en application des dispositions de l'article 706-76. **Art. 706-81** Lorsque les nécessités de l'enquête ou de l'instruction concernant l'un des crimes ou délits entrant dans le champ d'application de l'article 706-73 le justifient, le procureur de la République ou, après avis de ce magistrat, le juge d'instruction saisi peuvent autoriser qu'il soit procédé, sous leur contrôle respectif, à une opération d'infiltration dans les conditions prévues par la présente section. L'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs. L'officier ou l'agent de police judiciaire est à cette fin autorisé à faire usage d'une identité d'emprunt et à commettre si nécessaire les actes mentionnés à l'article 706-82. A peine de nullité, ces actes ne peuvent constituer une incitation à commettre des infractions. L'infiltration fait l'objet d'un rapport rédigé par l'officier de police judiciaire ayant coordonné l'opération, qui comprend les éléments strictement nécessaires à la constatation des infractions et ne mettant pas en danger la sécurité de l'agent infiltré et des personnes requises au sens de l'article 706-82. **Art. 706-82** Les officiers ou agents de police judiciaire autorisés à procéder à une opération d'infiltration peuvent, sur l'ensemble du territoire national, sans être pénalement responsables de ces actes : 1° Acquérir, détenir, transporter, livrer ou délivrer des substances, biens, produits, documents ou informations tirés de la commission des infractions ou servant à la commission de ces infractions ; 2° Utiliser ou mettre à disposition des personnes se livrant à ces infractions des moyens de caractère juridique ou financier ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	L'exonération de responsabilité prévue au premier alinéa est également applicable, pour les actes commis à seule fin de procéder à l'opération d'infiltration, aux personnes requises par les officiers ou agents de police judiciaire pour permettre la réalisation de cette opération. **Art. 706-83** A peine de nullité, l'autorisation donnée en application de l'article 706-81 est délivrée par écrit et doit être spécialement motivée. Elle mentionne la ou les infractions qui justifient le recours à cette procédure et l'identité de l'officier de police judiciaire sous la responsabilité duquel se déroule l'opération. Cette autorisation fixe la durée de l'opération d'infiltration, qui ne peut pas excéder quatre mois. L'opération peut être renouvelée dans les mêmes conditions de forme et de durée. Le magistrat qui a autorisé l'opération peut, à tout moment, ordonner son interruption avant l'expiration de la durée fixée. L'autorisation est versée au dossier de la procédure après achèvement de l'opération d'infiltration. **Art. 706-84** L'identité réelle des officiers ou agents de police judiciaire ayant effectué l'infiltration sous une identité d'emprunt ne doit apparaître à aucun stade de la procédure. La révélation de l'identité de ces officiers ou agents de police judiciaire est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque cette révélation a causé des violences, coups et blessures à l'encontre de ces personnes ou de leurs conjoints, enfants et ascendants directs, les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende. Lorsque cette révélation a causé la mort de ces personnes ou de leurs conjoints, enfants et ascendants directs, les peines sont portées à dix ans d'emprisonnement et à 150 000 euros d'amende, sans préjudice, le cas échéant, de l'application des dispositions du chapitre Ier du titre II du livre II du code pénal. **Art. 706-85** En cas de décision d'interruption de l'opération ou à l'issue du délai fixé par la décision autorisant l'infiltration et en l'absence de prolongation, l'agent infiltré peut poursuivre les activités mentionnées à l'article 706-82, sans en être pénalement responsable, le temps strictement nécessaire pour lui permettre de cesser sa surveillance dans des conditions assurant sa sécurité sans que cette durée puisse excéder quatre mois. Le magistrat ayant délivré l'autorisation prévue à l'article 706-81 en est informé dans les meilleurs délais. Si, à l'issue du délai de quatre mois, l'agent infiltré ne peut cesser son opération dans des conditions assurant sa sécurité, ce magistrat en autorise la prolongation pour une durée de quatre mois au plus. **Art. 706-86** L'officier de police judiciaire sous la responsabilité duquel se déroule l'opération d'infiltration peut seul être entendu en qualité de témoin sur l'opération. Toutefois, s'il ressort du rapport mentionné au troisième alinéa de l'article 706-81 que la personne mise en examen ou comparaissant devant la juridiction de jugement est directement mise en cause par des constatations effectuées par un agent ayant personnellement réalisé les opérations d'infiltration, cette personne peut demander à être confrontée avec cet agent dans les conditions prévues par l'article 706-61. Les questions posées à l'agent infiltré à l'occasion de cette confrontation ne doivent pas avoir pour objet ni pour effet de révéler, directement ou indirectement, sa véritable identité. **Art. 706-87** Aucune condamnation ne peut être prononcée sur le seul fondement des déclarations faites par les officiers ou agents de police judiciaire ayant procédé à une opération d'infiltration. Les dispositions du présent article ne sont cependant pas applicables lorsque les officiers ou agents de police judiciaire déposent sous leur véritable identité.
"*Tapping of phones, and placing of sound-recording devices in any public or private place or vehicle*"	**Art. 706-96** Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou plusieurs personnes se trouvant dans un lieu privé. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction. En vue de mettre en place le dispositif technique mentionné au premier alinéa, le juge d'instruction peut autoriser l'introduction dans un véhicule ou un lieu privé, y compris hors des heures prévues à l'article 59, à l'insu ou sans le consentement du propriétaire ou du possesseur du véhicule ou de l'occupant des lieux ou de toute personne titulaire d'un droit sur ceux-ci.S'il s'agit d'un lieu d'habitation et que l'opération doit intervenir hors des heures prévues à l'article 59, cette autorisation est délivrée par le juge des libertés et de la détention saisi à cette fin par le juge d'instruction. Ces opérations, qui ne peuvent avoir d'autre fin que la mise en place du dispositif technique, sont effectuées sous l'autorité et le contrôle du juge d'instruction. Les dispositions du présent alinéa sont également applicables aux opérations ayant pour objet la désinstallation du dispositif technique ayant été mis en place. La mise en place du dispositif technique mentionné au premier alinéa ne peut concerner les lieux visés aux articles 56-1,56-2 et 56-3 ni être mise en oeuvre dans le véhicule, le bureau ou le domicile des personnes visées à l'article 100-7. Le fait que les opérations prévues au présent article révèlent des infractions autres que celles visées dans la décision du juge d'instruction ne constitue pas une cause de nullité des procédures incidentes.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	Art. 706-97 Les décisions prises en application de l'article 706-96 doivent comporter tous les éléments permettant d'identifier les véhicules ou les lieux privés ou publics visés, l'infraction qui motive le recours à ces mesures ainsi que la durée de celles-ci. **Art. 706-98** Ces décisions sont prises pour une durée maximale de quatre mois. Elles ne peuvent être renouvelées que dans les mêmes conditions de forme et de durée. **Art. 706-99** Le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service, d'une unité ou d'un organisme placé sous l'autorité ou la tutelle du ministre de l'intérieur et dont la liste est fixée par décret, en vue de procéder à l'installation des dispositifs techniques mentionnés à l'article 706-96. Les officiers ou agents de police judiciaire ou les agents qualifiés mentionnés au premier alinéa du présent article chargés de procéder aux opérations prévues par l'article 706-96 sont autorisés à détenir à cette fin des appareils relevant des dispositions de l'article 226-3 du code pénal. **Art. 706-100** Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse procès-verbal de chacune des opérations de mise en place du dispositif technique et des opérations de captation, de fixation et d'enregistrement sonore ou audiovisuel. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée. Les enregistrements sont placés sous scellés fermés. **Art. 706-101** Le juge d'instruction ou l'officier de police judiciaire commis par lui décrit ou transcrit, dans un procès-verbal qui est versé au dossier, les images ou les conversations enregistrées qui sont utiles à la manifestation de la vérité. Les conversations en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin. **Art. 706-102** Les enregistrements sonores ou audiovisuels sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il est dressé procès-verbal de l'opération de destruction.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(d) Current SPECIAL PROCEDURES Used to Prevent the Commission of Terrorism in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011)

Both before and after 11 September 2001, countries surveyed have created or broadened frameworks for the detention of terrorist suspects. To date, the most contentious framework is undoubtedly the military prison set up in Guantanamo Bay, Cuba, by the United States. However, all anti-terrorism legislation dealing with the detention of terrorist suspects have to a certain extent attracted criticisms and/or judicial challenges. As is the case with other subject matters within the scope of this research, countries surveyed have addressed the issue of detention of terrorists for an extended period of time in different ways, based on their own national security concerns, constitutional standards, and legal system tenets. While some countries have decided to rely primarily on criminal law to detain terrorist suspects (United Kingdom, France), other have relied on administrative immigration law to hold in custody persons suspected of terrorism-related activity (Canada, New Zealand). Other countries have yet favoured a third approach in detaining terrorist suspects pursuant to statues or executive decrees passed in the name of national security in response to a state of national emergency (United States, Australia). Although the various approaches can be differentiated through their legal basis, it is worth noting that boundaries between the detention regimes are sometimes blurred in practice. The chart under this current Title of the research draws some distinctions between preventative detention regimes and pre-charge detentions. For a thorough analysis of this subject, please refer to: Stella BURCH ELIAS, "Rethinking 'Preventive Detention' From a Comparative Perspective: Three Frameworks for Detaining Terrorist Suspects", 41:2009-2010 *Columbia Human Rights Law Review* 99. Special procedures or regimes allowing for the prolonged detention of terrorist suspects in Canada, the United States (US), the United Kingdom (UK), Australia, New Zealand (NZ), and France are described below. Unlike the approach for subject matters previously dealt with in this research, the relevant information is presented in a single chart.

d.1 – Special Procedures	
Country	**Presentation and definitions**
Canada "*Security certificates*"	In Canada, a separate system of immigration detention exists alongside a criminal law detention framework. After 11 September 2001, Canada relied heavily on the security certificate process available under the administrative immigration law to detain terrorist suspects for extended periods of time. The security certificate process seeks the removal of a permanent resident or foreign national (i.e. a non-citizen) on grounds of security, violating human rights, and/or serious or organized criminality. This procedure was established in 1978 through an amendment to the *Immigration Act* of 1976. In 2001, the *Immigration Act* was superseded by the *Immigration and Refugee Protection Act* (*IRPA*), which increased the authority of the security certificate process in order to make it more effective and efficient in the protection of national security. In 2007, the Supreme Court of Canada (SCC) upheld Canada's practice of holding terrorist suspects for several years pending deportation under the security certificate process (*Charkaoui v. Canada*, [2007] 1 SCR 350). However, the SCC found that additional safeguards should be incorporated into the security certificate process. The SCC ruling lead in 2008 to the passing of *An Act to Amend the Immigration and Refugee Protection Act (Certificate and Special Advocate) and to Make a Consequential Amendment to Another Act*. This new legislation introduced a special advocate into the certificate process, whose role is to protect the interest of the person subject to a certificate during closed proceedings. Despite the improvement, the security certificate process' value as a functional anti-terrorism tool was seriously undermined in 2009, by a Federal Court's decision to drop the security certificate case against Adil Charkaoui, with no opportunity for the government to appeal (*Charkaoui (Re)*, 2009 CF 1030). With respect to preventive or special pre-charge detention, Canadian criminal law permitted a limited form of preventive detention in terrorism case between 2001 and February 2007. Under the *Criminal Code* (as amended by the *Anti-terrorism Act* of 2001), police officers were empowered to arrest and detain a terrorist suspect without an arrest warrant if an officer suspected on reasonable grounds that it was necessary to do so in order to prevent a terrorist activity (section 83.3(4) of the amended *Criminal Code*).[68] Persons suspected of terrorist activity could accordingly be preventively detained for up to 72 hours. This power did not truly constitute an attenuated form of pre-charge detention since even when the suspected terrorist was detained without warrant the peace officer was obliged to swear an "information" as soon as possible after the detention. The relevant provision was allowed to sunset on 1 March 2007. In April 2010, the *Bill C-17 An Act to Amend the Criminal Code (Investigative Hearing and Recognizance with Conditions)* was introduced, and proposed to reinstate the anti-terrorism preventive detention regime. This Bill was before Parliament at its dissolution for the general election in March 2011. ***Immigration and Refugee Protection Act*[69]:** **Sec. 77 Referral of certificate** (1) The Minister and the Minister of Citizenship and Immigration shall sign a certificate stating that a permanent resident or foreign national is inadmissible on grounds of security, violating human

[68] Please refer directly to the Canadian *Criminal Code* (see sections 83.3 and 83.32): http://laws-lois.justice.gc.ca/eng/acts/C-46/FullText.html
[69] Canada the *Immigration and Refugee Protection Act*: http://laws-lois.justice.gc.ca/eng/acts/I-2.5/FullText.html

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	or international rights, serious criminality or organized criminality, and shall refer the certificate to the Federal Court. Filing of evidence and summary (2) When the certificate is referred, the Minister shall file with the Court the information and other evidence on which the certificate is based, and a summary of information and other evidence that enables the person who is named in the certificate to be reasonably informed of the case made by the Minister but that does not include anything that, in the Minister's opinion, would be injurious to national security or endanger the safety of any person if disclosed. Effect of referral (3) Once the certificate is referred, no proceeding under this Act respecting the person who is named in the certificate — other than proceedings relating to sections 82 to 82.3, 112 and 115 — may be commenced or continued until the judge determines whether the certificate is reasonable. **Sec. 78 Determination** The judge shall determine whether the certificate is reasonable and shall quash the certificate if he or she determines that it is not. **Sec. 79 Appeal** An appeal from the determination may be made to the Federal Court of Appeal only if the judge certifies that a serious question of general importance is involved and states the question. However, no appeal may be made from an interlocutory decision in the proceeding. **Sec. 80 Effect of certificate** A certificate that is determined to be reasonable is conclusive proof that the person named in it is inadmissible and is a removal order that is in force without it being necessary to hold or continue an examination or admissibility hearing. **Sec. 81 Ministers' warrant** The Minister and the Minister of Citizenship and Immigration may issue a warrant for the arrest and detention of a person who is named in a certificate if they have reasonable grounds to believe that the person is a danger to national security or to the safety of any person or is unlikely to appear at a proceeding or for removal. **Sec. 82 Initial review of detention** (1) A judge shall commence a review of the reasons for the person's continued detention within 48 hours after the detention begins. Further reviews of detention — before determining reasonableness (2) Until it is determined whether a certificate is reasonable, a judge shall commence another review of the reasons for the person's continued detention at least once in the six-month period following the conclusion of each preceding review. Further reviews of detention — after determining reasonableness (3) A person who continues to be detained after a certificate is determined to be reasonable may apply to the Federal Court for another review of the reasons for their continued detention if a period of six months has expired since the conclusion of the preceding review. Reviews of conditions (4) A person who is released from detention under conditions may apply to the Federal Court for another review of the reasons for continuing the conditions if a period of six months has expired since the conclusion of the preceding review. Order (5) On review, the judge (a) shall order the person's detention to be continued if the judge is satisfied that the person's release under conditions would be injurious to national security or endanger the safety of any person or that they would be unlikely to appear at a proceeding or for removal if they were released under conditions; or (b) in any other case, shall order or confirm the person's release from detention and set any conditions that the judge considers appropriate. **Sec. 82.1 Variation of orders** (1) A judge may vary an order made under subsection 82(5) on application of the Minister or of the person who is subject to the order if the judge is satisfied that the variation is desirable because of a material change in the circumstances that led to the order. Calculation of period for next review (2) For the purpose of calculating the six-month period referred to in subsection 82(2), (3) or (4), the conclusion of the preceding review is deemed to have taken place on the day on which the decision under subsection (1) is made. **Sec. 82.2 Arrest and detention — breach of conditions** (1) A peace officer may arrest and detain a person released under section 82 or 82.1 if the officer has reasonable grounds to believe that the person has contravened or is about to contravene any condition applicable to their release.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

Appearance before judge
(2) The peace officer shall bring the person before a judge within 48 hours after the detention begins.
Order
(3) If the judge finds that the person has contravened or was about to contravene any condition applicable to their release, the judge shall
(a) order the person's detention to be continued if the judge is satisfied that the person's release under conditions would be injurious to national security or endanger the safety of any person or that they would be unlikely to appear at a proceeding or for removal if they were released under conditions;
(b) confirm the release order; or
(c) vary the conditions applicable to their release.
Calculation of period for next review
(4) For the purpose of calculating the six-month period referred to in subsection 82(2), (3) or (4), the conclusion of the preceding review is deemed to have taken place on the day on which the decision under subsection (3) is made.

Sec. 82.3 Appeal
An appeal from a decision made under any of sections 82 to 82.2 may be made to the Federal Court of Appeal only if the judge certifies that a serious question of general importance is involved and states the question. However, no appeal may be made from an interlocutory decision in the proceeding.

Sec. 82.4 Minister's order to release
The Minister may, at any time, order that a person who is detained under any of sections 82 to 82.2 be released from detention to permit their departure from Canada.

Sec. 83 Protection of information
(1) The following provisions apply to proceedings under any of sections 78 and 82 to 82.2:
(a) the judge shall proceed as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit;
(b) the judge shall appoint a person from the list referred to in subsection 85(1) to act as a special advocate in the proceeding after hearing representations from the permanent resident or foreign national and the Minister and after giving particular consideration and weight to the preferences of the permanent resident or foreign national;
(c) at any time during a proceeding, the judge may, on the judge's own motion — and shall, on each request of the Minister — hear information or other evidence in the absence of the public and of the permanent resident or foreign national and their counsel if, in the judge's opinion, its disclosure could be injurious to national security or endanger the safety of any person;
(d) the judge shall ensure the confidentiality of information and other evidence provided by the Minister if, in the judge's opinion, its disclosure would be injurious to national security or endanger the safety of any person;
(e) throughout the proceeding, the judge shall ensure that the permanent resident or foreign national is provided with a summary of information and other evidence that enables them to be reasonably informed of the case made by the Minister in the proceeding but that does not include anything that, in the judge's opinion, would be injurious to national security or endanger the safety of any person if disclosed;
(f) the judge shall ensure the confidentiality of all information or other evidence that is withdrawn by the Minister;
(g) the judge shall provide the permanent resident or foreign national and the Minister with an opportunity to be heard;
(h) the judge may receive into evidence anything that, in the judge's opinion, is reliable and appropriate, even if it is inadmissible in a court of law, and may base a decision on that evidence;
(i) the judge may base a decision on information or other evidence even if a summary of that information or other evidence is not provided to the permanent resident or foreign national; and
(j) the judge shall not base a decision on information or other evidence provided by the Minister, and shall return it to the Minister, if the judge determines that it is not relevant or if the Minister withdraws it.
Clarification
(1.1) For the purposes of paragraph (1)(h), reliable and appropriate evidence does not include information that is believed on reasonable grounds to have been obtained as a result of the use of torture within the meaning of section 269.1 of the Criminal Code, or cruel, inhuman or degrading treatment or punishment within the meaning of the Convention Against Torture.
Appointment of special advocate
(1.2) If the permanent resident or foreign national requests that a particular person be appointed under paragraph (1)(b), the judge shall appoint that person unless the judge is satisfied that
(a) the appointment would result in the proceeding being unreasonably delayed;
(b) the appointment would place the person in a conflict of interest; or
(c) the person has knowledge of information or other evidence whose disclosure would be injurious to national security or endanger the safety of any person and, in the circumstances, there is a risk of inadvertent disclosure of that information or other evidence.
For greater certainty
(2) For greater certainty, the judge's power to appoint a person to act as a special advocate in a proceeding includes the power to terminate the appointment and to appoint another person.

Sec. 84 Protection of information on appeal
Section 83 — other than the obligation to provide a summary — and sections 85.1 to 85.5 apply to an appeal under section 79 or 82.3, and to any further appeal, with any necessary modifications.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

Sec. 85 Special Advocate – List of persons who may act as special advocates
(1) The Minister of Justice shall establish a list of persons who may act as special advocates and shall publish the list in a manner that the Minister of Justice considers appropriate to facilitate public access to it.
Statutory Instruments Act
(2) The Statutory Instruments Act does not apply to the list.
Administrative support and resources
(3) The Minister of Justice shall ensure that special advocates are provided with adequate administrative support and resources.

Sec. 85.1 Special advocate's role
(1) A special advocate's role is to protect the interests of the permanent resident or foreign national in a proceeding under any of sections 78 and 82 to 82.2 when information or other evidence is heard in the absence of the public and of the permanent resident or foreign national and their counsel.
Responsibilities
(2) A special advocate may challenge
(a) the Minister's claim that the disclosure of information or other evidence would be injurious to national security or endanger the safety of any person; and
(b) the relevance, reliability and sufficiency of information or other evidence that is provided by the Minister and is not disclosed to the permanent resident or foreign national and their counsel, and the weight to be given to it.
For greater certainty
(3) For greater certainty, the special advocate is not a party to the proceeding and the relationship between the special advocate and the permanent resident or foreign national is not that of solicitor and client.
Protection of communications with special advocate
(4) However, a communication between the permanent resident or foreign national or their counsel and the special advocate that would be subject to solicitor-client privilege if the relationship were one of solicitor and client is deemed to be subject to solicitor-client privilege. For greater certainty, in respect of that communication, the special advocate is not a compellable witness in any proceeding.

Sec. 85.2 Powers
A special advocate may
(a) make oral and written submissions with respect to the information and other evidence that is provided by the Minister and is not disclosed to the permanent resident or foreign national and their counsel;
(b) participate in, and cross-examine witnesses who testify during, any part of the proceeding that is held in the absence of the public and of the permanent resident or foreign national and their counsel; and
(c) exercise, with the judge's authorization, any other powers that are necessary to protect the interests of the permanent resident or foreign national.

Sec. 85.3 Immunity
A special advocate is not personally liable for anything they do or omit to do in good faith under this Division.

Sec. 85.4 Obligation to provide information
(1) The Minister shall, within a period set by the judge, provide the special advocate with a copy of all information and other evidence that is provided to the judge but that is not disclosed to the permanent resident or foreign national and their counsel.
Restrictions on communications — special advocate
(2) After that information or other evidence is received by the special advocate, the special advocate may, during the remainder of the proceeding, communicate with another person about the proceeding only with the judge's authorization and subject to any conditions that the judge considers appropriate.
Restrictions on communications — other persons
(3) If the special advocate is authorized to communicate with a person, the judge may prohibit that person from communicating with anyone else about the proceeding during the remainder of the proceeding or may impose conditions with respect to such a communication during that period.

Sec. 85.5 Disclosure and communication prohibited
With the exception of communications authorized by a judge, no person shall
(a) disclose information or other evidence that is disclosed to them under section 85.4 and that is treated as confidential by the judge presiding at the proceeding; or
(b) communicate with another person about the content of any part of a proceeding under any of sections 78 and 82 to 82.2 that is heard in the absence of the public and of the permanent resident or foreign national and their counsel.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	Sec. 85.6 Rules (1) The Chief Justice of the Federal Court of Appeal and the Chief Justice of the Federal Court may each establish a committee to make rules governing the practice and procedure in relation to the participation of special advocates in proceedings before the court over which they preside. The rules are binding despite any rule of practice that would otherwise apply. Composition of committees (2) Any committee established shall be composed of the Chief Justice of the Federal Court of Appeal or the Chief Justice of the Federal Court, as the case may be, the Attorney General of Canada or one or more representatives of the Attorney General of Canada, and one or more members of the bar of any province who have experience in a field of law relevant to those types of proceedings. The Chief Justices may also designate additional members of their respective committees. Chief Justices shall preside (3) The Chief Justice of the Federal Court of Appeal and the Chief Justice of the Federal Court — or a member designated by them — shall preside over their respective committees. [*Please also refer to sections 76, 86 to 87.2 of the* Immigration and Refugee Protection Act].
United States "*Special mandatory detention of aliens suspected of terrorism*"	The US is currently involved in the process of determining whether it should continue to hold terrorist suspects in extra-territorial preventive detention in Guantanamo Bay, should develop a new system of preventive detention to hold terrorist suspects on domestic soil, or should eschew any use of preventive detention. In addition to persons suspected of terrorism currently detained pursuant to executive war power privilege in Guantanamo Bay, the US has so far also detained terrorist suspects under the auspices of both administrative immigration law and criminal law. With respect to special procedure under immigration law, after the 11 September 2001 the US Congress granted the extension of pre-charge detention periods for aliens (i.e. non-citizens) suspected of terrorism. Section 1226a, Title 8, of the *United States Code* (as amended by the *USA Patriot Act*) provides for mandatory detention without charge of suspected terrorists for an initial period of 7 days (section 1226a(a)(5)). At the end of the 7-day period, the alien detainee must be either charged or removal proceedings must be commenced. Under section 1226a(a)(6), an alien who has not been removed under section 1231(a)(1)(A) of the *US Code* after 7 days, may continue to be detained if the release of the alien will threaten the national security or the safety of the community or any person. In accordance with section 1226a(a)(3), the discretion to order indefinite preventive detention of aliens suspected of terrorism rests solely with the Attorney General or the Deputy Attorney General, which must however review the detention every six months pursuant to section 1226a(7). In addition to immigration law, and as stated previously under Title (c) of the research, the US has deployed the material witness procedure to detain persons suspected of terrorism-related activity after the events of 11 September 2001. This investigative procedure allows a judge to order the detention of witnesses who possess information material to a criminal proceeding where such witnesses pose a high flight risk (section 3144 of the *US Code*). Under US federal law, the maximum period of pre-charge detention for criminal suspects is 48 hours. This limit derives from the Fourth Amendment to the *US Constitution* and also applies to persons suspected of terrorism-related offences. A 9th Circuit Court of Appeal held in *Abdullah Al-Kidd v. John Ashcroft* (580 F.3d 949, 970 (2009)) that detention by law enforcement authorities of individuals under the material witness statute for the purpose of conducting a criminal investigation, without "probable cause", is a violation of the Fourth Amendment. As a general rule, a person arrested for questioning should leave custody after 48 hours if that person is not charged within that period. However, the 9th Circuit Court in the *Al-Kidd* case admitted that a "probable cause" hearing could be permissible after 48 hours due to "bona fide emergency or other extraordinary circumstance" (*Al-Kidd* decision at paras. 56-57). ***United States Code*[70]:** **Sec. 1226a Mandatory detention of suspected terrorists; habeas corpus; judicial review** (a) Detention of terrorist aliens (1) Custody The Attorney General shall take into custody any alien who is certified under paragraph (3). (2) Release Except as provided in paragraphs (5) and (6), the Attorney General shall maintain custody of such an alien until the alien is removed from the United States. Except as provided in paragraph (6), such custody shall be maintained irrespective of any relief from removal for which the alien may be eligible, or any relief from removal granted the alien, until the Attorney General determines that the alien is no longer an alien who may be certified under paragraph (3). If the alien is finally determined not to be removable, detention pursuant to this subsection shall terminate. (3) Certification The Attorney General may certify an alien under this paragraph if the Attorney General has reasonable grounds to believe that the alien— (A) is described in section 1182 (a)(3)(A)(i), 1182 (a)(3)(A)(iii), 1182 (a)(3)(B), 1227 (a)(4)(A)(i), 1227 (a)(4)(A)(iii), or 1227 (a)(4)(B) of this title; or (B) is engaged in any other activity that endangers the national security of the United States. (4) Nondelegation The Attorney General may delegate the authority provided under paragraph (3) only to the Deputy Attorney General. The Deputy Attorney General may not delegate such authority. (5) Commencement of proceedings The Attorney General shall place an alien detained under paragraph (1) in removal proceedings, or shall charge the alien with a criminal offense, not later than 7 days after the commencement of

[70] *United States Code* (Title 8): http://www.law.cornell.edu/uscode/html/uscode08/usc_sup_01_8_10_12_20_II_30_II.html

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

such detention. If the requirement of the preceding sentence is not satisfied, the Attorney General shall release the alien.
(6) Limitation on indefinite detention
An alien detained solely under paragraph (1) who has not been removed under section 1231(a)(1)(A) of this title, and whose removal is unlikely in the reasonably foreseeable future, may be detained for additional periods of up to six months only if the release of the alien will threaten the national security of the United States or the safety of the community or any person.
(7) Review of certification
The Attorney General shall review the certification made under paragraph (3) every 6 months. If the Attorney General determines, in the Attorney General's discretion, that the certification should be revoked, the alien may be released on such conditions as the Attorney General deems appropriate, unless such release is otherwise prohibited by law. The alien may request each 6 months in writing that the Attorney General reconsider the certification and may submit documents or other evidence in support of that request.
(b) Habeas corpus and judicial review
(1) In general
Judicial review of any action or decision relating to this section (including judicial review of the merits of a determination made under subsection (a)(3) or (a)(6) of this section) is available exclusively in habeas corpus proceedings consistent with this subsection. Except as provided in the preceding sentence, no court shall have jurisdiction to review, by habeas corpus petition or otherwise, any such action or decision.
(2) Application
(A) In general
Notwithstanding any other provision of law, including section 2241 (a) of title 28, habeas corpus proceedings described in paragraph (1) may be initiated only by an application filed with—
(i) the Supreme Court;
(ii) any justice of the Supreme Court;
(iii) any circuit judge of the United States Court of Appeals for the District of Columbia Circuit; or
(iv) any district court otherwise having jurisdiction to entertain it.
(B) Application transfer
Section 2241 (b) of title 28 shall apply to an application for a writ of habeas corpus described in subparagraph (A).
(3) Appeals
Notwithstanding any other provision of law, including section 2253 of title 28, in habeas corpus proceedings described in paragraph (1) before a circuit or district judge, the final order shall be subject to review, on appeal, by the United States Court of Appeals for the District of Columbia Circuit. There shall be no right of appeal in such proceedings to any other circuit court of appeals.
(4) Rule of decision
The law applied by the Supreme Court and the United States Court of Appeals for the District of Columbia Circuit shall be regarded as the rule of decision in habeas corpus proceedings described in paragraph (1).
(c) Statutory construction
The provisions of this section shall not be applicable to any other provision of this chapter.

SUBSECTION 1226a(a)(3) REFERS *INTER ALIA* TO THE FOLLOWING PROVISIONS OF THE *US CODE*:

Sec. 1182 Inadmissible aliens
(a) Classes of aliens ineligible for visas or admission
Except as otherwise provided in this chapter, aliens who are inadmissible under the following paragraphs are ineligible to receive visas and ineligible to be admitted to the United States:
[…]
(3) Security and related grounds
(A) In general
[…]
(B) Terrorist activities
(i) In general Any alien who—
(I) has engaged in a terrorist activity;
(II) a consular officer, the Attorney General, or the Secretary of Homeland Security knows, or has reasonable ground to believe, is engaged in or is likely to engage after entry in any terrorist activity (as defined in clause (iv));
(III) has, under circumstances indicating an intention to cause death or serious bodily harm, incited terrorist activity;
(IV) is a representative (as defined in clause (v)) of—
(aa) a terrorist organization (as defined in clause (vi)); or
(bb) a political, social, or other group that endorses or espouses terrorist activity;
(V) is a member of a terrorist organization described in subclause (I) or (II) of clause (vi);
(VI) is a member of a terrorist organization described in clause (vi)(III), unless the alien can demonstrate by clear and convincing evidence that the alien did not know, and should not reasonably

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	have known, that the organization was a terrorist organization; (VII) endorses or espouses terrorist activity or persuades others to endorse or espouse terrorist activity or support a terrorist organization; (VIII) has received military-type training (as defined in section 2339D (c)(1) of title 18) from or on behalf of any organization that, at the time the training was received, was a terrorist organization (as defined in clause (vi)); or (IX) is the spouse or child of an alien who is inadmissible under this subparagraph, if the activity causing the alien to be found inadmissible occurred within the last 5 years, is inadmissible. An alien who is an officer, official, representative, or spokesman of the Palestine Liberation Organization is considered, for purposes of this chapter, to be engaged in a terrorist activity. (ii) Exception Subclause (IX) of clause (i) does not apply to a spouse or child— (I) who did not know or should not reasonably have known of the activity causing the alien to be found inadmissible under this section; or (II) whom the consular officer or Attorney General has reasonable grounds to believe has renounced the activity causing the alien to be found inadmissible under this section. (iii) "Terrorist activity" defined As used in this chapter, the term "terrorist activity" means any activity which is unlawful under the laws of the place where it is committed (or which, if it had been committed in the United States, would be unlawful under the laws of the United States or any State) and which involves any of the following: (I) The highjacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle). (II) The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained. (III) A violent attack upon an internationally protected person (as defined in section 1116 (b)(4) of title 18) or upon the liberty of such a person. (IV) An assassination. (V) The use of any— (a) biological agent, chemical agent, or nuclear weapon or device, or (b) explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property. (VI) A threat, attempt, or conspiracy to do any of the foregoing. (iv) "Engage in terrorist activity" defined As used in this chapter, the term "engage in terrorist activity" means, in an individual capacity or as a member of an organization— (I) to commit or to incite to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity; (II) to prepare or plan a terrorist activity; (III) to gather information on potential targets for terrorist activity; (IV) to solicit funds or other things of value for— (aa) a terrorist activity; (bb) a terrorist organization described in clause (vi)(I) or (vi)(II); or (cc) a terrorist organization described in clause (vi)(III), unless the solicitor can demonstrate by clear and convincing evidence that he did not know, and should not reasonably have known, that the organization was a terrorist organization; (V) to solicit any individual— (aa) to engage in conduct otherwise described in this subsection; (bb) for membership in a terrorist organization described in clause (vi)(I) or (vi)(II); or (cc) for membership in a terrorist organization described in clause (vi)(III) unless the solicitor can demonstrate by clear and convincing evidence that he did not know, and should not reasonably have known, that the organization was a terrorist organization; or (VI) to commit an act that the actor knows, or reasonably should know, affords material support, including a safe house, transportation, communications, funds, transfer of funds or other material financial benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training— (aa) for the commission of a terrorist activity; (bb) to any individual who the actor knows, or reasonably should know, has committed or plans to commit a terrorist activity; (cc) to a terrorist organization described in subclause (I) or (II) of clause (vi) or to any member of such an organization; or (dd) to a terrorist organization described in clause (vi)(III), or to any member of such an organization, unless the actor can demonstrate by clear and convincing evidence that the actor did not know, and should not reasonably have known, that the organization was a terrorist organization. (v) "Representative" defined As used in this paragraph, the term "representative" includes an officer, official, or spokesman of an organization, and any person who directs, counsels, commands, or induces an organization or its members to engage in terrorist activity. (vi) "Terrorist organization" defined As used in this section, the term "terrorist organization" means an organization— (I) designated under section 1189 of this title; (II) otherwise designated, upon publication in the Federal Register, by the Secretary of State in consultation with or upon the request of the Attorney General or the Secretary of Homeland Security, as a terrorist organization, after finding that the organization engages in the activities described in subclauses (I) through (VI) of clause (iv); or (III) that is a group of two or more individuals, whether organized or not, which engages in, or has a subgroup which engages in, the activities described in subclauses (I) through (VI) of clause (iv). […]

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Material witness procedure*"	For an explanation of the material witness procedure and relevant provisions applicable to it under the *United States Code*, please refer directly to Title (c) of the research, *supra*.
United Kingdom "*Control orders*"	The UK has shifted from an immigration detention framework to its current regime of preventive detention. The *Prevention of Terrorism Act 2005* and the *Terrorism Act 2006* were enacted to amend the *Anti-Terrorism, Crime and Security Act 2001* (*ATCSA*), the legislation that previously governed the detention of terrorist suspects in the UK. The *ATCSA* broadened police powers to combat terrorism (previously enumerated in the *Terrorism Act 2000*), and granted the Home Secretary the power to "certify" foreign nationals who were suspected of terrorism. Once an individual had been certified, that individual could be repatriated. However, if the conditions were such that upon repatriation the individual might face torture or other forms of ill treatment upon his or her return, that individual could be detained until such conditions changed (i.e. potentially indefinitely) or until another country indicated that it was willing to receive the suspected individual. After detainees challenged the lawfulness of their detention under this framework, the House of Lords hold that sections of the *ATCSA* were incompatible with the UK pre-existing human rights commitments under Article 5 (right to liberty and security) of the *European Convention on Human Rights* (*ECHR*). The UK government responded to this ruling in repealing Part 4 of the *ATCSA* and introducing the *Prevention of Terrorism Act 2005*, which provides for UK current regime of detention of terrorist suspects under "control orders". Against this legislative backdrop, the *Terrorism Act 2006* was also enacted and provides for enhanced provisions for the detention of individuals arrested under section 41 of the *Terrorism Act 2000* (criminal law pre-charge detention). According to the *Terrorism Act 2006*, UK authorities may detain, without charge, persons suspected of involvement in terrorism or terrorism-related activities for an initial period of 48 hours, and, with judicial authorisation, may detain those persons for an additional period of up to 28 days. Details on the control orders procedure and the detention of terrorist suspects without charge are provided below. CONTROL ORDERS: The *Prevention of Terrorism Act 2005* provides for the imposition of control orders upon those believed to be involved in terrorism-related activity. A control order is a preventative order which impose one or more obligations upon an individual which are designed to prevent, restrict or disrupt his or her involvement in terrorist activity. A range of possible obligations may be imposed by the control order, so each order will be tailored to the particular risk posed by the individual concerned. Under UK law, control orders can be imposed on any person suspected of involvement in terrorist-related activity irrespective of nationality. There are two types of control orders: control orders which impose obligations that do not require derogation from Article 5 of the *ECHR* (non-derogating control orders), and control orders that can be made only if the necessary derogation from the *ECHR* is in place (derogating control orders). ***Prevention of Terrorism Act 2005***[71]**:** **Sec. 1 Power to make control orders** (1) In this Act "control order" means an order against an individual that imposes obligations on him for purposes connected with protecting members of the public from a risk of terrorism. (2) The power to make a control order against an individual shall be exercisable— (a) except in the case of an order imposing obligations that are incompatible with the individual's right to liberty under Article 5 of the Human Rights Convention, by the Secretary of State; and (b) in the case of an order imposing obligations that are or include derogating obligations, by the court on an application by the Secretary of State. (3) The obligations that may be imposed by a control order made against an individual are any obligations that the Secretary of State or (as the case may be) the court considers necessary for purposes connected with preventing or restricting involvement by that individual in terrorism-related activity. (4) Those obligations may include, in particular— (a) a prohibition or restriction on his possession or use of specified articles or substances; (b) a prohibition or restriction on his use of specified services or specified facilities, or on his carrying on specified activities; (c) a restriction in respect of his work or other occupation, or in respect of his business; (d) a restriction on his association or communications with specified persons or with other persons generally; (e) a restriction in respect of his place of residence or on the persons to whom he gives access to his place of residence; (f) a prohibition on his being at specified places or within a specified area at specified times or on specified days; (g) a prohibition or restriction on his movements to, from or within the United Kingdom, a specified part of the United Kingdom or a specified place or area within the United Kingdom; (h) a requirement on him to comply with such other prohibitions or restrictions on his movements as may be imposed, for a period not exceeding 24 hours, by directions given to him in the specified manner, by a specified person and for the purpose of securing compliance with other obligations imposed by or under the order; (i) a requirement on him to surrender his passport, or anything in his possession to which a prohibition or restriction imposed by the order relates, to a specified person for a period not exceeding the period for which the order remains in force; (j) a requirement on him to give access to specified persons to his place of residence or to other premises to which he has power to grant access; (k) a requirement on him to allow specified persons to search that place or any such premises for the purpose of ascertaining whether obligations imposed by or under the order have been, are being or are about to be contravened; (l) a requirement on him to allow specified persons, either for that purpose or for the purpose of securing that the order is complied with, to remove anything found in that place or on any such

[71] UK *Prevention of Terrorism Act 2005*: http://www.legislation.gov.uk/ukpga/2005/2/contents

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	premises and to subject it to tests or to retain it for a period not exceeding the period for which the order remains in force; (m) a requirement on him to allow himself to be photographed; (n) a requirement on him to co-operate with specified arrangements for enabling his movements, communications or other activities to be monitored by electronic or other means; (o) a requirement on him to comply with a demand made in the specified manner to provide information to a specified person in accordance with the demand; (p) a requirement on him to report to a specified person at specified times and places. (5) Power by or under a control order to prohibit or restrict the controlled person's movements includes, in particular, power to impose a requirement on him to remain at or within a particular place or area (whether for a particular period or at particular times or generally). (6) The reference in subsection (4)(n) to co-operating with specified arrangements for monitoring includes a reference to each of the following— (a) submitting to procedures required by the arrangements; (b) wearing or otherwise using apparatus approved by or in accordance with the arrangements; (c) maintaining such apparatus in the specified manner; (d) complying with directions given by persons carrying out functions for the purposes of those arrangements. (7) The information that the controlled person may be required to provide under a control order includes, in particular, advance information about his proposed movements or other activities. (8) A control order may provide for a prohibition, restriction or requirement imposed by or under the order to apply only where a specified person has not given his consent or approval to what would otherwise contravene the prohibition, restriction or requirement. (9) For the purposes of this Act involvement in terrorism-related activity is any one or more of the following— (a) the commission, preparation or instigation of acts of terrorism; (b) conduct which facilitates the commission, preparation or instigation of such acts, or which is intended to do so; (c) conduct which gives encouragement to the commission, preparation or instigation of such acts, or which is intended to do so; (d) conduct which gives support or assistance to individuals who are known or believed to be involved in terrorism-related activity; and for the purposes of this subsection it is immaterial whether the acts of terrorism in question are specific acts of terrorism or acts of terrorism generally. (10) In this Act— "derogating obligation" means an obligation on an individual which (a) is incompatible with his right to liberty under Article 5 of the Human Rights Convention; but (b) is of a description of obligations which, for the purposes of the designation of a designated derogation, is set out in the designation order; "designated derogation" has the same meaning as in the Human Rights Act 1998 (c. 42) (see section 14(1) of that Act); "designation order", in relation to a designated derogation, means the order under section 14(1) of the Human Rights Act 1998 by which the derogation is designated.
"*Non-derogating control orders*"	**Sec. 2 Making of non-derogating control orders** (1) The Secretary of State may make a control order against an individual if he— (a) has reasonable grounds for suspecting that the individual is or has been involved in terrorism-related activity; and (b) considers that it is necessary, for purposes connected with protecting members of the public from a risk of terrorism, to make a control order imposing obligations on that individual. (2) The Secretary of State may make a control order against an individual who is for the time being bound by a control order made by the court only if he does so— (a) after the court has determined that its order should be revoked; but (b) while the effect of the revocation has been postponed for the purpose of giving the Secretary of State an opportunity to decide whether to exercise his own powers to make a control order against the individual. (3) A control order made by the Secretary of State is called a non-derogating control order. (4) A non-derogating control order— (a) has effect for a period of 12 months beginning with the day on which it is made; but (b) may be renewed on one or more occasions in accordance with this section. (5) A non-derogating control order must specify when the period for which it is to have effect will end. (6) The Secretary of State may renew a non-derogating control order (with or without modifications) for a period of 12 months if he— (a) considers that it is necessary, for purposes connected with protecting members of the public from a risk of terrorism, for an order imposing obligations on the controlled person to continue in force; and (b) considers that the obligations to be imposed by the renewed order are necessary for purposes connected with preventing or restricting involvement by that person in terrorism-related activity.

[72] UK *Police and Criminal Evidence Act 1984*: http://www.legislation.gov.uk/ukpga/1984/60/contents
[73] On this subject, please see: http://www.homeoffice.gov.uk/police/powers/pace-codes/
[74] UK *Terrorism Act 2000* (Schedule 8 as modified by the *Terrorism Act 2006*): http://www.legislation.gov.uk/ukpga/2000/11/schedule/8
[75] UK *Terrorism Act 2000*: http://www.legislation.gov.uk/ukpga/2000/11/contents
[76] UK *Terrorism Act 2006*: http://www.legislation.gov.uk/ukpga/2006/11/contents

000479

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Derogating control orders*"	(7) Where the Secretary of State renews a non-derogating control order, the 12 month period of the renewal begins to run from whichever is the earlier of— (a) the time when the order would otherwise have ceased to have effect; or (b) the beginning of the seventh day after the date of renewal. (8) The instrument renewing a non-derogating control order must specify when the period for which it is renewed will end. (9) It shall be immaterial, for the purposes of determining what obligations may be imposed by a control order made by the Secretary of State, whether the involvement in terrorism-related activity to be prevented or restricted by the obligations is connected with matters to which the Secretary of State's grounds for suspicion relate. **Sec. 4 Power of court to make derogating control orders** (1) On an application to the court by the Secretary of State for the making of a control order against an individual, it shall be the duty of the court— (a) to hold an immediate preliminary hearing to determine whether to make a control order imposing obligations that are or include derogating obligations (called a "derogating control order") against that individual; and (b) if it does make such an order against that individual, to give directions for the holding of a full hearing to determine whether to confirm the order (with or without modifications). (2) The preliminary hearing under subsection (1)(a) may be held— (a) in the absence of the individual in question; (b) without his having had notice of the application for the order; and (c) without his having been given an opportunity (if he was aware of the application) of making any representations to the court; but this subsection is not to be construed as limiting the matters about which rules of court may be made in relation to that hearing. (3) At the preliminary hearing, the court may make a control order against the individual in question if it appears to the court— (a) that there is material which (if not disproved) is capable of being relied on by the court as establishing that the individual is or has been involved in terrorism-related activity; (b) that there are reasonable grounds for believing that the imposition of obligations on that individual is necessary for purposes connected with protecting members of the public from a risk of terrorism; (c) that the risk arises out of, or is associated with, a public emergency in respect of which there is a designated derogation from the whole or a part of Article 5 of the Human Rights Convention; and (d) that the obligations that there are reasonable grounds for believing should be imposed on the individual are or include derogating obligations of a description set out for the purposes of the designated derogation in the designation order. (4) The obligations that may be imposed by a derogating control order in the period between— (a) the time when the order is made, and (b) the time when a final determination is made by the court whether to confirm it, include any obligations which the court has reasonable grounds for considering are necessary as mentioned in section 1(3). (5) At the full hearing under subsection (1)(b), the court may— (a) confirm the control order made by the court; or (b) revoke the order; and where the court revokes the order, it may (if it thinks fit) direct that this Act is to have effect as if the order had been quashed. (6) In confirming a control order, the court— (a) may modify the obligations imposed by the order; and (b) where a modification made by the court removes an obligation, may (if it thinks fit) direct that this Act is to have effect as if the removed obligation had been quashed. (7) At the full hearing, the court may confirm the control order (with or without modifications) only if— (a) it is satisfied, on the balance of probabilities, that the controlled person is an individual who is or has been involved in terrorism-related activity; (b) it considers that the imposition of obligations on the controlled person is necessary for purposes connected with protecting members of the public from a risk of terrorism; (c) it appears to the court that the risk is one arising out of, or is associated with, a public emergency in respect of which there is a designated derogation from the whole or a part of Article 5 of the Human Rights Convention; and (d) the obligations to be imposed by the order or (as the case may be) by the order as modified are or include derogating obligations of a description set out for the purposes of the designated derogation in the designation order. (8) A derogating control order ceases to have effect at the end of the period of 6 months beginning with the day on which it is made unless— (a) it is previously revoked (whether at the hearing under subsection (1)(b) or otherwise under this Act); (b) it ceases to have effect under section 6; or (c) it is renewed. (9) The court, on an application by the Secretary of State, may renew a derogating control order (with or without modifications) for a period of 6 months from whichever is the earlier of— (a) the time when the order would otherwise have ceased to have effect; and (b) the beginning of the seventh day after the date of renewal. (10) The power of the court to renew a derogating control order is exercisable on as many occasions as the court thinks fit; but, on each occasion, it is exercisable only if—

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Arrest and detention pending derogating control order*"	(a) the court considers that it is necessary, for purposes connected with protecting members of the public from a risk of terrorism, for a derogating control order to continue in force against the controlled person; (b) it appears to the court that the risk is one arising out of, or is associated with, a public emergency in respect of which there is a designated derogation from the whole or a part of Article 5 of the Human Rights Convention; (c) the derogating obligations that the court considers should continue in force are of a description that continues to be set out for the purposes of the designated derogation in the designation order; and (d) the court considers that the obligations to be imposed by the renewed order are necessary for purposes connected with preventing or restricting involvement by that person in terrorism-related activity. (11) Where, on an application for the renewal of a derogating control order, it appears to the court— (a) that the proceedings on the application are unlikely to be completed before the time when the order is due to cease to have effect if not renewed, and (b) that that is not attributable to an unreasonable delay on the part of the Secretary of State in the making or conduct of the application, the court may (on one or more occasions) extend the period for which the order is to remain in force for the purpose of keeping it in force until the conclusion of the proceedings. (12) Where the court exercises its power under subsection (11) and subsequently renews the control order in question, the period of any renewal still runs from the time when the order would have ceased to have effect apart from that subsection. (13) It shall be immaterial, for the purposes of determining what obligations may be imposed by a control order made by the court, whether the involvement in terrorism-related activity to be prevented or restricted by the obligations is connected with matters in relation to which the requirements of subsection (3)(a) or (7)(a) were satisfied. **Sec. 5 Arrest and detention pending derogating control order** (1) A constable may arrest and detain an individual if— (a) the Secretary of State has made an application to the court for a derogating control order to be made against that individual; and (b) the constable considers that the individual's arrest and detention is necessary to ensure that he is available to be given notice of the order if it is made. (2) A constable who has arrested an individual under this section must take him to the designated place that the constable considers most appropriate as soon as practicable after the arrest. (3) An individual taken to a designated place under this section may be detained there until the end of 48 hours from the time of his arrest. (4) If the court considers that it is necessary to do so to ensure that the individual in question is available to be given notice of any derogating control order that is made against him, it may, during the 48 hours following his arrest, extend the period for which the individual may be detained under this section by a period of no more than 48 hours. (5) An individual may not be detained under this section at any time after— (a) he has become bound by a derogating control order made against him on the Secretary of State's application; or (b) the court has dismissed the application. (6) A person who has the powers of a constable in one part of the United Kingdom may exercise the power of arrest under this section in that part of the United Kingdom or in any other part of the United Kingdom. (7) An individual detained under this section— (a) shall be deemed to be in legal custody throughout the period of his detention; and (b) after having been taken to a designated place shall be deemed— (i) in England and Wales, to be in police detention for the purposes of the Police and Criminal Evidence Act 1984 (c. 60); and (ii) in Northern Ireland, to be in police detention for the purposes of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989/1341 (N.I. 12)); but paragraph (b) has effect subject to subsection (8). (8) Paragraphs 1(6), 2, 6 to 9 and 16 to 19 of Schedule 8 to the Terrorism Act 2000 (c. 11) (powers and safeguards in the case of persons detained under section 41 of that Act) apply to an individual detained under this section as they apply to a person detained under section 41 of that Act, but with the following modifications— (a) the omission of paragraph 2(2)(b) to (d) (which confers powers on persons specified by the Secretary of State, prison officers and examining officers); (b) the omission of paragraph 8(2), (5) and (5A) (which relates to the postponement of a person's rights in England and Wales or Northern Ireland); and (c) the omission of paragraphs 16(9) and 17(4) and (4A) (which make similar provision for Scotland). (9) The power to detain an individual under this section includes power to detain him in a manner that is incompatible with his right to liberty under Article 5 of the Human Rights Convention if, and only if— (a) there is a designated derogation in respect of the detention of individuals under this section in connection with the making of applications for derogating control orders; and (b) that derogation and the designated derogation relating to the power to make the orders applied for are designated in respect of the same public emergency. (10) In this section "designated place" means any place which the Secretary of State has designated under paragraph 1(1) of Schedule 8 to the Terrorism Act 2000 (c. 11) as a place at which persons may be detained under section 41 of that Act. [*Please also refer to sections 3, and 6 to 9 of the* Prevention of Terrorism Act 2005].

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

"*Special detention of terrorist suspects without charge*"	SPECIAL PRE-CHARGE DETENTION: The *Terrorism Act 2000* allows a constable to arrest a person reasonably suspected by him or her of being a terrorist. Once arrested, custody procedure is based on the *Police and Criminal Evidence Act 1984*[72], and the associated Codes of practice.[73] Schedule 8 to the *Terrorism Act 2000* provides enhanced and specific provisions for detention of individuals arrested under section 41 of that *Act*.[74] The *Terrorism Act 2006* extends the maximum period that a terrorist suspect can be held prior to charge to 28 days. The *Protection of Freedoms Bill* currently before the UK Parliament provides for the repeal of the provisions in the *Terrorism Act 2006* that allow the maximum period of pre-charge detention under Schedule 8 to the *Terrorism Act* to be set at 28 days. For additional information on this *Bill*, please refer directly to Chart e.2 under Title (e) of the research, *infra*. ***Terrorism Act 2000*[75]:** **Sec. 41 Arrest without warrant** (1) A constable may arrest without a warrant a person whom he reasonably suspects to be a terrorist. (2) Where a person is arrested under this section the provisions of Schedule 8 (detention: treatment, review and extension) shall apply. (3) Subject to subsections (4) to (7), a person detained under this section shall (unless detained under any other power) be released not later than the end of the period of 48 hours beginning— (a) with the time of his arrest under this section, or (b) if he was being detained under Schedule 7 when he was arrested under this section, with the time when his examination under that Schedule began. (4) If on a review of a person's detention under Part II of Schedule 8 the review officer does not authorise continued detention, the person shall (unless detained in accordance with subsection (5) or (6) or under any other power) be released. (5) Where a police officer intends to make an application for a warrant under paragraph 29 of Schedule 8 extending a person's detention, the person may be detained pending the making of the application. (6) Where an application has been made under paragraph 29 or 36 of Schedule 8 in respect of a person's detention, he may be detained pending the conclusion of proceedings on the application. (7) Where an application under paragraph 29 or 36 of Schedule 8 is granted in respect of a person's detention, he may be detained, subject to paragraph 37 of that Schedule, during the period specified in the warrant. (8) The refusal of an application in respect of a person's detention under paragraph 29 or 36 of Schedule 8 shall not prevent his continued detention in accordance with this section. (9) A person who has the powers of a constable in one Part of the United Kingdom may exercise the power under subsection (1) in any Part of the United Kingdom. ***Terrorism Act 2006*[76]:** **Sec. 23 Extension of period of detention of terrorist suspects** (1) Schedule 8 to the Terrorism Act 2000 (c. 11) (detention of terrorist suspects) is amended as follows. (2) In sub-paragraph (1) of each of paragraphs 29 and 36 (applications by a superintendent or above for a warrant extending detention or for the extension of the period of such a warrant), for the words from the beginning to "may" substitute— "(1) Each of the following— (a) in England and Wales, a Crown Prosecutor, (b) in Scotland, the Lord Advocate or a procurator fiscal, (c) in Northern Ireland, the Director of Public Prosecutions for Northern Ireland, (d) in any part of the United Kingdom, a police officer of at least the rank of superintendent, may". (3) In sub-paragraph (3) of paragraph 29 (period of extension to end no later than 7 days after arrest)— (a) for "Subject to paragraph 36(3A)" substitute " Subject to sub-paragraph (3A) and paragraph 36"; and (b) for "end not later than the end of" substitute " be". (4) After that sub-paragraph insert— "(3A) A judicial authority may issue a warrant of further detention in relation to a person which specifies a shorter period as the period for which that person's further detention is authorised if— (a) the application for the warrant is an application for a warrant specifying a shorter period; or (b) the judicial authority is satisfied that there are circumstances that would make it inappropriate for the specified period to be as long as the period of seven days mentioned in sub-paragraph (3)." (5) In paragraph 34(1) (persons who can apply for information to be withheld from person to whom application for a warrant relates) for "officer" substitute " person". (6) In paragraph 36(applications for extension or further extension), omit the words "to a judicial authority" in sub-paragraph (1), and after that sub-paragraph insert— "(1A) The person to whom an application under sub-paragraph (1) may be made is— (a) in the case of an application falling within sub-paragraph (1B), a judicial authority; and (b) in any other case, a senior judge. (1B) An application for the extension or further extension of a period falls within this sub-paragraph if— (a) the grant of the application otherwise than in accordance with sub-paragraph (3AA)(b) would extend that period to a time that is no more than fourteen days after the relevant time; and (b) no application has previously been made to a senior judge in respect of that period."

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(7) For sub-paragraphs (3) and (3A) of that paragraph (period for which warrants may be extended) substitute— "(3) Subject to sub-paragraph (3AA), the period by which the specified period is extended or further extended shall be the period which— (a) begins with the time specified in sub-paragraph (3A); and (b) ends with whichever is the earlier of— (i) the end of the period of seven days beginning with that time; and (ii) the end of the period of 28 days beginning with the relevant time. (3A) The time referred to in sub-paragraph (3)(a) is— (a) in the case of a warrant specifying a period which has not previously been extended under this paragraph, the end of the period specified in the warrant, and (b) in any other case, the end of the period for which the period specified in the warrant was last extended under this paragraph. (3AA) A judicial authority or senior judge may extend or further extend the period specified in a warrant by a shorter period than is required by sub-paragraph (3) if— (a) the application for the extension is an application for an extension by a period that is shorter than is so required; or (b) the judicial authority or senior judge is satisfied that there are circumstances that would make it inappropriate for the period of the extension to be as long as the period so required." (8) In sub-paragraph (4) of that paragraph (application of paragraphs 30(3), and 31 to 34), at the end insert "but, in relation to an application made by virtue of sub-paragraph (1A)(b) to a senior judge, as if— (a) references to a judicial authority were references to a senior judge; and (b) references to the judicial authority in question were references to the senior judge in question." (9) In sub-paragraph (5) of that paragraph, after "authority" insert " or senior judge". (10) After sub-paragraph (6) of that paragraph insert— "(7) In this paragraph and paragraph 37 'senior judge' means a judge of the High Court or of the High Court of Justiciary." (11) For paragraph 37 (release of detained person) substitute— "37 (1) This paragraph applies where— (a) a person ('the detained person') is detained by virtue of a warrant issued under this Part of this Schedule; and (b) his detention is not authorised by virtue of section 41(5) or (6) or otherwise apart from the warrant. (2) If it at any time appears to the police officer or other person in charge of the detained person's case that any of the matters mentioned in paragraph 32(1)(a) and (b) on which the judicial authority or senior judge last authorised his further detention no longer apply, he must— (a) if he has custody of the detained person, release him immediately; and (b) if he does not, immediately inform the person who does have custody of the detained person that those matters no longer apply in the detained person's case. (3) A person with custody of the detained person who is informed in accordance with this paragraph that those matters no longer apply in his case must release that person immediately." (12) This section does not apply in a case in which— (a) the arrest of the person detained under section 41 of the Terrorism Act 2000 (c. 11) took place before the commencement of this section; or (b) his examination under Schedule 7 to that Act began before the commencement of this section. **Sec. 24 Grounds for extending detention** (1) In Schedule 8 to the Terrorism Act 2000, in paragraph 23(1) (grounds on which a review officer may authorise continued detention), after paragraph (b) insert— "(ba) pending the result of an examination or analysis of any relevant evidence or of anything the examination or analysis of which is to be or is being carried out with a view to obtaining relevant evidence;". (2) In sub-paragraph (1) of paragraph 32 of that Schedule (grounds on which a judicial authority may authorise further detention), for the words from "to obtain" to "preserve relevant evidence" substitute " as mentioned in sub-paragraph (1A)". (3) After that sub-paragraph insert— "(1A) The further detention of a person is necessary as mentioned in this sub-paragraph if it is necessary— (a) to obtain relevant evidence whether by questioning him or otherwise; (b) to preserve relevant evidence; or (c) pending the result of an examination or analysis of any relevant evidence or of anything the examination or analysis of which is to be or is being carried out with a view to obtaining relevant evidence." (4) In paragraph 23(4) (meaning of "relevant evidence"), for "sub-paragraph (1)(a) and (b)" substitute " this paragraph". (5) In paragraph 32(2) (meaning of "relevant evidence"), for "sub-paragraph (1)" substitute " this paragraph". (6) This section does not apply in a case in which— (a) the arrest of the person detained under section 41 of the Terrorism Act 2000 took place before the commencement of this section; or (b) his examination under Schedule 7 to that Act began before the commencement of this section.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	Sec. 25 Expiry or renewal of extended maximum detention period (1) This section applies to any time which— (a) is more than one year after the commencement of section 23; and (b) does not fall within a period in relation to which this section is disapplied by an order under subsection (2). (2) The Secretary of State may by order made by statutory instrument disapply this section in relation to any period of not more than one year beginning with the coming into force of the order. (3) Schedule 8 to the Terrorism Act 2000 (c. 11) has effect in relation to any further extension under paragraph 36 of that Schedule for a period beginning at a time to which this section applies— (a) as if in sub-paragraph (3)(b) of that paragraph, for "28 days" there were substituted " 14 days"; and (b) as if that paragraph and paragraph 37 of that Schedule had effect with the further consequential modifications set out in subsection (4). (4) The further consequential modifications are— (a) the substitution of the words "a judicial authority" for paragraphs (a) and (b) of sub-paragraph (1A) of paragraph 36; (b) the omission of sub-paragraphs (1B) and (7) of that paragraph; (c) the omission of the words "or senior judge" wherever occurring in sub-paragraphs (3AA) and (5) of that paragraph and in paragraph 37(2); and (d) the omission of the words from "but" onwards in paragraph 36(4). (5) Where at a time to which this section applies— (a) a person is being detained by virtue of a further extension under paragraph 36 of Schedule 8 to the Terrorism Act 2000, (b) his further detention was authorised (at a time to which this section did not apply) for a period ending more than 14 days after the relevant time, and (c) that 14 days has expired, the person with custody of that individual must release him immediately. (6) The Secretary of State must not make an order containing (with or without other provision) any provision disapplying this section in relation to any period unless a draft of the order has been laid before Parliament and approved by a resolution of each House. (7) In this section "the relevant time" has the same meaning as in paragraph 36 of Schedule 8 to the Terrorism Act 2000.
Australia	The *Anti-Terrorism Act (No. 2) 2005* introduced new divisions into Australia's *Criminal Code Act 1995* allowing for control orders (Division 104 of the *Code*) and preventive detention orders (Division 105 of the *Code*) to be issued against terrorist suspects. These orders are not predicated on immigration status, nor are they issued pursuant to an ongoing investigation leading to criminal trial; they are solely determined by national security concerns. With respect to preventive detention orders, the relevant provisions of the *Criminal Code Act 1995* provide for the detention of a person for up to 72 hours without charge where it is reasonably necessary to prevent a terrorist activity. The consent of the Attorney General is not required, and senior members of the Australian Federal Police (AFP) are permitted to issue an initial preventive detention order ordering the detention of a suspect for up to 24 hours and to issue continued preventive order, which may last for a further period of up to 48 hours from the time when the suspect was first detained. This period of detention can be extended by individual states' legislation. The control orders procedure provides for the monitoring of terrorist suspects who pose a risk to the community. These orders can be granted on the basis that they would assist in preventing a terrorist act or when a person has trained with a terrorist organisation. Unlike preventive detention orders, control orders can only be made with the Attorney General's consent and only be issued by a judge for a period of 12 months. The legislation specifically lists possible conditions that may accompany such orders, including wearing a tracking device, prohibition from using specific forms of telecommunication technologies (like the Internet), and not associating with specific individuals. In 2007, the Australian High Court upheld the constitutional validity of control orders (*Thomas v. Mowbray* [2007] HCA 33 (2 August 2007)). The doctrine suggests that the limited rights available to individuals detained pursuant to such orders ensure that Australia's special detention regime for terrorist suspects fits within the national security detention framework, although the limited period of time during which an individual may be detained separates Australia from the general approach to national security detention followed by other countries (Burch Elias, at 186). With respect to special pre-charge detention under criminal law, a person arrested for a terrorism offence can be detained for no more than 4 hours from the time of arrest for the purpose of investigation. The detainee must be released within the period or brought before a judicial officer. In terrorism cases the pre-charge detention period can be extended a number of times to a total of 20 hours on application by the investigating official to a magistrate. However, "dead time" is not included in these periods of reference ("dead time" is time that may be disregarded pursuant to section 23DB(9) of the *Crimes Act 1914*). As a result, "dead time" can allow a person to be detained longer than 20 hours in practice, but the total amount of time spent questioning the person (investigation period) cannot in any case be longer than 20 hours. The *National Security Legislation Amendment Act 2010* introduced a statutory limitation on the maximum amount of "dead time" that can be authorised. Under section 23DB(11) of that *Act*, "dead time" is not allowed by Australian law beyond a 7 days period.
"*Control orders*"	CONTROL ORDERS ***Criminal Code Act 1995***[77]**:** **Sec. 104.1 Object of this Division** The object of this Division is to allow obligations, prohibitions and restrictions to be imposed on a person by a control order for the purpose of protecting the public from a terrorist act.

[77] Australian *Criminal Code Act 1995* (as modified by the *Anti-Terrorism Act (No. 2) 2005*): http://www.comlaw.gov.au/Details/C2011C00123

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

Sec. 104.2 Attorney-General's consent to request an interim control order
(1) A senior AFP member must not request an interim control order in relation to a person without the Attorney-General's written consent.
Note: However, in urgent circumstances, a senior AFP member may request an interim control order without first obtaining the Attorney-General's consent (see Subdivision C).
(2) A senior AFP member may only seek the Attorney-General's written consent to request an interim control order in relation to a person if the member:
(a) considers on reasonable grounds that the order in the terms to be requested would substantially assist in preventing a terrorist act; or
(b) suspects on reasonable grounds that the person has provided training to, or received training from, a listed terrorist organisation.
(3) In seeking the Attorney-General's consent, the member must give the Attorney-General a draft request that includes:
(a) a draft of the interim control order to be requested; and
(b) the following:
(i) a statement of the facts relating to why the order should be made;
(ii) if the member is aware of any facts relating to why the order should not be made—a statement of those facts; and
(c) the following:
(i) an explanation as to why each of the obligations, prohibitions and restrictions should be imposed on the person;
(ii) if the member is aware of any facts relating to why any of those obligations, prohibitions or restrictions should not be imposed on the person—a statement of those facts; and
(d) the following:
(i) the outcomes and particulars of all previous requests for interim control orders (including the outcomes of the hearings to confirm the orders) in relation to the person;
(ii) the outcomes and particulars of all previous applications for variations of control orders made in relation to the person;
(iii) the outcomes of all previous applications for revocations of control orders made in relation to the person;
(iv) the outcomes and particulars of all previous applications for preventative detention orders in relation to the person;
(v) information (if any) that the member has about any periods for which the person has been detained under an order made under a corresponding State preventative detention law; and
(e) information (if any) that the member has about the person's age; and
(f) a summary of the grounds on which the order should be made.
Note 1: An interim control order cannot be requested in relation to a person who is under 16 years of age (see section 104.28).
Note 2: The member might commit an offence if the draft request is false or misleading (see sections 137.1 and 137.2).
(3A) To avoid doubt, paragraph (3)(f) does not require any information to be included in the summary if disclosure of that information is likely to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004).
(4) The Attorney-General's consent may be made subject to changes being made to the draft request (including the draft of the interim control order to be requested).
(5) To avoid doubt, a senior AFP member may seek the Attorney-General's consent to request an interim control order in relation to a person, even if such a request has previously been made in relation to the person.

Sec. 104.3 Requesting the court to make an interim control order
If the Attorney-General consents to the request under section 104.2, the senior AFP member may request the interim control order by giving an issuing court:
(a) a request:
(i) that is the same as the draft request, except for the changes (if any) required by the Attorney-General; and
(ii) the information in which is sworn or affirmed by the member; and
(b) a copy of the Attorney-General's consent.
Note: The member might commit an offence if the request is false or misleading (see sections 137.1 and 137.2).

Sec. 104.4 Making an interim control order
(1) The issuing court may make an order under this section in relation to the person, but only if:
(a) the senior AFP member has requested it in accordance with section 104.3; and
(b) the court has received and considered such further information (if any) as the court requires; and
(c) the court is satisfied on the balance of probabilities:
(i) that making the order would substantially assist in preventing a terrorist act; or
(ii) that the person has provided training to, or received training from, a listed terrorist organisation; and
(d) the court is satisfied on the balance of probabilities that each of the obligations, prohibitions and restrictions to be imposed on the person by the order is reasonably necessary, and reasonably appropriate and adapted, for the purpose of protecting the public from a terrorist act.
(2) In determining whether each of the obligations, prohibitions and restrictions to be imposed on the person by the order is reasonably necessary, and reasonably appropriate and adapted, the

[78] Australia *Crimes Act 1914*: http://www.comlaw.gov.au/Details/C2011C00233

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	court must take into account the impact of the obligation, prohibition or restriction on the person's circumstances (including the person's financial and personal circumstances). (3) The court need not include in the order an obligation, prohibition or restriction that was sought by the senior AFP member if the court is not satisfied as mentioned in paragraph (1)(d) in respect of that obligation, prohibition or restriction. **Sec. 104.5 Terms of an interim control order** (1) If the issuing court makes the interim control order, the order must: (a) state that the court is satisfied of the matters mentioned in paragraphs 104.4(1)(c) and (d); and (b) specify the name of the person to whom the order relates; and (c) specify all of the obligations, prohibitions and restrictions mentioned in subsection (3) that are to be imposed on the person by the order; and (d) state that the order does not begin to be in force until it is served personally on the person; and (e) specify a day on which the person may attend the court for the court to: (i) confirm (with or without variation) the interim control order; or (ii) declare the interim control order to be void; or (iii) revoke the interim control order; and (f) specify the period during which the confirmed control order is to be in force, which must not end more than 12 months after the day on which the interim control order is made; and (g) state that the person's lawyer may attend a specified place in order to obtain a copy of the interim control order; and (h) set out a summary of the grounds on which the order is made. (1A) The day specified for the purposes of paragraph (1)(e) must be as soon as practicable, but at least 72 hours, after the order is made. (2) Paragraph (1)(f) does not prevent the making of successive control orders in relation to the same person. (2A) To avoid doubt, paragraph (1)(h) does not require any information to be included in the summary if disclosure of that information is likely to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004). Obligations, prohibitions and restrictions (3) The obligations, prohibitions and restrictions that the court may impose on the person by the order are the following: (a) a prohibition or restriction on the person being at specified areas or places; (b) a prohibition or restriction on the person leaving Australia; (c) a requirement that the person remain at specified premises between specified times each day, or on specified days; (d) a requirement that the person wear a tracking device; (e) a prohibition or restriction on the person communicating or associating with specified individuals; (f) a prohibition or restriction on the person accessing or using specified forms of telecommunication or other technology (including the internet); (g) a prohibition or restriction on the person possessing or using specified articles or substances; (h) a prohibition or restriction on the person carrying out specified activities (including in respect of his or her work or occupation); (i) a requirement that the person report to specified persons at specified times and places; (j) a requirement that the person allow himself or herself to be photographed; (k) a requirement that the person allow impressions of his or her fingerprints to be taken; (l) a requirement that the person participate in specified counselling or education. Communicating and associating (4) Subsection 102.8(4) applies to paragraph (3)(e) and the person's communication or association in the same way as that subsection applies to section 102.8 and a person's association. (5) This section does not affect the person's right to contact, communicate or associate with the person's lawyer unless the person's lawyer is a specified individual as mentioned in paragraph (3)(e). If the person's lawyer is so specified, the person may contact, communicate or associate with any other lawyer who is not so specified. Counselling and education (6) A person is required to participate in specified counselling or education as mentioned in paragraph (3)(l) only if the person agrees, at the time of the counselling or education, to participate in the counselling or education.
"*Urgent control orders*"	URGENT CONTROL ORDERS ***Criminal Code Act 1995*:** **Sec. 104.6 Requesting an urgent interim control order by electronic means** (1) A senior AFP member may request, by telephone, fax, email or other electronic means, an issuing court to make an interim control order in relation to a person if: (a) the member considers it necessary to use such means because of urgent circumstances; and (b) the member either considers or suspects the matters mentioned in subsection 104.2(2) on reasonable grounds.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(2) The Attorney-General's consent under section 104.2 is not required before the request is made.
Note: However, if the Attorney-General's consent is not obtained before the member makes the request, the Attorney-General's consent must be obtained within 4 hours of the member making the request (see section 104.10).
(3) The issuing court may require communication by voice to the extent that is practicable in the circumstances.
(4) The request must include the following:
(a) all that is required under subsection 104.2(3) in respect of an ordinary request for an interim control order (including, if the Attorney-General's consent has been obtained before making the request, the changes (if any) required by the Attorney-General);
(b) an explanation as to why the making of the interim control order is urgent;
(c) if the Attorney-General's consent has been obtained before making the request—a copy of the Attorney-General's consent.
Note: The member might commit an offence if the request is false or misleading (see sections 137.1 and 137.2).
(5) The information and the explanation included in the request must be sworn or affirmed by the member, but do not have to be sworn or affirmed before the request is made.
Note: Subsection 104.7(5) requires the information and the explanation to be sworn or affirmed within 24 hours.

Sec. 104.7 Making an urgent interim control order by electronic means
(1) Before making an order in response to a request under section 104.6, the issuing court must:
(a) consider the information and the explanation included in the request; and
(b) receive and consider such further information (if any) as the court requires.
(2) If the issuing court is satisfied that an order should be made urgently, the court may complete the same form of order that would be made under sections 104.4 and 104.5.
Procedure after urgent interim control order is made
(3) If the issuing court makes the order, the court must inform the senior AFP member, by telephone, fax, email or other electronic means, of:
(a) the terms of the order; and
(b) the day on which, and the time at which, it was completed.
(4) The member must then complete a form of order in terms substantially corresponding to those given by the issuing court, stating on the form:
(a) the name of the court; and
(b) the day on which, and the time at which, the order was completed.
(5) Within 24 hours of being informed under subsection (3), the member must give or transmit the following to the issuing court:
(a) the form of order completed by the member;
(b) if the information and the explanation included in the request were not already sworn or affirmed—that information and explanation duly sworn or affirmed;
(c) if the Attorney-General's consent was not obtained before making the request—a copy of the Attorney-General's consent.
(6) The issuing court must attach to the documents provided under subsection (5) the form of order the court has completed.

Sec. 104.8 Requesting an urgent interim control order in person
(1) A senior AFP member may request, in person, an issuing court to make an interim control order in relation to a person without first obtaining the Attorney-General's consent under section 104.2 if:
(a) the member considers it necessary to request the order without the consent because of urgent circumstances; and
(b) the member either considers or suspects the matters mentioned in subsection 104.2(2) on reasonable grounds.
Note: The Attorney-General's consent must be obtained within 4 hours of making the request (see section 104.10).
(2) The request must include the following:
(a) all that is required under subsection 104.2(3) in respect of an ordinary request for an interim control order (including information that is sworn or affirmed by the member);
(b) an explanation that is sworn or affirmed as to why the making of the interim control order without first obtaining the Attorney-General's consent is urgent.
Note: The member might commit an offence if the request is false or misleading (see sections 137.1 and 137.2).

Sec. 104.9 Making an urgent interim control order in person
(1) Before making an order in response to a request under section 104.8, the issuing court must:
(a) consider the information and the explanation included in the request; and
(b) receive and consider such further information (if any) as the court requires.
(2) If the issuing court is satisfied that an order should be made urgently, the court may make the same order that would be made under sections 104.4 and 104.5.
(3) Within 24 hours of the order being made under subsection (2), the member must:
(a) give or transmit a copy of the order to the issuing court; and
(b) either:
(i) give or transmit a copy of the Attorney-General's consent to request the order to the court; or

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(ii) notify the court in writing that the Attorney-General's consent was not obtained. Note: Section 104.10 deals with the Attorney-General's consent. **Sec. 104.10 Obtaining the Attorney-General's consent within 4 hours** (1) If the Attorney-General's consent to request an interim control order was not first sought before making a request under section 104.6 or 104.8, the senior AFP member who made the request must, in accordance with subsection 104.2(3), seek that consent within 4 hours of making the request. (2) In any case, if the Attorney-General: (a) refuses his or her consent to request the order; or (b) has not given his or her consent to request the order; within 4 hours of the request being made, the order immediately ceases to be in force. Note: However, the senior AFP member can vary the request and seek the Attorney-General's consent to request a new interim control order in relation to the person (see subsection 104.2(5)). (3) If the order ceases to be in force under subsection (2), the senior AFP member must, as soon as practicable: (a) notify the court that the order has ceased to be in force; and (b) if the order has been served on the person in relation to whom it was made: (i) annotate the order to indicate that it has ceased to be in force; and (ii) cause the annotated order to be served personally on the person. **Sec. 104.11 Court to assume that exercise of power not authorised by urgent interim control order** If: (a) it is material, in any proceedings, for a court to be satisfied that an interim control order was duly made under section 104.7; and (b) the form of order completed by the relevant issuing court is not produced in evidence; the first-mentioned court is to assume, unless the contrary is proved, that the order was not duly made. [*Please also refer to sections 104.12 to 104.32 of the* Criminal Code Act 1995].
"*Preventive detention orders*"	PREVENTIVE DETENTION ORDERS ***Criminal Code Act 1995*:** **Sec. 105.1 Object** The object of this Division is to allow a person to be taken into custody and detained for a short period of time in order to: (a) prevent an imminent terrorist act occurring; or (b) preserve evidence of, or relating to, a recent terrorist act. **Sec. 105.2 Issuing authorities for continued preventative detention orders** (1) The Minister may, by writing, appoint as an issuing authority for continued preventative detention orders: (a) a person who is a judge of a State or Territory Supreme Court; or (b) a person who is a Judge; or (c) a person who is a Federal Magistrate; or (d) a person who: (i) has served as a judge in one or more superior courts for a period of 5 years; and (ii) no longer holds a commission as a judge of a superior court; or (e) a person who: (i) holds an appointment to the Administrative Appeals Tribunal as President or Deputy President; and (ii) is enrolled as a legal practitioner of a federal court or of the Supreme Court of a State or Territory; and (iii) has been enrolled for at least 5 years. (2) The Minister must not appoint a person unless: (a) the person has, by writing, consented to being appointed; and (b) the consent is in force.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

Sec. 105.3 Police officer detaining person under a preventative detention order
If:
(a) a number of police officers are detaining, or involved in the detention of, a person under a preventative detention order at a particular time; and
(b) an obligation is expressed in this Division to be imposed on the police officer detaining the person;
the obligation is imposed at that time on:
(c) if those police officers include only one AFP member—that AFP member; or
(d) if those police officers include 2 or more AFP members—the most senior of those AFP members; or
(e) if those police officers do not include an AFP member—the most senior of those police officers.

Sec. 105.4 Basis for applying for, and making, preventative detention orders
(1) An AFP member may apply for a preventative detention order in relation to a person only if the AFP member meets the requirements of subsection (4) or (6).
(2) An issuing authority may make a preventative detention order in relation to a person only if the issuing authority meets the requirements of subsection (4) or (6).
(3) The person in relation to whom the preventative detention order is applied for, or made, is the subject for the purposes of this section.
(4) A person meets the requirements of this subsection if the person is satisfied that:
(a) there are reasonable grounds to suspect that the subject:
(i) will engage in a terrorist act; or
(ii) possesses a thing that is connected with the preparation for, or the engagement of a person in, a terrorist act; or
(iii) has done an act in preparation for, or planning, a terrorist act; and
(b) making the order would substantially assist in preventing a terrorist act occurring; and
(c) detaining the subject for the period for which the person is to be detained under the order is reasonably necessary for the purpose referred to in paragraph (b).
(5) A terrorist act referred to in subsection (4):
(a) must be one that is imminent; and
(b) must be one that is expected to occur, in any event, at some time in the next 14 days.
(6) A person meets the requirements of this subsection if the person is satisfied that:
(a) a terrorist act has occurred within the last 28 days; and
(b) it is necessary to detain the subject to preserve evidence of, or relating to, the terrorist act; and
(c) detaining the subject for the period for which the person is to be detained under the order is reasonably necessary for the purpose referred to in paragraph (b).
(7) An issuing authority may refuse to make a preventative detention order unless the AFP member applying for the order gives the issuing authority any further information that the issuing authority requests concerning the grounds on which the order is sought.

Sec. 105.6 Restrictions on multiple preventative detention orders
Preventative detention orders under this Division
(1) If:
(a) an initial preventative detention order is made in relation to a person on the basis of assisting in preventing a terrorist act occurring within a particular period; and
(b) the person is taken into custody under the order;
another initial preventative detention order cannot be applied for, or made, in relation to the person on the basis of assisting in preventing the same terrorist act occurring within that period.
(2) If:
(a) an initial preventative detention order is made in relation to a person on the basis of assisting in preventing a terrorist act occurring within a particular period; and
(b) the person is taken into custody under the order;
another initial preventative detention order cannot be applied for, or made, in relation to the person on the basis of assisting in preventing a different terrorist act occurring within that period unless the application, or the order, is based on information that became available to be put before an issuing authority only after the initial preventative detention order referred to in paragraph (a) was made.
(3) If:
(a) an initial preventative detention order is made in relation to a person on the basis of preserving evidence of, or relating to, a terrorist act; and
(b) the person is taken into custody under the order;
another initial preventative detention order cannot be applied for, or made, in relation to the person on the basis of preserving evidence of, or relating to, the same terrorist act.
Detention orders under corresponding State preventative detention laws
(4) If:
(a) an order for a person's detention is made under a corresponding State preventative detention law on the basis of assisting in preventing a terrorist act occurring within a particular period; and
(b) the person is taken into custody under that order;
an initial preventative detention order cannot be applied for, or made, under this Division in relation to the person on the basis of assisting in preventing the same terrorist act occurring within that

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

period.
(5) If:
(a) an order for a person's detention is made under a corresponding State preventative detention law on the basis of assisting in preventing a terrorist act occurring within a particular period; and
(b) the person is taken into custody under that order;
an initial preventative detention order cannot be applied for, or made, under this Division in relation to the person on the basis of assisting in preventing a different terrorist act occurring within that period unless the application, or the order, is based on information that became available to be put before an issuing authority only after the order referred to in paragraph (a) was made.
(6) If:
(a) an order for a person's detention is made under a corresponding State preventative detention law on the basis of preserving evidence of, or relating to, a terrorist act; and
(b) the person is taken into custody under that order;
an initial preventative detention order cannot be applied for, or made, under this Division in relation to the person on the basis of preserving evidence of, or relating to, the same terrorist act.

Sec. 105.7 Application for initial preventative detention order
(1) An AFP member may apply to an issuing authority for an initial preventative detention order in relation to a person.
Note 1: Senior AFP members are issuing authorities for initial preventative detention orders (see the definition of issuing authority in subsection 100.1(1)).
Note 2: For the definition of senior AFP member, see subsection 100.1(1).
(2) The application must:
(a) be made in writing; and
(b) set out the facts and other grounds on which the AFP member considers that the order should be made; and
(c) specify the period for which the person is to be detained under the order and set out the facts and other grounds on which the AFP member considers that the person should be detained for that period; and
(d) set out the information (if any) that the applicant has about the person's age; and
(e) set out the following:
(i) the outcomes and particulars of all previous applications for preventative detention orders in relation to the person;
(ii) the outcomes and particulars of all previous requests for interim control orders (including the outcomes of the hearings to confirm the orders) in relation to the person;
(iii) the outcomes and particulars of all previous applications for variations of control orders made in relation to the person;
(iv) the outcomes of all previous applications for revocations of control orders made in relation to the person; and
(f) set out the information (if any) that the applicant has about any periods for which the person has been detained under an order made under a corresponding State preventative detention law; and
(g) set out a summary of the grounds on which the AFP member considers that the order should be made.
Note: Sections 137.1 and 137.2 create offences for providing false or misleading information or documents.
(2A) To avoid doubt, paragraph (2)(g) does not require any information to be included in the summary if disclosure of that information is likely to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004).
(3) If:
(a) an initial preventative detention order is made in relation to a person on the basis of assisting in preventing a terrorist act occurring within a particular period; and
(b) the person is taken into custody under the order; and
(c) an application is made for another initial preventative detention order in relation to the person on the basis of assisting in preventing a different terrorist act occurring within that period;
the application must also identify the information on which the application is based that became available to be put before an issuing authority only after the initial preventative detention order referred to in paragraph (a) was made.
Note: See subsection 105.6(2).
(4) If:
(a) an order for a person's detention is made under a corresponding State preventative detention law on the basis of assisting in preventing a terrorist act occurring within a particular period; and
(b) the person is taken into custody under that order; and
(c) an application is made for an initial preventative detention order in relation to the person on the basis of assisting in preventing a different terrorist act occurring within that period;
the application must also identify the information on which the application is based that became available to be put before an issuing authority only after the order referred to in paragraph (a) was made.

Sec. 105.8 Senior AFP member may make initial preventative detention order
(1) On application by an AFP member, an issuing authority may make an initial preventative detention order under this section in relation to a person.
Note 1: Senior AFP members are issuing authorities for initial preventative detention orders (see the definition of issuing authority in subsection 100.1(1)).
Note 2: For the definition of senior AFP member, see subsection 100.1(1).
(2) Subsection (1) has effect subject to sections 105.4, 105.5 and 105.6.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(3) An initial preventative detention order under this section is an order that the person specified in the order may be: (a) taken into custody; and (b) detained during the period that: (i) starts when the person is first taken into custody under the order; and (ii) ends a specified period of time after the person is first taken into custody under the order. (4) The order must be in writing. (5) The period of time specified in the order under subparagraph (3)(b)(ii) must not exceed 24 hours. (6) An initial preventative detention order under this section must set out: (a) the name of the person in relation to whom it is made; and (b) the period during which the person may be detained under the order; and (c) the date on which, and the time at which, the order is made; and (d) the date and time after which the person may not be taken into custody under the order; and (e) a summary of the grounds on which the order is made. Note: Paragraph (d)—see subsection 105.9(2). (6A) To avoid doubt, paragraph (6)(e) does not require any information to be included in the summary if disclosure of that information is likely to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004). (7) If the person in relation to whom the order is made is: (a) under 18 years of age; or (b) incapable of managing his or her affairs; the order may provide that the period each day for which the person is entitled to have contact with another person under subsection 105.39(2) is the period of more than 2 hours that is specified in the order. (8) The senior AFP member nominated under subsection 105.19(5) in relation to the initial preventative detention order must: (a) notify the Commonwealth Ombudsman in writing of the making of the order; and (b) give the Commonwealth Ombudsman a copy of the order; and (c) if the person in relation to whom the order is made is taken into custody under the order—notify the Commonwealth Ombudsman in writing that the person has been taken into custody under the order. **Sec. 105.9 Duration of initial preventative detention order** (1) An initial preventative detention order in relation to a person starts to have effect when it is made. Note: The order comes into force when it is made and authorises the person to be taken into custody (see paragraph 105.8(3)(a)). The period for which the person may then be detained under the order only starts to run when the person is first taken into custody under the order (see subparagraph 105.8(3)(b)(i)). (2) An initial preventative detention order in relation to a person ceases to have effect at the end of the period of 48 hours after the order is made if the person has not been taken into custody under the order within that period. (3) If the person is taken into custody under the order within 48 hours after the order is made, the order ceases to have effect when whichever of the following first occurs: (a) the end of: (i) the period specified in the order as the period during which the person may be detained under the order; or (ii) if that period is extended or further extended under section 105.10—that period as extended or further extended; (b) the revocation of the order under section 105.17. [*Please also refer to sections 105.10 to 105.27 of the* Criminal Code Act 1995].
"*Special detention of terrorist suspects without charge*"	SPECIAL PRE-CHARGE DETENTION ***Crimes Act 1914***[78]**:** **Sec. 23DB Period of investigation if arrested for a terrorism offence** (1) If a person is arrested for a terrorism offence, the following provisions apply. Note: A person would not be arrested for a terrorism offence if, for example, the person has been released under subsection 3W(2)—see the definition of arrested in subsection 23B(1). (2) The person may, while arrested for the terrorism offence, be detained for the purpose of investigating either or both of the following: (a) whether the person committed the offence;

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(b) whether the person committed another Commonwealth offence that an investigating official reasonably suspects that the person has committed.
(3) Subsection (2) ceases to apply at the end of the investigation period, but that cessation does not affect any other power to detain the person.
(4) If the person is not released within the investigation period, the person must be brought before a judicial officer within the investigation period or, if it is not practicable to do so within the investigation period, as soon as practicable after the end of the investigation period.
(5) For the purposes of this section, but subject to subsections (7) and (9), the investigation period begins when the person is arrested, and ends at a later time that is reasonable, having regard to all the circumstances, but does not extend beyond:
(a) if the person is or appears to be under 18, an Aboriginal person or a Torres Strait Islander—2 hours; or
(b) in any other case—4 hours;
after the arrest, unless the period is extended under section 23DF.
(6) In ascertaining any period of time for the purposes of this section, regard shall be had to the number and complexity of matters being investigated.
(7) If the person has been arrested more than once within any period of 48 hours, the investigation period for each arrest other than the first is reduced by so much of any of the following periods as occurred within that 48 hours:
(a) any earlier investigation period or periods under this section;
(b) any earlier investigation period or periods under section 23C.
(8) However, in relation to each first arrest, disregard subsection (7) for any later arrest if:
(a) the later arrest is for a Commonwealth offence:
(i) that was committed after the end of the person's period of detention under this Part for the first arrest; or
(ii) that arose in different circumstances to those in which any Commonwealth offence to which the first arrest relates arose, and for which new evidence has been found since the first arrest; and
(b) the person's questioning associated with the later arrest does not relate to:
(i) a Commonwealth offence to which the first arrest relates; or
(ii) the circumstances in which such an offence was committed.
(9) In ascertaining any period of time for the purposes of subsection (5) or (7), disregard any reasonable time during which the questioning of the person is suspended, or delayed, for one or more of the following reasons:
(a) to allow the person to be conveyed from the place at which the person is arrested to the nearest premises at which the investigating official has access to facilities for complying with this Part;
(b) to allow the person, or someone else on the person's behalf, to communicate with a legal practitioner, friend, relative, parent, guardian, interpreter or other person as provided by this Part;
(c) to allow such a legal practitioner, friend, relative, parent, guardian, interpreter or other person to arrive at the place where the questioning is to take place;
(d) to allow the person to receive medical attention;
(e) because of the person's intoxication;
(f) to allow for an identification parade to be arranged and conducted;
(g) to allow the making of an application under section 3ZQB or the carrying out of a prescribed procedure within the meaning of Division 4A of Part IAA;
(h) to allow the making and disposing of an application under section 23DC, 23DE, 23WU or 23XB;
(i) to allow a constable to inform the person of matters specified in section 23WJ;
(j) to allow the person to rest or recuperate;
(k) to allow a forensic procedure to be carried out on the person by order of a magistrate under Division 5 of Part ID;
(l) because section 23XGD applies and the time is to be disregarded in working out a period of time for the purposes of that section;
(m) subject to subsection (11), because the time is within a period specified under section 23DD, so long as the suspension or delay in the questioning of the person is reasonable.
(10) To avoid doubt:
(a) subsection (9) does not prevent the person being questioned during a time covered by a paragraph of subsection (9), but if the person is questioned during such a time, the time is not to be disregarded; and
(b) a period specified under section 23DD is not extended by any time covered by a paragraph of subsection (9).
Limit on time that may be disregarded under paragraph (9)(m)
(11) No more than 7 days may be disregarded under paragraph (9)(m) in relation to an arrest. However:
(a) if the person has been arrested more than once within any period of 48 hours, the 7 day period for each arrest other than the first arrest is reduced by any period or periods specified under section 23DD in relation to any earlier arrest; and
(b) subsection (8) applies as if the reference in that subsection to subsection (7) were a reference to this subsection.
Evidentiary provision
(12) In any proceedings, the burden lies on the prosecution to prove that:
(a) the person was brought before a judicial officer as soon as practicable; or
(b) any particular time was covered by a provision of subsection (9).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

Sec. 23DC Time during which suspension or delay of questioning may be disregarded—application
(1) This section applies if:
(a) a person is arrested for a terrorism offence; and
(b) an investigation is being conducted into whether the person committed that terrorism offence or another terrorism offence.
Application for specification of period
(2) At or before the end of the investigation period, an investigating official (within the meaning of paragraph (a) or (b) of the definition of that expression) may apply, in writing, to a magistrate for a period to be specified for the purpose of paragraph 23DB(9)(m).
(3) The application must not be made unless the application is authorised, in writing, by an authorising officer.
(4) Subject to subsection (5), the application must include statements of all of the following:
(a) whether it appears to the investigating official that the person is under 18;
(b) whether it appears to the investigating official that the person is an Aboriginal person or a Torres Strait Islander;
(c) the outcome of any previous application under this section in relation to:
(i) the person and the arrest; and
(ii) if the person was arrested at any time during the period of 48 hours before the arrest—the person and the earlier arrest or arrests;
(d) the total amount of time that has been disregarded under subsection 23DB(9) in ascertaining the investigation period in relation to:
(i) the person and the arrest; and
(ii) if the person was arrested at any time during the period of 48 hours before the arrest—the person and the earlier arrest or arrests;
(e) the reasons why the investigating official believes the period should be specified, which may, for example, be or include one or more of the following:
(i) the need to collate and analyse information relevant to the investigation from sources other than the questioning of the person (including, for example, information obtained from a place outside Australia);
(ii) the need to allow authorities in or outside Australia (other than authorities in an organisation of which the investigating official is part) time to collect information relevant to the investigation on the request of the investigating official;
(iii) the fact that the investigating official has requested the collection of information relevant to the investigation from a place outside Australia that is in a time zone different from the investigating official's time zone;
(iv) the fact that translation is necessary to allow the investigating official to seek information from a place outside Australia and/or be provided with such information in a language that the official can readily understand;
(f) the period that the investigating official believes should be specified.
(5) Subsection (4) does not require any information to be included in the application if disclosure of that information is likely:
(a) to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004); or
(b) to be protected by public interest immunity; or
(c) to put at risk ongoing operations by law enforcement agencies or intelligence agencies; or
(d) to put at risk the safety of the community, law enforcement officers or intelligence officers.
(6) Before the application is considered by the magistrate, the investigating official must:
(a) provide a copy of the application to the person or to his or her legal representative; and
(b) inform the person that he or she, or his or her legal representative, may make representations to the magistrate about the application.
(7) If the application contains any information of a kind mentioned in subsection (5), the investigating official may remove it from the copy of the application that is provided to the person or to his or her legal representative.
(8) The person, or his or her legal representative, may make representations to the magistrate about the application.

Sec. 23DD Time during which suspension or delay of questioning may be disregarded—time specified by magistrate
(1) This section applies if:
(a) a person is arrested for a terrorism offence; and
(b) an application has been made under subsection 23DC(2) to a magistrate in respect of the person.
Specification of period
(2) The magistrate may, by signed instrument, specify a period starting at the time the instrument is signed, if satisfied that:
(a) it is appropriate to do so, having regard to:
(i) the application; and
(ii) the representations (if any) made by the person, or his or her legal representative, about the application; and
(iii) any other relevant matters; and
(b) the offence is a terrorism offence; and
(c) detention of the person is necessary to preserve or obtain evidence or to complete the investigation into the offence or into another terrorism offence; and

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(d) the investigation into the offence is being conducted properly and without delay; and
(e) the application has been authorised by an authorising officer; and
(f) the person, or his or her legal representative, has been given the opportunity to make representations about the application.
Instrument specifying period
(3) Subject to subsection (4), the instrument must:
(a) specify the period as a number (which may be less than one) of hours; and
(b) set out the day and time when it was signed; and
(c) set out the reasons for specifying the period.
(4) Subsection (3) does not require any information to be included in the instrument if disclosure of that information is likely:
(a) to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004); or
(b) to be protected by public interest immunity; or
(c) to put at risk ongoing operations by law enforcement agencies or intelligence agencies; or
(d) to put at risk the safety of the community, law enforcement officers or intelligence officers.
(5) The magistrate must:
(a) give the investigating official a copy of the instrument as soon as practicable after signing it; and
(b) if the instrument was made as a result of an application made by telex, fax or other electronic means—inform the investigating official of the matters included in the instrument.
Note: See section 23E.
(6) The investigating official must:
(a) as soon as practicable after receiving a copy of the instrument under paragraph (5)(a), give the person, or his or her legal representative, a copy of it; and
(b) if the instrument was made as a result of an application made by telex, fax or other electronic means—inform the person, or his or her legal representative, of the matters included in the instrument as soon as practicable after being informed of them under paragraph (5)(b).

Sec. 23DE Application may be made for extension of investigation period
(1) If a person is arrested for a terrorism offence, an investigating official (within the meaning of paragraph (a) or (b) of the definition of that expression) may, at or before the end of the investigation period, apply, in writing, to a magistrate for an extension of the investigation period.
(2) The application must not be made unless the application is authorised, in writing, by an authorising officer.
(3) Subject to subsection (4), the application must include statements of all of the following:
(a) whether it appears to the investigating official that the person is under 18;
(b) whether it appears to the investigating official that the person is an Aboriginal person or a Torres Strait Islander;
(c) the outcome of any previous application under this section in relation to the person and the investigation period;
(d) the period (if any) by which the investigation period has been reduced under subsection 23DB(7);
(e) the total amount of time (if any) that has been disregarded under subsection 23DB(9) in ascertaining the investigation period;
(f) the maximum amount of time by which the investigation period could be extended;
(g) the reasons why the investigating official believes the investigation period should be extended;
(h) the period by which the investigating official believes the investigation period should be extended.
(4) Subsection (3) does not require any information to be included in the application if disclosure of that information is likely:
(a) to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004); or
(b) to be protected by public interest immunity; or
(c) to put at risk ongoing operations by law enforcement agencies or intelligence agencies; or
(d) to put at risk the safety of the community, law enforcement officers or intelligence officers.
(5) Before the application is considered by the magistrate, the investigating official must:
(a) provide a copy of the application to the person or to his or her legal representative; and
(b) inform the person that he or she, or his or her legal representative, may make representations to the magistrate about the application.
(6) If the application contains any information of a kind mentioned in subsection (4), the investigating official may remove it from the copy of the application that is provided to the person or to his or her legal representative.
(7) The person, or his or her legal representative, may make representations to the magistrate about the application.

Sec. 23DF Magistrate may extend investigation period
(1) This section applies if:
(a) a person is arrested for a terrorism offence; and
(b) an application has been made under subsection 23DE(1) to a magistrate in respect of the person.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	Extension of investigation period (2) Subject to subsection (3), the magistrate may extend the investigation period, by signed written instrument, if satisfied that: (a) the offence is a terrorism offence; and (b) further detention of the person is necessary to: (i) reserve or obtain evidence related to the offence or to another terrorism offence; or (ii) complete the investigation into the offence or into another terrorism offence; and (c) the investigation into the offence is being conducted properly and without delay; and (d) the application has been authorised by an authorising officer; and (e) the person, or his or her legal representative, has been given the opportunity to make representations about the application. (3) Subject to subsection (4), the instrument must set out: (a) the day and time when the extension was granted; and (b) the reasons for granting the extension; and (c) the terms of the extension. (4) Subsection (3) does not require any information to be included in the instrument if disclosure of that information is likely: (a) to prejudice national security (within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004); or (b) to be protected by public interest immunity; or (c) to put at risk ongoing operations by law enforcement agencies or intelligence agencies; or (d) to put at risk the safety of the community, law enforcement officers or intelligence officers. (5) The magistrate must: (a) give the investigating official a copy of the instrument as soon as practicable after signing it; and (b) if the instrument was made as a result of an application made by telex, fax or other electronic means—inform the investigating official of the matters included in the instrument. Note: See section 23E. (6) The investigating official must: (a) as soon as practicable after receiving a copy of the instrument under paragraph (5)(a), give the person, or his or her legal representative, a copy of it; and (b) if the instrument was made as a result of an application made by telex, fax or other electronic means—inform the person, or his or her legal representative, of the matters included in the instrument as soon as practicable after being informed of them under paragraph (5)(b). (7) The investigation period may be extended any number of times, but the total of the periods of extension cannot be more than 20 hours.
New Zealand "*Security risk certificates*"	The *Immigration Amendment Act 1999* introduced new Part 4A into the *Immigration Act 1987* providing for a special security regime. The *Immigration Act 1987* (as amended) grants the Director of the New Zealand Security Intelligence Service (NZSIS) the power to issue a security risk certificate if he possesses credible classified security information pertaining to a foreign national suspected of involvement with terrorist activities. Under the *Act*, the Director of NZSIS is required to forward to the Minister of Immigration this certificate stating that there are reasonable grounds to suppose that a foreign national poses a threat to national security. The Minister must make a preliminary decision about the certificate's reliability. He may request an oral briefing from the Director, but may not record it or divulge it to anyone. The existence of a security risk certificate is evidence of sufficient grounds for the conclusion certified, subject only to a review by the Inspector-General of Intelligence and Security (by statute a retired High Court judge). If the Minister is satisfied that the intelligence underlying the certificate is reliable, he may decide to remove or deport a person based on the security risk certificate. The *Immigration Act 1987* grants the person subject to a certificate the right to appeal the Minister's decision. Review of this decision is not, however, undertaken by a court of law, but rather by the appointed Inspector-General of Intelligence and Security, which task is to confirm whether or not the security risk certificate has been issued properly and appropriately. Under NZ law, persons held under the *Immigration Act 1987* may be detained for up to 28 days without review, and thereafter a district judge must review their detention every 7 days (see section 100 of the amended *Immigration Act 1987*). In theory, individuals could be detained indefinitely in those conditions. With respect to special pre-charge detention under criminal law, NZ does not have an equivalent of the UK law allowing terrorist suspects to be detained without charge for an extended period of time. Neither the *Terrorism Suppression Act 2002* nor the amendments made to various statutes by the various Acts coming from the *Counter-Terrorism Bill 2003* allow for extended detention in the context of terrorism-related offences. Thus, any person suspected of terrorism in NZ has the same rights as any other crime suspect, that is to be either charged "promptly" or released (section 23(2) of the *New Zealand Bill of Rights Act 1990*). SECURITY RISK CERTIFICATES ***Immigration Act 1987***[79]**:** **Sec. 114A Object of Part**

[79] NZ *Immigration Act 1987* (as amended by the *Immigration Amendment Act 1999*, the *Immigration Amendment Act 1999 (No. 16)* and the *Immigration Amendment Act (No 2) 2003 (2003 No. 47)*): http://www.legislation.govt.nz/act/public/1987/0074/latest/whole.html#DLM112300

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

The object of this Part is to—
(a) recognise that the New Zealand Security Intelligence Service holds classified security information that is relevant to the administration of this Act; and
(b) recognise that such classified security information should continue to be protected in any use of it under this Act or in any proceedings which relate to such use; and
(c) recognise that the public interest requires nevertheless that such information be used for the purposes of this Act, but equally that fairness requires some protection for the rights of any individual affected by it; and
(d) establish that the balance between the public interest and the individual's rights is best achieved by allowing an independent person of high judicial standing to consider the information and approve its proposed use; and
(e) recognise that the significance of the information in question in a security sense is such that its approved use should mean that no further avenues are available to the individual under this Act and that removal or deportation, as the case may require, can normally proceed immediately; and thus
(f) ensure that persons covered by this Act who pose a security risk can where necessary be effectively and quickly detained and removed or deported from New Zealand.

Sec. 114B Definitions
(1) In this Part, unless the context otherwise requires— certificate, or security risk certificate, means a certificate made under section 114D classified security information means information about the threat to security, public order, or public interest posed by an identifiable individual which is held by the New Zealand Security Intelligence Service, being information which, in the opinion of the Director, cannot be divulged to the individual in question or to other persons because both—
(a) the information—
(i) might lead to the identification of, or provide details of, the source of the information, the nature, content, or scope of the information, or the nature or type of the assistance or operational methods available to the New Zealand Security Intelligence Service; or
(ii) is about particular operations that have been undertaken, or are being or are proposed to be undertaken, in pursuance of any of the functions of the Service or of another intelligence and security agency (as defined in section 2 of the Intelligence and Security Committee Act 1996); or
(iii) has been provided to the New Zealand Security Intelligence Service by the government of any other country or by an agency of such a government, and is information that cannot be disclosed by the Service because the government or agency by which that information has been provided will not consent to the disclosure; and
(b) disclosure of the information would be likely—
(i) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or
(ii) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the government of another country or any agency of such a government, or by any international organisation; or
(iii) to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; or
(iv) to endanger the safety of any person
Director, or Director of Security, means the Director of Security within the meaning of the New Zealand Security Intelligence Service Act 1969 Inspector-General means the Inspector-General of Intelligence and Security established and appointed under the Inspector-General of Intelligence and Security Act 1996, and, in any case where the Inspector-General is not available, within a time that will ensure that any review is completed with all reasonable speed, to review a decision of the Director of Security, includes a person appointed under subsection (2) to act as Inspector-General relevant security criterion, or security criterion, has the meaning given by section 114C.
(2) The Governor-General, on the recommendation of the Prime Minister following consultation with the Leader of the Opposition, may appoint a person who has previously held office as a Judge of the High Court of New Zealand to act as Inspector-General in any case where the Inspector-General is not available, within a time that will ensure that any review is completed with all reasonable speed, to review a decision of the Director of Security under this Part.
(3) The fact that a person appointed under subsection (2) exercises or performs any function or power of the Inspector-General under this Part is conclusive evidence of the authority of the person to do so, and no person may in any proceedings question whether the occasion requiring or authorising the person to exercise or perform the function or power has arisen or has ceased.

Sec. 114C Relevant security criteria
(1) For the purposes of this Part, relevant security criterion means any of the following, as the case may require:
(a) a relevant entry security criterion within the meaning of subsection (2), where a decision is to be taken as to whether—
(i) a temporary visa or permit should be issued or granted to any person; or
(ii) a limited purpose visa or permit should be issued or granted to any person; or
(iii) a residence visa or permit should be issued or granted to any person; or
(iv) an exemption should apply to any person:
(b) a relevant removal security criterion within the meaning of subsection (3), where a decision is to be taken as to whether—
(i) a temporary permit should be revoked and a removal order served; or
(ii) a limited purpose permit should be revoked and a removal order served; or
(iii) a person unlawfully in New Zealand should be served with a removal order:
(c) a relevant deportation security criterion within the meaning of subsection (4), where a decision is to be taken as to whether—
(i) the holder of a temporary permit or a limited purpose permit or a residence permit should be deported; or

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(ii) a person who is exempt under this Act from the requirement to hold a permit should be deported; or
(iii) a person unlawfully in New Zealand should be deported:
(d) a relevant refugee removal security criterion within the meaning of subsection (5), where a decision is to be taken as to whether a person in New Zealand who is a refugee status claimant or refugee—
(i) who holds a temporary permit should have that permit revoked and a removal order served; or
(ii) who holds a limited purpose permit should have that permit revoked and a removal order served; or
(iii) who is in New Zealand unlawfully should be served with a removal order:
(e) a relevant refugee deportation security criterion within the meaning of subsection (6), where a decision is to be taken as to whether a person in New Zealand who is a refugee status claimant or refugee—
(i) who holds a temporary permit or a limited purpose permit or a residence permit should be deported; or
(ii) who is exempt under this Act from the requirement to hold a permit should be deported; or
(iii) who is in New Zealand unlawfully should be deported.
(2) The relevant entry security criteria are as follows:
(a) any of the criteria set out in section 7(1)(e), (f), (g)(i), and (h) (which relate to terrorism and danger to security or public order):
(b) that the person constitutes a threat to national security in terms of section 72:
(c) any of the criteria set out in section 73(1) (which relates to suspected terrorists).
(3) The relevant removal security criteria are any of the criteria set out in section 7(1)(e), (f), (g)(i), and (h) (which relate to terrorism and danger to security or public order).
(4) The relevant deportation security criteria are as follows:
(a) that the person constitutes a threat to national security in terms of section 72:
(b) any of the criteria set out in section 73(1) (which relates to suspected terrorists).
(5) The relevant refugee removal security criteria are a combination of any 1 or more of the criteria listed in subsection (3) as relevant removal security criteria, taken together with either or both of the following criteria:
(a) that there are reasonable grounds for regarding the person as a danger to the security of New Zealand, in terms of Article 33.2 of the Refugee Convention:
(b) that the person is a danger to the community of New Zealand, having been convicted by a final judgment of a particularly serious crime, in terms of Article 33.2 of the Refugee Convention.
(6) The relevant refugee deportation security criteria are a combination of any 1 or more of the criteria listed in subsection (4) as relevant deportation security criteria, taken together with either or both of the following criteria:
(a) that there are reasonable grounds for regarding the person as a danger to the security of New Zealand, in terms of Article 33.2 of the Refugee Convention:
(b) that the person is a danger to the community of New Zealand, having been convicted by a final judgment of a particularly serious crime, in terms of Article 33.2 of the Refugee Convention.
(7) More than 1 relevant security criterion may be applicable at the same time to a particular person, but nothing in this section requires more than 1 relevant security criterion to be applied under this Part in any particular case (except to the extent that subsections (5) and (6) require a combination of criteria in relation to refugees and refugee status claimants).

Sec. 114D Director of Security may provide Minister with security risk certificate
(1) If the Director of Security holds classified security information that the Director is satisfied—
(a) relates to an identifiable individual who is not a New Zealand citizen and about whom decisions are to be, or can be, made under this Act; and
(b) is credible, having regard to the source or sources of the information and its nature, and is relevant to the relevant security criterion; and
(c) would mean, when applying a relevant security criterion to the situation of that person in light of that information, that the person meets the criterion,—
the Director may provide a security risk certificate to the Minister to that effect.
(2) A certificate must be in writing and must clearly identify the relevant security criterion or criteria that it relates to.
(3) In making a decision under subsection (1) the Director may take into account any relevant information that does not itself meet the definition of classified security information.
(4) For the purposes of applying this section and this Part, any reference to the belief or opinion of the Minister in the wording of a particular security criterion is to be read as including an alternative reference to the belief or opinion of the Director.

Sec. 114G Effect where Minister makes preliminary decision to rely on certificate
(1) If the Minister makes a preliminary decision to rely on a security risk certificate in relation to an individual, the Minister must give a notice to that effect to the chief executive of the Department of Labour.
(2) The effect of the giving of a notice under subsection (1) in the case of a person who is not in New Zealand is—
(a) to require the processing of any application or other matter in relation to the named individual by a visa officer or immigration officer that is currently under way to be suspended, despite any other requirement of this Act; and
(b) to require the chief executive to immediately ensure that the processing is in fact stopped; and
(c) to require any matter under this Act in relation to the named individual that is proceeding in an Authority, the Board, the Tribunal, the District Court, or the High Court to be suspended, notwithstanding anything in this Act or any other enactment or rule of law; and

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	(d) to require the chief executive to send to the person a copy of the notice and to notify the person of the matters specified in subparagraphs (i) to (v) of subsection (4)(d). (3) The effect of the giving of a notice under subsection (1) in the case of a person who is in New Zealand is— (a) to require the processing of any application or other matter in relation to the named individual by an immigration officer that is currently underway to be suspended, notwithstanding any other requirement of this Act; and (b) to require any matter under this Act in relation to the named individual that is proceeding in an Authority (other than the Refugee Status Appeals Authority), the Board, the Tribunal, the District Court, or the High Court to be suspended, notwithstanding anything in this Act or any other enactment or rule of law; and (c) to require the detention of the named individual by a member of the Police under subsection (5). (4) On receipt of a notice under subsection (1) in respect of a person who is in New Zealand, the chief executive must— (a) immediately ensure that the processing of any application or other matter in relation to the named individual by an immigration officer that is currently under way is stopped; and (b) not accept for processing any application or other matter in relation to the named individual (other than applications or matters relating to refugee status); and (c) if appropriate, immediately advise an Authority, the Board, the Tribunal, the District Court, or the High Court, in the prescribed manner, that any proceedings or matter under this Act in relation to the named individual are to be stopped in accordance with subsection (2); and (d) arrange for a member of the Police to as soon as is practicable personally serve on the person concerned a copy of the notice, along with written information stating— (i) that the Director of Security has made a security risk certificate in relation to the person; and (ii) that the Minister has made a preliminary decision to rely on the certificate; and (iii) the relevant security criterion or criteria that the certificate relates to; and (iv) the potential effect of the certificate; and (v) the rights of the person under section 114H (including the right to be heard by the Inspector-General under section 19(4) of the Inspector-General of Intelligence and Security Act 1996), and the time within which the right to a review must be exercised. (5) Where a member of the Police serves a notice on a person under subsection (4), that member or any other member of the Police must arrest the person without warrant and place the person in custody. (6) A person arrested under subsection (5) must be brought before a District Court Judge as soon as possible, and may in no case be detained for more than 48 hours unless, within that period, a Judge issues a warrant of commitment under section 114O for the continued detention of the person in custody. **Sec. 114H Rights of person in respect of whom security risk certificate given and relied on** (1) A person on whom a Ministerial notice is served under section 114G(4)(d) or who receives notification under section 114G(2)(d) may, under section 114I, seek a review by the Inspector-General of Intelligence and Security of the decision of the Director of Security to make the security risk certificate. (2) A person who seeks a review under section 114I may— (a) be represented, whether by counsel or otherwise, in his or her dealings with the Inspector-General; and (b) have access, to the extent provided by the Privacy Act 1993, to any information about the person other than the classified security information; and (c) make written submissions to the Inspector-General about the matter, whether or not the person also wishes to be heard under section 19(4) of the Inspector-General of Intelligence and Security Act 1996 (as applied by section 114I(6) of this Act). (3) No action may be taken to remove or deport the person on whom a notice served under section 114G(4)(d) remains in force unless and until section 114K applies in respect of the person. (4) No review proceedings may be brought in any court in respect of the certificate or the Director's decision to make the certificate. [*Please also refer to sections 114E, 114D, and 114I to 114Q of the* Immigration Act 1987].
France "*Special police custody*"	France rejected a national security approach for detention of terrorist suspects after its experience with the Algerian war of independence. Since 1986, France's response to terrorism has been towards accommodating the investigation and prevention of terrorist acts within the regular criminal justice system. A major difference, however, between terrorism cases and other criminal cases is that all terrorism-related cases are heard before a special section of the Trial Court (*Cour d'assise*) of Paris rather than in regular French courts. This specialised and centralised judicial system was introduced through the *Law No. 86-1020* and is currently provided in the *Code de procédure pénale* (French Code of Penal Procedure or CPP). Under French criminal law, special provisions and exceptions do apply to the treatment of terrorist suspects, including with regard to their detention. In particular, the French CPP provides for special police custody (*garde à vue*) during an investigation of terrorism offences, and for extended period of pre-trial detention during a judicial investigation. Information is provided below regarding these different detention regimes. SPECIAL POLICE CUSTODY: In France, the normal time limit for ordinary pre-charge detention cannot exceed 48 hours. Under articles 63*, 77, or 154 of the CPP, a person against whom there is one or more plausible reasons to suspect that he or she has committed or attempted to commit a criminal law offence may be detained for up to 48 hours before charges are brought against him or her. For a person suspected to have committed or attempted to commit a terrorism-related offence, the maximum time limit for pre-charge detention is increased to 96 hours (i.e. two possible extensions of 24 hours each, as provided by Article 706-88 al. 1* of the CPP). For a person suspected to be involved in the organisation of an imminent terrorist attack in France or abroad, or where the requirements of international cooperation so require, the time limit for pre-charge detention under French criminal law cannot exceed 144 hours (Article 706-88 al. 7*). Law enforcement officers must bring a detainee suspected of an act of terrorism before a sitting judge (*juge du siège*) in order to seek permission to hold him or her for a period lasting longer than the initial detention period

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	of 48 hours. Consequently, special police custody without charge in cases of terrorism-related offences investigation is a judicially authorised departure from the regular criminal procedure. ***Code de procédure pénale* (French Code of Penal Procedure)[80]:** **Art. 706-73** La procédure applicable à l'enquête, la poursuite, l'instruction et le jugement des crimes et des délits suivants est celle prévue par le présent code, sous réserve des dispositions du présent titre : […] 11° Crimes et délits constituant des actes de terrorisme prévus par les articles 421-1 à 421-6 du code pénal ; […] **Art. 706-88*** Pour l'application des articles 63*, 77 et 154, si les nécessités de l'enquête ou de l'instruction relatives à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, la garde à vue d'une personne peut, à titre exceptionnel, faire l'objet de deux prolongations supplémentaires de vingt-quatre heures chacune. Ces prolongations sont autorisées, par décision écrite et motivée, soit, à la requête du procureur de la République, par le juge des libertés et de la détention, soit par le juge d'instruction. La personne gardée à vue doit être présentée au magistrat qui statue sur la prolongation préalablement à cette décision. La seconde prolongation peut toutefois, à titre exceptionnel, être autorisée sans présentation préalable de la personne en raison des nécessités des investigations en cours ou à effectuer. Lorsque la première prolongation est décidée, la personne gardée à vue est examinée par un médecin désigné par le procureur de la République, le juge d'instruction ou l'officier de police judiciaire. Le médecin délivre un certificat médical par lequel il doit notamment se prononcer sur l'aptitude au maintien en garde à vue, qui est versé au dossier. La personne est avisée par l'officier de police judiciaire du droit de demander un nouvel examen médical. Ces examens médicaux sont de droit. Mention de cet avis est portée au procès-verbal et émargée par la personne intéressée; en cas de refus d'émargement, il en est fait mention. Par dérogation aux dispositions du premier alinéa, si la durée prévisible des investigations restant à réaliser à l'issue des premières quarante-huit heures de garde à vue le justifie, le juge des libertés et de la détention ou le juge d'instruction peuvent décider, selon les modalités prévues au deuxième alinéa, que la garde à vue fera l'objet d'une seule prolongation supplémentaire de quarante-huit heures. La personne dont la garde à vue est prolongée en application des dispositions du présent article peut demander à s'entretenir avec un avocat, selon les modalités prévues par l'article 63-4*, à l'issue de la quarante-huitième heure puis de la soixante-douzième heure de la mesure ; elle est avisée de ce droit lorsque la ou les prolongations lui sont notifiées et mention en est portée au procès-verbal et émargée par la personne intéressée ; en cas de refus d'émargement, il en est fait mention. Toutefois, lorsque l'enquête porte sur une infraction entrant dans le champ d'application des 3° et 11° de l'article 706-73, l'entretien avec un avocat ne peut intervenir qu'à l'issue de la soixante-douzième heure. S'il ressort des premiers éléments de l'enquête ou de la garde à vue elle-même qu'il existe un risque sérieux de l'imminence d'une action terroriste en France ou à l'étranger ou que les nécessités de la coopération internationale le requièrent impérativement, le juge des libertés peut, à titre exceptionnel et selon les modalités prévues au deuxième alinéa, décider que la garde à vue en cours d'une personne, se fondant sur l'une des infractions visées au 11° de l'article 706-73, fera l'objet d'une prolongation supplémentaire de vingt-quatre heures, renouvelable une fois. A l'expiration de la quatre-vingt-seizième heure et de la cent-vingtième heure, la personne dont la prolongation de la garde à vue est ainsi décidée peut demander à s'entretenir avec un avocat, selon les modalités prévues par l'article 63-4*. La personne gardée à vue est avisée de ce droit dès la notification de la prolongation prévue au présent article. Outre la possibilité d'examen médical effectué à l'initiative du gardé à vue, dès le début de chacune des deux prolongations supplémentaires, il est obligatoirement examiné par un médecin désigné par le procureur de la République, le juge d'instruction ou l'officier de police judiciaire. Le médecin requis devra se prononcer sur la compatibilité de la prolongation de la mesure avec l'état de santé de l'intéressé. S'il n'a pas été fait droit à la demande de la personne gardée à vue de faire prévenir, par téléphone, une personne avec laquelle elle vit habituellement ou l'un de ses parents en ligne directe, l'un de ses frères et sœurs ou son employeur, de la mesure dont elle est l'objet, dans les conditions prévues aux articles 63-1 et 63-2*, elle peut réitérer cette demande à compter de la quatre-vingt-seizième heure. * *On 14 April 2011, the French Parliament adopted the* Loi n° 2011-392 du 14 avril 2011 relative à la garde à vue *(i.e. after 1 February 2011), which amends* inter alia *sections 63 and sq., and 706-88 of the French Code of Penal Procedure. This* Law *relating to police custody (garde à vue) and special police custody for terrorism-related offences is due to enter into force on 1 June 2011. See also Chart e.2 under Title (e) of the research,* infra.
"*Extended period of pre-trial detention*"	SPECIAL PRE-TRIAL DETENTION: In France, once formal charges (*mise en examen*) for terrorism-related crimes have been brought, terrorist suspects may be held for up to 4 years in pre-trial detention (Article 145-2 of the French Code of Penal Procedure). With regard to lesser indictable offences ("*délits*" falling within the scope of "correctional matters"), an investigating magistrate can detain a terrorist suspect for up to 2 years on quite general grounds (Article 145-1 al. 2). These measures are intended to facilitate the judicial investigation in terrorism-related cases. ***Code de procédure pénale* (French Code of Penal Procedure):**

[80] *Code français de procédure pénale* (French Code of Penal Procedure): http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154 (in French).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

Art. 145-1
En matière correctionnelle, la détention provisoire ne peut excéder quatre mois si la personne mise en examen n'a pas déjà été condamnée pour crime ou délit de droit commun soit à une peine criminelle, soit à une peine d'emprisonnement sans sursis d'une durée supérieure à un an et lorsqu'elle encourt une peine inférieure ou égale à cinq ans.
Dans les autres cas, à titre exceptionnel, le juge des libertés et de la détention peut décider de prolonger la détention provisoire pour une durée qui ne peut excéder quatre mois par une ordonnance motivée conformément aux dispositions de l'article 137-3 et rendue après un débat contradictoire organisé conformément aux dispositions du sixième alinéa de l'article 145, l'avocat ayant été convoqué selon les dispositions du deuxième alinéa de l'article 114. Cette décision peut être renouvelée selon la même procédure, sous réserve des dispositions de l'article 145-3, la durée totale de la détention ne pouvant excéder un an. Toutefois, cette durée est portée à deux ans lorsqu'un des faits constitutifs de l'infraction a été commis hors du territoire national ou lorsque la personne est poursuivie pour trafic de stupéfiants, terrorisme, association de malfaiteurs, proxénétisme, extorsion de fonds ou pour une infraction commise en bande organisée et qu'elle encourt une peine égale à dix ans d'emprisonnement.
A titre exceptionnel, lorsque les investigations du juge d'instruction doivent être poursuivies et que la mise en liberté de la personne mise en examen causerait pour la sécurité des personnes et des biens un risque d'une particulière gravité, la chambre de l'instruction peut prolonger pour une durée de quatre mois la durée de deux ans prévue au présent article. La chambre de l'instruction, devant laquelle la comparution personnelle du mis en examen est de droit, est saisie par ordonnance motivée du juge des libertés et de la détention selon les modalités prévues par le dernier alinéa de l'article 137-1, et elle statue conformément aux dispositions des articles 144, 144-1, 145-3, 194, 197, 198, 199, 200, 206 et 207.

Art. 145-2
En matière criminelle, la personne mise en examen ne peut être maintenue en détention au-delà d'un an. Toutefois, sous réserve des dispositions de l'article 145-3, le juge des libertés et de la détention peut, à l'expiration de ce délai, prolonger la détention pour une durée qui ne peut être supérieure à six mois par une ordonnance motivée conformément aux dispositions de l'article 137-3 et rendue après un débat contradictoire organisé conformément aux dispositions du sixième alinéa de l'article 145, l'avocat ayant été convoqué conformément aux dispositions du deuxième alinéa de l'article 114. Cette décision peut être renouvelée selon la même procédure.
La personne mise en examen ne peut être maintenue en détention provisoire au-delà de deux ans lorsque la peine encourue est inférieure à vingt ans de réclusion ou de détention criminelles et au-delà de trois ans dans les autres cas. Les délais sont portés respectivement à trois et quatre ans lorsque l'un des faits constitutifs de l'infraction a été commis hors du territoire national. Le délai est également de quatre ans lorsque la personne est poursuivie pour plusieurs crimes mentionnés aux livres II et IV du code pénal, ou pour trafic de stupéfiants, terrorisme, proxénétisme, extorsion de fonds ou pour un crime commis en bande organisée.
A titre exceptionnel, lorsque les investigations du juge d'instruction doivent être poursuivies et que la mise en liberté de la personne mise en examen causerait pour la sécurité des personnes et des biens un risque d'une particulière gravité, la chambre de l'instruction peut prolonger pour une durée de quatre mois les durées prévues au présent article. La chambre de l'instruction, devant laquelle la comparution personnelle du mis en examen est de droit, est saisie par ordonnance motivée du juge des libertés et de la détention selon les modalités prévues par le dernier alinéa de l'article 137-1, et elle statue conformément aux dispositions des articles 144, 144-1, 145-3, 194, 197, 198, 199, 200, 206 et 207. Cette décision peut être renouvelée une fois sous les mêmes conditions et selon les mêmes modalités.
Les dispositions du présent article sont applicables jusqu'à l'ordonnance de règlement.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

(e) Relevant GOVERNMENT PROPOSALS NOT YET ENACTED for Changes to the Current Anti-Terrorism Legislation in Canada, the United States, the United Kingdom, Australia, New Zealand, and France (as of 1 February 2011)

Under this Title of the research, information is provided about any anti-terrorism legislation that is proposed but has not yet been enacted in Canada, the United States (US), the United Kingdom (UK), Australia, New Zealand (NZ), and France. Chart e.2 below covers the information specifically requested by the Contract specification (Statement of work). Chart e.1 and Chart e.3 contain relevant additional information that has come to our attention in the course of the research (up to 18 April 2011).

e.1 – Anti-Terrorism Legislation Adopted After 1 February 2011	
Country	**Legislation and reference**
Canada	—
United States	—
United Kingdom	*Terrorism Act 2000 (Remedial Order) 2011* (came into force on 18 March 2011): http://www.legislation.gov.uk/uksi/2011/631/made Please see Chart e.2 below for details.
Australia	—
New Zealand	—
France	*Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieur*: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312 (in French) *Loi n° 2011-266 du 14 mars 2011 relative à la lutte contre la prolifération des armes de destruction massive et de leurs vecteurs*: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707202&fastPos=1&fastReqId=1161804005&categorieLien=id&oldAction=rechTexte (in French) *Loi n° 2011-392 du 14 avril 2011 relative à la garde à vue*: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023860729&dateTexte=&categorieLien=id (in French)

e.2 – Government Proposals As of 1 February 2011	
Country	**Summary of relevant anti-terrorism legislation not yet enacted**
Canada	THE FOLLOWING BILLS WERE BEFORE THE PARLIAMENT AT DISSOLUTION FOR GENERAL ELECTION IN MARCH 2011: *Bill C-17 An Act to Amend the Criminal Code (Investigative Hearing and Recognizance with Conditions)*: http://www2.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Parl=40&Ses=3&Mode=1&Pub=Bill&Doc=C-17_1 This Bill contained the provisions found in the former Bill C-19, which itself contained the provisions found in the former Bill S-32 as amended by the Special Senate Committee on the Anti-terrorism Act in March 2008. Bill C-17 proposed amendments to the *Criminal Code* that would have reinstated anti-terrorism provisions that expired under a sunset clause on 1 March 2007, namely sections 83.28 to 83.3 of the *Criminal Code*. These provisions relating to investigative hearings, recognizance with conditions, and preventive arrest to avert a potential terrorist attack are substantially similar to original provisions that first came into force with the *Anti-terrorism Act* in 2001. On 2 March 2011, the House of Commons Standing Committee on Public Safety and National Security had adopted three amendments to Bill C-17.[81] *Bill C-50 An Act to Amend the Criminal Code (Interception of Private Communications and Related Warrants and Orders)*: http://www2.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Parl=40&Ses=3&Mode=1&Pub=Bill&Doc=C-50_1

[81] For further information, please refer to: http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?Language=e&ls=C17&Mode=1&Parl=40&Ses=3&source=library_prb

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	This Bill proposed to amend the *Criminal Code*, primarily in respect of authorizations to intercept private communications and warrants and orders. Among other things, the Bill: provided that if an authorization is given under certain provisions of Part VI, the judge may at the same time issue a warrant or make an order that relates to the investigation in respect of which the authorization is given; provided that the rules respecting confidentiality that apply in respect of an authorization to intercept private communications also apply in respect of a request for a related warrant or order; required the Minister of Public Safety and Emergency Preparedness to report on the interceptions of private communications made without authorizations; provided that a person who has been the object of an interception made without an authorization must be notified of the interception within a specified period; permited a peace officer or a public officer, in certain circumstances, to install and make use of a number recorder without a warrant; and extended to one year the maximum period of validity of a warrant for a tracking device and a number recorder if the warrant is issued in respect of a terrorism offence or an offence relating to a criminal organization. *Bill S-7 An Act to Deter Terrorism and to Amend the State Immunity Act*: http://www.parl.gc.ca/HousePublications/Publication.aspx?Doc=S-7_3&Language=E&Mode=1&Parl=40&Pub=Bill&Ses=3 This Bill proposed to create, in order to deter terrorism, a cause of action that would have allowed victims of terrorism to sue perpetrators of terrorism and their supporters. This Bill also proposed to amend the *State Immunity Act* to prevent a foreign state from claiming immunity from the jurisdiction of Canadian courts in respect of actions that relate to its support of terrorism activity.
United States	The *USA Patriot Act*, as originally enacted, contained 16 provisions scheduled to sunset on 31 December 2005 unless reauthorized by Congress. After two short extensions of all the provisions destined to sunset, the Congress passed the *USA PATRIOT Improvement and Reauthorization Act of 2005*[82] and the *USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006*[83], both signed into law on 9 March 2006. Under these *Acts*, only two provisions destined to sunset under the *USA Patriot Act* were not made permanent: section 206 (roving *Foreign Intelligence Surveillance Act* orders) and section 215 (allowing broad access to a wide array of records). The expiry dates for these two provisions were initially extended to 31 December 2009, then to 27 May 2011[84]. The House of Representatives (H.R.) and the Senate (S.) are now conducting review to see whether further reauthorization of these sunset provisions is warranted and to what extent. Various proposals are made through the following Bills: *Bill H.R. 67 To Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 29, 2012* (introduced on 5 January 2011): http://www.gpo.gov/fdsys/pkg/BILLS-112hr67ih/pdf/BILLS-112hr67ih.pdf This Bill proposes to extend expiring provisions of the *USA PATRIOT Improvement and Reauthorization Act of 2005* and of the *Intelligence Reform and Terrorism Prevention Act of 2004* until February 29, 2012. *Bill S. 149 To Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005, the Intelligence Reform and Terrorism Prevention Act of 2004, and the FISA Amendments Act of 2008 until December 31, 2013, and for Other Purposes* (introduced on 25 January 2011): http://www.gpo.gov/fdsys/pkg/BILLS-112s149is/pdf/BILLS-112s149is.pdf This Bill proposes to extend expiring provisions of the *USA PATRIOT Improvement and Reauthorization Act of 2005*, the *Intelligence Reform and Terrorism Prevention Act of 2004*, and the *FISA Amendments Act of 2008* until December 31, 2013. *Bill S. 193 To Extend the Sunset of Certain Provisions of the USA PATRIOT Act, and for Other Purposes* (introduced on 26 January 2011): http://www.gpo.gov/fdsys/pkg/BILLS-112s193rs/pdf/BILLS-112s193rs.pdf This Bill proposes to extend the sunset of certain provisions of the *USA Patriot Act* until December 31, 2013.
United Kingdom	In January 2010, the European Court of Human Right ruled that the stop and search power contained in sections 44 to 47 of the *Terrorism Act 2000* violated Article 8 (privacy and family life) of the *European Convention on Human Rights* (*ECHR*), and that interference with this right was not in accordance with the law because the provisions lacked appropriate safeguards to protect people against arbitrary interferences with their right to privacy (*Gillan and Quinton v. The United Kingdom*, [2009] ECHR 28). The European Court's decision runs counter to a 2006 House of Lord decision in the same case, in which the House of Lords upheld the legality of the stop and search powers provided in the *Terrorism Act 2000*. In order to put the stop and search powers into line with the *ECHR*, the UK Government prepared a remedial order under section 10 of the UK *Human Rights Act 1998* to make immediate changes to the legislation. This remedial order entered into force on 18 March 2011 (*Terrorism Act 2000 (Remedial Order) 2011*). The remedial order replaces sections 44 to 47 of the *Terrorism Act 2000* with a more targeted and proportionate power. The provisions in the order will cease to have effect on the coming into force of the similar provisions in the *Protection of Freedoms Bill* that is currently being taken through Parliament. The *Protection of Freedoms Bill* also proposes the maximum period of pre-charge detention for terrorist suspects to be reduced to 14 days. Accordingly, clauses contained in *Protection of Freedoms Bill* provides for the repeal of the order-making provisions in the *Terrorism Act 2006* that allow the maximum period of pre-charge detention under Schedule 8 to the *Terrorism Act* to be set at 28 days. The UK counter-terrorism review found that there may be urgent situations where more than 14 days pre-charge detention is considered necessary, and the Secretary of State for the Home Department stated that such situations would be catered for by the use of emergency legislation. On February 2011, the Home Office published two Draft Bills relating to the detention of terrorist suspects, both of which would have the effect of extending the maximum period of pre-charge detention to 28 days, should they be introduced and Parliament approved. A Joint Committee of both Houses of Parliament has been appointed to conduct pre-legislative scrutiny of the Draft Detention of Terrorist Suspects (Temporary Extensions) Bills. *Terrorism Act 2000 (Remedial Order) 2011* (entered into force on 18 March 2011 – please also see Chart e.1 above): http://www.legislation.gov.uk/uksi/2011/631/made *Protection of Freedoms Bill* (currently before the UK Parliament): http://www.publications.parliament.uk/pa/bills/cbill/2010-2011/0146/cbill_2010-20110146_en_1.htm

[82] *USA PATRIOT Improvement and Reauthorization Act of 2005*: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h3199enr.txt.pdf
[83] *USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006*: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s2271enr.txt.pdf
[84] US *FISA Sunsets Extension Act of 2011* (Bill H. R. 154 which became public law on 25 February 2011): http://www.gpo.gov/fdsys/pkg/PLAW-112publ3/pdf/PLAW-112publ3.pdf

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA
On behalf of the Minister of Justice and Attorney General of Canada (2011)

	Draft Detention of Terrorist Suspects (Temporary Extension) Bills (currently under pre-legislative scrutiny): http://www.homeoffice.gov.uk/publications/counter-terrorism/draft-detention-terrorist-bills?view=Binary *Draft Bill 1* makes provision for the maximum period of detention for terrorist suspects under Schedule 8 to the *Terrorism Act 2000* to be increased from 14 days to 28 days, by "disapplying" section 25 of the *Terrorism Act 2006* (which provides for the maximum period of pre-charge detention to be 14 days for any period during which section 25 applies – and when that section is disapplied, the maximum period is 28 days). *Draft Bill 2* makes provision for the maximum period of detention for terrorist suspects under Schedule 8 to the *Terrorism Act 2000* to be increased from 14 days to 28 days for a period of 3 months, and makes provision for a requirement that applications for detention beyond 14 days to be approved by a senior judge.
Australia	*Combating the Financing of People Smuggling and Other Measures Bill 2011*: http://www.comlaw.gov.au/Details/C2011B00002 This Bill proposes to amend the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* to extend the regulatory regime for remittance dealers and providers of remittance networks, and expand the agencies with which Australian Transaction Reports and Analysis Centre (AUSTRAC) can share financial intelligence. The Bill also proposes to amend the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and the *Privacy Act 1988* to enable reporting entities to use credit reporting data to verify the identity of their customers. This Bill finally proposes to amend the *Financial Transaction Reports Act 1988* to enable the Chief Executive Officer of AUSTRAC to exempt a person from provisions of the Act.
New Zealand	*Criminal Procedure (Reform and Modernisation) Bill 243-1 (2010)*: http://www.legislation.govt.nz/bill/government/2010/0243/latest/whole.html?search=qs_bill_terrorism_resel&p=1#dlm3360716 The purpose of this Bill is to simplify criminal procedure and provide an enduring legislative framework that, *inter alia*, reduces unnecessary delay and inefficiency in the NZ courts, eliminates unnecessary complexity in the legislation governing criminal procedure; and addresses shortcomings in the legislative framework arising from piecemeal amendments over many years. In particular, the Bill provides for an integrated set of reforms that simplifies the way offences are categorised for the purpose of determining how they are to progress. Under the Bill, offences are re-categorised into 4 categories, which are broadly defined as follows: Category 1 (Offences not punishable by imprisonment); Category 2 (Offences punishable by a term of imprisonment that does not exceed 3 years); Category 3 (Offences punishable by more than 3 years' imprisonment except those offences that fall into category 4); Category 4 (Specified offences punishable by more than 3 years' imprisonment). Terrorism-related offences provided in the *Terrorism Suppression Act 2002* are categorised by the Bill as offences falling within Category 4. Offences have been allocated to Category 4 primarily on the basis that they are of such high public or symbolic importance that they must be tried in the High Court by a jury or that, because of their nature, there would be questions of fairness and impartiality if they were tried by a Judge alone.
France	—

e.3 – Government Proposals Introduced Between 1 February 2011 and 18 March 2011	
Country	**Legislation and reference**
Canada	—
United States	*Bill S. 289 To Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005, the Intelligence Reform and Terrorism Prevention Act of 2004, and the FISA Amendments Act of 2008 until December 31, 2013, and for Other Purposes* (introduced on 2 March 2011): http://www.gpo.gov/fdsys/pkg/BILLS-112s289pcs/pdf/BILLS-112s289pcs.pdf *Bill S. 290 To Extend the Sunset of Certain Provisions of the USA PATRIOT Act, and for Other Purposes* (introduced on 2 March 2011): http://www.gpo.gov/fdsys/pkg/BILLS-112s290pcs/pdf/BILLS-112s290pcs.pdf *Bill S. 291 To Repeal the Sunset Provisions in the USA PATRIOT Improvement and Reauthorization Act of 2005 and Other Related Provisions and Permanently Reauthorize the USA PATRIOT Act* (introduced on 2 March 2011): http://www.gpo.gov/fdsys/pkg/BILLS-112s291pcs/pdf/BILLS-112s291pcs.pdf
United Kingdom	—
Australia	—
New Zealand	—
France	—

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Research Proposal: Sentencing of Terrorism Offences in the United Kingdom, Australia, the United States and Canada from 2001 to date

Researcher
Derek Wade

Background

A comparison of fact patterns and sentences for convictions under British, Australian, and American anti-terrorism legislation widens the context within which to assess sentences under Canada's *Anti-terrorism Act*. The operation of anti-terrorism laws in any one of these four countries can give insight into the advisability and application of similar laws within the others.

Comparison of sentencing within the four anti-terrorism frameworks is appropriate for three reasons. First, the threat of international terrorism raises common security concerns for all four nations. The operation and financing of terrorist groups both within and across their borders demonstrate a need for concerted action in identifying, investigating, and preventing terrorist activities and the threat is a wider global one requiring international efforts at all levels.

A second reason for comparison is that it can be useful when drafting or considering anti-terrorism measures, since the governments of Canada, the United Kingdom, Australia and the United States all must balance security concerns with their mutual dedication to human rights. All four countries have tailored their antiterrorism laws so as to strike a balance between combating terrorism and protecting fundamental rights, albeit with the balance in some cases shifting towards combating terrorism.

Finally, security and rights concerns exist within a common law tradition shared by Canada, the United Kingdom, Australia and the United States. This tradition encompasses similar principles of constitutionalism and rights, and constructs a broader systemic context in which courts can adjudicate the anti-terrorism laws of their respective jurisdictions.

Comparison of these laws and the sentences that result from convictions under these offences draws upon multiple experiences and perspectives and may guide ongoing review and improvements to anti-terrorism legislation in Canada.

Research Questions

1. How has the sentencing following conviction (including guilty pleas) for terrorism-related crimes evolved over the course of the decade in the UK, Australia, Canada and the US?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Project Scope
The project will:

- examine only the reported judicial decisions on conviction and sentences relating to terrorism offences in the U.S., U.K., Australia and Canada (it will not include convictions under terrorism financing provisions);
- provide case summaries that sum up the fact scenario surrounding the specific criminal charges that were laid, resulted in a conviction as well as the sentence and ancillary orders that were given for each conviction; and
- provide information on whether or not classified or secret evidence was adduced during the trial.

Methodology
The Contractor will undertake the following to complete the project:

- In consultation with the Project Authority, the Contractor will review all reported cases involving convictions and sentences under anti terrorism law, other than terrorism financing provisions, in the Countries from 2001 to date. This will include both convictions subsequent to a trial as well as guilty pleas.
- The Contractor will indicate which offences were caught within the purview of the study.
- The Contractor will provide electronic links to the reported decisions.
- The Contractor will provide a summary of each case that was reported that resulted in convictions and the sentence, including ancillary orders that were awarded for each conviction.
- The case summaries will include both the fact scenarios and the salient portions of the reasons for sentencing in each case. For example, judge's remarks on aggravating, attenuating circumstances and references to jurisprudence and guiding principles on sentencing for terrorism offences will be included.
- The Contractor will also provide the legislated penalty structure for all offences that were charged.
- If the information is readily available during a review of the case law, the Contractor will also indicate if classified or secret evidence was adduced during the trial.
- The Contractor will analyse the data collected and compare and contrast the fact scenarios, the convictions for similar offences and the sentences and ancillary orders that were handed down in each case.
- The deliverable will be in the format of a table (template to be provided by the contract authority) in MSWord (7.0 or higher) in electronic format sent to the Project Authority.

Budget
25 K

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Timeframe
January – March 2012

Ethics
The contractor will sign a confidentiality agreement

Reviewed by: Kelly Morton-Bourgon, Glen Gilmour

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Security, Terrorism and Governance Team Meeting
Minutes of the June 22, 2011 Meeting

Below is a brief synopsis of the discussion which was held on June 22, 2011 between members of the Security, Terrorism and Governance Team and Derek Wade of the Research and Statistics Division.

Present: Karine Bolduc, Doug Breithaupt, Glenn Gilmour, Dorette Pollard, Derek Wade.

Agenda Item 1 – 2010-2011 STG Research Projects:

Status of 2010-2011 projects:

1. Citizen Engagement in National Security Issues: A Five Country Review: **Completed**

2. A Summary of De-Radicalization and Counter-Terrorism Programs: **Completed**

3. A comparison of anti-terrorism offences and related police powers: Canada, the United States, the United Kingdom, Australia, New Zealand, and France: **Completed**

Other projects:

1. Research on Foreign Domestic Implementation of Nuclear Terrorism Conventions (CPPNM Amendment and ICSANT): **To be completed by STG** (Karine Bolduc)

2. Terrorist Listing Procedures: A Research Synthesis of Legislation, Cases and Literature on the UN 1267 Process, the European Union, the United Kingdom, the United States, Australia and New Zealand: **Completed**

Agenda Item 2 – 2011-2012 Potential STG Research Projects:

- Dorette mentions that her call for proposals within STG team was unfruitful.

- Topics formerly proposed by Nicole Crutcher:

1. A literature review on the role women are playing in radicalization/de-radicalization/terrorist incidents

2. A literature review on the role of support systems (e.g. community, family) to prevent terrorism/to be resilient

   → Karine will inquire with Brett Kubicek (Manager, Research and Academic Relations, Strategic Policy Branch, Public Safety Canada) if Public Safety intends to be conducting those two research projects in the near future.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(a)

3. A study on the economic costs of terrorism:

   → Doug says this kind of study has already been conducted; there is no need for any further work on this.

Other potential research ideas:

1. [redacted]

2. [redacted]

3. Intelligence as evidence: Dorette to inquire with Stanley Cohen

Agenda Item 3 – Other Business

- Dorette asked STG members present and Derek Wade to put their thinking caps on during the summer and suggested to meet at the beginning of September 2011 to discuss any new ideas related to research (bearing in mind the potential costs of a study on [redacted]).

Next meeting
Wednesday, September 14, 2011.

Page 509

is withheld pursuant to sections

est retenue en vertu des articles

21(1)(a), 21(1)(b)

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Research and Statistics Division
RRC Meeting/
Division de la recherché et de la statistique
Réunion du CER

Agenda / Ordre du jour

s.21(1)(a)

Meeting of Wednesday / Réunion du mercredi
January 11, 2012 / Le 11 janvier, 2012
2:00 - 3:00 p.m. / 14h 00 à 15h 00
EMB 6015

Research Proposal // Proposition de recherche	Researcher(s) // Chercheur(s)
1. Sentencing of Terrorism Offences in the United Kingdom, Australia, the United States and Canada from 2001 to date	Derek Wade
2. [redacted]	Derek Wade
3. Updates / Mise à jour	All/Tous

Pages 511 to / à 609

are withheld pursuant to section

sont retenues en vertu de l'article

68(a)

of the Access to Information Act

de la Loi sur l'accès à l'information

Pages 610 to / à 637

are withheld pursuant to section

sont retenues en vertu de l'article

68(a)

of the Access to Information Act

de la Loi sur l'accès à l'information

Pages 638 to / à 650

are withheld pursuant to section

sont retenues en vertu de l'article

21(1)(a)

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

JUSTICE POLICY IMPLICATIONS OF ANTI-TERRORISM RESEARCH APPLYING SOCIAL NETWORK ANALYSIS

by

Dr. Stéphane Leman-Langlois

of the
University of Montreal,
Director, Terrorism and Counterterrorism Research Team

A discussion paper presented to the

Department of Justice Canada

The views expressed in this report are those of the authors and do not necessarily represent the views of the Department of Justice Canada

000651

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

6 848 words

Keywords: social network analysis, terrorism, Canada, criminal justice, law enforcement, prevention

Abstract: This paper examines the possible use of social network analysis for the purposes of terrorism prevention. Social network analysis is briefly described, as is the state and trends of terrorism in Canada. Final sections look at network-based strategies for terrorist disruption. In conclusion, a number of criminal justice implications of the above are presented.

Released under the Access to Information Act
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTRODUCTION

This paper examines the ways in which "social network analysis" (SNA) might be used in governmental efforts towards the prevention of terrorism or prosecution of offenders. It does not purport to evaluate the strength of SNA as a technique or with regards to its sociological theoretical framework or in its application to terrorist groups. It also should not be considered in any way as a "meta-analysis" of existing SNA work on terrorist networks. For the time being, the sum total of such work is insufficient for meta-analyses.

SNA was as designed to better understand the structure and the workings or "networks", groups of individuals linked together by various types of social ties, and sometimes engaged in collective action. It is meant to shed light on various functional aspects of networks, such as their "recruitment" process, the division of labour among their members, the various forms of bonds that link them together, etc. With that, the potential usefulness of social network analysis for justice policy and in law enforcement it immediately obvious.

In fact, the analysis of networks (though not quite SNA *per se*) has been used in criminal and security intelligence for quite a while already: investigators and analysts routinely use it to prepare organized crime trials and to identify the role of individuals in a conspiracy, for instance. However, modern SNA, as it is used in scientific research, is a very complex method usually involving painstaking datamining and specialized statistical analysis and modelling software. Accordingly, its development has followed the greater availability of affordable powerful personal computers in the 1990s. In fact, network analysis is also used to understand the connections between the computers themselves, and the analogy between computer and human networks has deeply shaped our conception of both.

Renewed concerns for terrorism, in the years following 9/11, have triggered an intensive hunt for new preventative tactics that could help mitigate the risk of new attacks. Datamining through vast databases of personal information, in an effort to find patterns of terrorist activity, is one such tactic. It has been deemed contrary to the Bill of rights by the US Congress, who put an end to all funding allocated to the Total Information Awareness (TIA) project through the Defence Advanced Research Projects Agency (DARPA) in 2003. More important to the present paper, a key sub-program of TIA, called "Scalable Social Network Analysis," involved the discovery, identification and analysis of functioning terrorist networks within massive amounts of transactional data (the "footprints" left by any and all actions involving databases, such as using a credit card, making a phone call or ordering large amounts of chemical fertilizer).

Barring "total information awareness," the most serious problem SNA will run into when applied to covert networks is, by definition, the lack of data about individuals and their relationships. SNA is a data organisation and analysis tool and not a data collection tool. It is one thing to use SNA to map a network once its members are arrested or dead (and identified), quite another to use it in a preventative fashion, as a way to gather information not yet available. However, when such information becomes available SNA can prove useful in many ways, from understanding social functions of members to disrupting the network.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Before taking matters further it is useful to distinguish between three levels of what is commonly referred to as "prevention" in relation to terrorism (see table 1). The most difficult, but also the safest and most durable type of prevention manages to recognize radicalization patterns and dissolves groups *before* they formulate violent plans. In its broadest sense it is social prevention that lowers the risk of radicalization for all current and future groups. Of course, because it is so close to policing subversion and political dissent, the manner in which it is accomplished becomes fundamentally important. Second, one may also prevent terrorism by disrupting terrorist plots. Though far less ethically problematic, it is also extremely dangerous since all interventions constantly take place *in extremis*. Last, one may speak of prevention when referring to criminal sanctions which make it impossible for the condemned to repeat the acts he or she has been convicted of. This is the least controversial of all forms of prevention, but since at least one attack has to take place before it is mobilized, it probably should not count it as actual "prevention."

Table 1: three levels of prevention

early prevention	late prevention	post-incident
• detects radicalization processes • produces maximum security • with maximum effectiveness • most difficult • possible ethical problems	• detects conspiracies and preparations • high risk, *in extremis* intervention • ethically less problematic • does not prevent *future* conspiracies	• prevention of repeat offences • ethically non problematic • is not actually preventative

1 OVERVIEW OF SOCIAL NETWORK ANALYSIS AS APPLIED TO TERRORISM

There is actually very little current research on terrorism using SNA techniques, and SNA has developed mostly around *overt*, legal and legitimate social networks. The explanation for this is rather simple: acts of terrorism, as people and groups identified as terrorists, remain extremely rare.

1.1 WHAT IS MEANT BY "TERRORISM" AND "TERRORISTS"

In Canada, the official definition of terrorism now includes a variety of actions peripheral to the acts of violence that typically characterize terrorism. The intent of the legislator was clearly to reach terrorism *before* bombs explode, through the criminalization and eventual police detection and neutralization of many forms of preparation, or so-called "**secondary**" terrorist activities. Secondary activities include conducts that are otherwise legal, but criminalized when conducted in connexion with "primary activities." They include financing, training, recruiting, equipping, encouraging terrorists anywhere in the world[1].

---

1) In this paper we do not differentiate between the terrorists who want to strike within Canada from those whose targets are elsewhere. We do not assess the comparative value of stopping terrorists within Canada or internationally and consider that giving priority to one or the other is a political choice.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

One important aspect of current research about terrorism is a dispute not only about what constitutes terrorism, but what **type of object** is being defined in the first place: is the label meant to apply to individuals, to groups, to objectives or to techniques and strategies — or to various combinations of these facets? Roughly speaking, police and prosecutors tend to apply the label to individuals and groups (who can be formally accused), politicians to objectives (which can be denounced) and social scientists to techniques and strategies (which can be counted and measured). It is a well accepted fact, in terrorism studies, that individuals or groups have no distinctive psychological or social characteristics that can explain their desire to commit terrorist acts. This is a problem for the scientific use of SNA for the study of terrorism. Because SNA centres on groups and their members, its application to terrorist networks rests on either of two shaky premises: 1) that *previous* terrorist acts allow group and/or member labelling or 2) that a potentially successful[2] *future* objective of the group is related to terrorism. One solution is to build analytical strategies around group tasks rather than around individuals.

Lastly, many groups currently labelled as terrorist are in fact only marginally involved in terrorist acts. Such is the case of the Liberation Tigers of Tamil Eelam, FARC, Hamas or Hezbollah, to give only a few examples. These groups may be involved in guerrilla warfare, in governing territories and therefore in a myriad of activities having little or nothing at all to do with terrorism *per se*. In terms of social network analysis, then, they can be expected to have a structure very different from groups formed specifically in order to accomplish violent terrorist acts.

1.2 THE BASICS OF *COVERT* OR *DARK* SOCIAL NETWORK ANALYSIS

It is important to note that the networks this paper is concerned with are covert, or clandestine. Though social network analysis has been used to lay out and describe the activities of such networks in the past (notably, organised crime networks), the large majority of networks that helped the creation and refinement of the technique are different: they are overt, accepted, everyday networks we are all parts of: families, acquaintances, coworkers, Facebook "friends," etc. Information about these networks is easy to collect by observation or interaction and members are willing, if not eager, to cooperate. Covert networks, by contrast, yield extremely low levels of information, which must then painstakingly be pieced together from discrete elements of information. In fact, **the more apt the members, the less information will transpire from a covert network.**

As Krebs (2002) has remarked, terrorist networks are only visible when active — meaning, extremely rarely, for very short periods of time *and usually too late for countermeasures*. This is why the sum total of available examples of SNA applied to covert networks is *ex post facto*

---

2) Social interaction and "one-upmanship" within peer groups may lead to exaggerated claims or overly enthusiastic calls for action which may seem extremist but are, in the end, unlikely to be followed through. Many such cases have been identified in the US, notably in the 2006 Sears Tower bomb plot (or "Liberty City 7" plot) uncovered in Miami, for which all involved were subsequently released (one acquittal, six mistrials).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

analysis, conducted once a substantial portion, or better yet all members of the group are arrested, interrogated, and eventually incarcerated. At that point, most of the information necessary to conduct SNA becomes available. Krebs (2002), in his famous analysis of the 9/11 network, collected his basic data via media reports that followed the attack. This might be useful to subsequent prosecution (assuming living members of the network can be found), but prosecution is already the easiest part of counterterrorism. It is at the phase where the *prevention* of terrorist acts is possible — the hard part — that SNA is more promising.

All networks have the same building blocks: their "nodes," or in our case individual actors (nodes can also be countries, organisations, websites, etc.), and the "links" or "relations" existing between. SNA builds mathematical maps of these nodes, with their links, in order to evaluate various aspects of the network. The visual representation of these maps, well-known and often spectacular, is in fact the least meaningful aspect of SNA. The interesting analyses rest in the evaluation, and comparison, of a number of key aspects: which individuals hold central positions in this network, who controls the most connections and information flows, how closely related are they with the others, what their function (both their social "network" function and their actual task within the group) within the network are.

Once drawn, the network map reveals specific **social characteristics** that are crucial to analysts:

$ *Network density*: is revealed by the number of ties that exist between actors. The more actors are known to other actors, the denser the network. Dense networks are more cohesive because they offer many different paths for information and the incapacitation of an actor-node is of little consequence to the flow (e.g. a family network). This multiplicity of information paths also means that corroboration is easy and the introduction of disruptive false information is difficult. Finally, multiple connections usually rest on and produce *trust* between actors. Such networks will be highly resistant to infiltration. They are, however, extremely vulnerable to surveillance and mapping.

  It is important to note that density is almost never homogenous, that "lumps" exist in the map of connections: there are "elites" who are more connected than others and lay at the centre of a network, with peripheral actors who are much less connected (note that these elites do not necessarily *control* the network; see below).

$ *Actor centrality and "distance:"* this is key to network analysis, since it represents the ability of any actor to connect to any other actor in the group. If all actors know all other actors the distance is kept to a minimum. However, because of the nature of covert networks, where benefits are drawn precisely from *not knowing* as many as possible of the other actors, such groupings typically have very high geodesic distance. In the most secretive cell, relations would be structured as a string of actors where any one only knows, at the most, two other members. Arrest (or disappearance) of any node would cut the flow of information to zero and incapacitate the network (or instantly create two networks instead of one); however, police surveillance is rendered extremely difficult.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Generally speaking, the centrality of an actor is a measure of his freedom within the network. Those with more ties to more of the other actors are less vulnerable to manipulation and more able to manipulate others. However, though this position is beneficial to the member who holds it, this does not mean that the neutralisation of that actor would adversely affect the network, much less disrupt it. Prior knowledge or alternate connections is key. If the removal of this actor does not impact information flows, results are likely to be disappointing — if not entirely counter-productive: it may improve equilibrium between the other members and trigger sufficient change in the way they function to render all previous analyses null and void.

$ *Actor social function or network position*: traditional non-SNA representations of networks or criminal groups rested on the identification of kingpins who set agendas and strategies, recruited other members and profited most from the collective endeavour — the basic idea being that a successful investigation would lead to the arrest of the kingpin and other "big fish" in the organisation. In SNA the importance of any actor to the rest of the network is determined by the relationships the actor has with the other actors. Individuals who fulfill functions approximately equivalent to others are, from the network's point of view, expendable. Unique individuals are, on the contrary, indispensable.

  It is wrong to assume that the more central actors are the most indispensable in the network. They may simply be the more visible. Attention has to be given to actors who are in key positions of linking otherwise isolated portions of the network (so-called "brokers") and those with unique skills.

These sociological characteristics are fundamental to understanding any network, but still not sufficiently precise for investigative purposes. The main objective of social network analysis has always been the study of the organisation of human societies. Its adaptation to law enforcement and intelligence missions, especially in prevention phases, is a recent development and demands further adaptation. In his noted paper, twenty years ago, Sparrow (1991) argued for increased use of SNA in investigations, beyond the graphic representation of criminal gangs that has always been popular. Little has been done since.

Once network and actor characteristics are found, **actor and group tasks** may be inferred with the help of social theory and knowledge of terrorist behaviour.

$ *Actor role within the group*: in terrorist networks some actors sometimes have special skills that make them crucial to the execution of the task. Bomb makers, pilots or computer experts are such examples. Of course any skill is only "key" if it happens to be an integral part of the overall strategy and not a simple coincidence. Those key actors are likely to lay at the periphery, rather than at the centre of the network.

$ *Time to execution*: research is ongoing about structural transformations and especially tell-tale changes in information flows that may indicate that the network is close to an important event, such as an actual attack for terrorists or the arrival of a shipment of drugs for a trafficking ring.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Promising as they may be, these developments run against a series of obstacles that are proving quite difficult to surmount. One is the problem of getting sufficient data to run the statistical link analyses. It is typical to rely on phone records, chatroom records, direct observation and informants/witnesses. For instance, Morselli (2009) presents 5 case studies where police surveillance has uncovered, after months of work, most of the participants in criminal networks. In the case of terrorist networks, such information is extremely difficult to get by, for three reasons: 1) terrorist groups are far less active and have considerably shorter lives than criminal gangs; 2) the objective of the network (its "task") is often not known until it is performed; 2) preparations for the task are usually extremely low-intensity periods of activity, where many individuals are contacted for purposes entirely unrelated.

This missing data problem makes it impossible to evaluate network boundaries, density or any other aspect above. It may result in failure to recognize members of the network, but also in the false identification of outsiders as playing a role, since the nature and contours of the network remain fuzzy. The reason is that networks have multiple levels of overlapping. Any individual is part of many networks at the same time, and thus serves as a connecting node between groups of people who have absolutely nothing else in common. As the Maher Arar case has shown, overlooking this problem can lead to gross misinterpretations of the nature of the relations between individuals. It has been suggested (but is nearly impossible to test) that within 6 degrees of separation, the entire population of earth forms one very large network (Watts, 2003).

1.3 NOTABLE TERRORISM RESEARCH USING SOCIAL NETWORK ANALYSIS

Most SNA applied to terrorism has focussed on the 9/11 attacks. This is unfortunate since these attacks are in fact extreme outliers and can in no way be seen as adequate examples for the bulk of terrorism actually committed Western nations. For instance, no other attack has shown the same level of organisation, the same number of clues (money transfers, pilot training, trips to Afghanistan, etc.), the same network size or the same transnational ramifications. In short, SNA applied to terrorism is in its infancy and conclusions are, at best, tentative.

1.3.1 Krebs' *Uncloaking Terrorism Networks* (2002)

Vladis Krebs is famous for his application of computerized SNA analytical tools to the group responsible for the 9/11 attacks. He organized his map according to media reports and linked individuals together according to three levels of relationships: those living or studying together had the

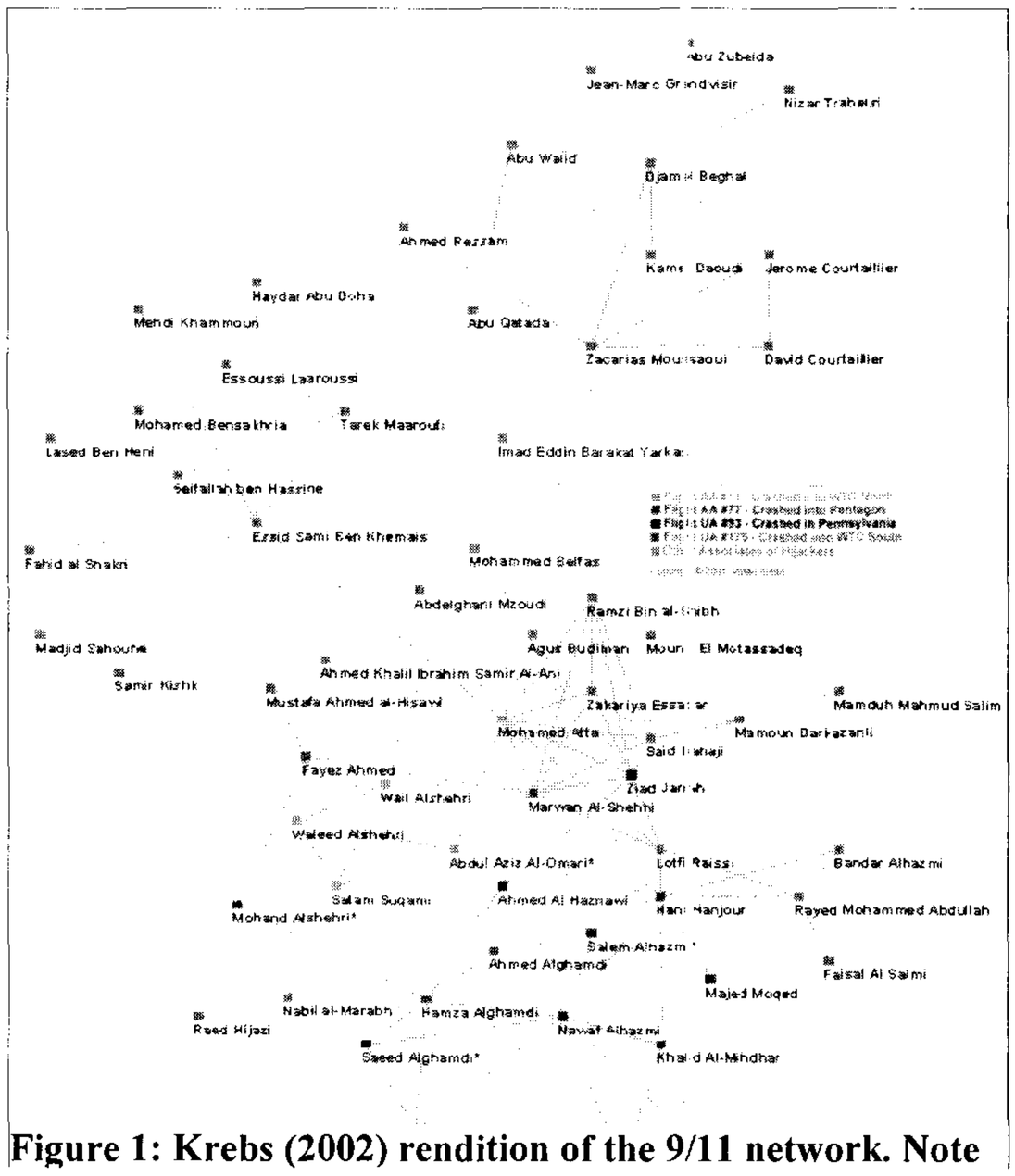


Figure 1: Krebs (2002) rendition of the 9/11 network. Note

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

"strongest" ties, those having travelled together had mid-level ties and those only meeting occasionally had "weak" ties. For the 19 attackers the result is a string-like network of individuals having minimal ties with other members. This means information flows were extremely mediated and inefficient; however this structure resists best to law enforcement detection and surveillance. In figure 1, left, the entire network of known associates is mapped.

One might object that in fact many of the 19 (10, actually) had visa problems and other characteristics that should have put them on the FBI's watch list, and that if the network was geared towards secrecy, it is more coincidence than deliberate planning. Airport cameras also show Atta walking *around* metal detectors, not a behaviour typical of secrecy-minded individuals. In fact, the active 9/11 network was string or snake-like not because of a desire for secrecy, but because members mobilized pre-existing personal (unknown to others) networks in their activities.

One of Krebs' important notes is that in covert networks the strength of ties is not indicative of actual cooperation: actors who wish to remain hidden will minimize contacts with their co-conspirators. Yet those are generally key individuals in the group task. Another is that, as visible in figure 1, non-9/11 prior personal network ties made it possible to repair information flows if one of the conspirators were to be arrested. The only way to stop this network would have been to arrest or otherwise disconnect the "unique skill" members — the pilots. However, in order to do that, intelligence personnel would have to know what the task (flying into buildings) was. In this case it was relatively easy since the pilots had been in training just prior to the attacks and after their arrival in the US. In other cases the task and the unique skill members are likely to be far less obvious.

1.3.2 Sageman's *Understanding Terror Networks* (2003)

Marc Sageman's is probably the best known application of SNA to terrorist networks. His database was constructed from the study of the biography of 172 members of what he has called the Global Salafi jihad. His map, shown on figure 2, reveals 4 main subgroups centred on ethnic background. This matches ethnic origin groupings in pre-2001 al-Qaeda camps.

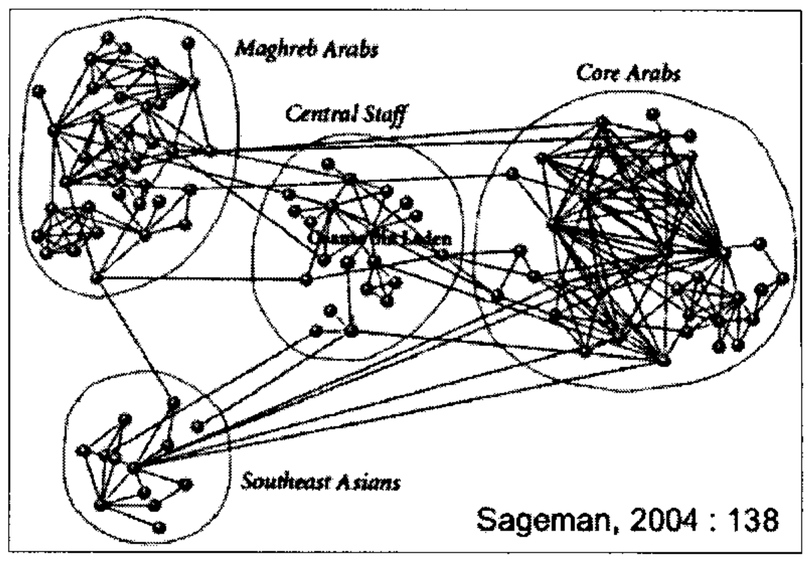


Figure 2: breakdown of worldwide salafi terrorist network according to Sageman (2004).

In each of the subgroups lay rather dense subnetworks organized around "hubs" that act as brokerage points. These points are the only vulnerability of the network: removal would isolate nodes and break down the flow of information. They are also very few, less than 15% of the network's population.

One important point raised by Sageman is the peculiarities of what could be termed "recruitment" to the network — though the word is misleading. The networks never recruit in the classic sense: they do not need to. Networks rest on trust and expand along the lines of previous relationships:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

unknown "free agents" are not welcomed. This is why networks are not necessarily formed in obvious places, such as areas with high concentration of Muslims. Montreal was a disproportionate contributor to the jihad not because of a greater immigrant Muslim population than, say, Paris, but because a hub of the network happened to live there (Sageman, 2002: 143-145). The process of **radicalisation** is essentially network-driven: through a selection process peripheral members become more central as they accept the necessity of violent response to perceived injustice and humiliation against Muslims.

In this first book Sageman raised the possibility of *virtual* networks, where felt bonds to the umma served as ties to a global movement. This argument robs SNA from a lot of its power since it dilutes the nature of the "ties" far too much. In a later book (Sageman, 2008), he abandons this notion and argues that the global movement is not a real-world object but an ideology. His analysis goes back to empirical data and identifies multiple, much smaller, "home grown" networks and abandons the notion of a transnational threat, for which there is no evidence (Sageman, 2008: 125-126).

2 CHARACTERISTICS OF TERRORISM IN CANADA

The Terrorism and Counterterrorism Research Group (erta-tcrg.org) maintains a database of all terrorist and terrorist-related activities in Canada since 1973. Based on media reports, the database now contains over 500 reports categorized according to a wide range of criteria (level of violence, political objective, group affiliation, etc. terrorist incidents alone number 326 for 1973-2006 period). The fact that there is no consensus definition of terrorism is not new and further discussion is unlikely to solve this problem. For research purposes, our group uses an admittedly flawed, but extremely useful operational definition meant to collect a very broad category of acts, which can then be sorted out according to selected variables such as group objectives, organisation, the methods that were used or the results achieved. At the core of our database is this definition: a terrorist act uses or threatens to use of coercive violence for political goals. We can then add specific characteristics (e.g. level of violence, state sponsorship, nature of the target) and observe changes in the intensity or the chronological evolution of terrorism in Canada.

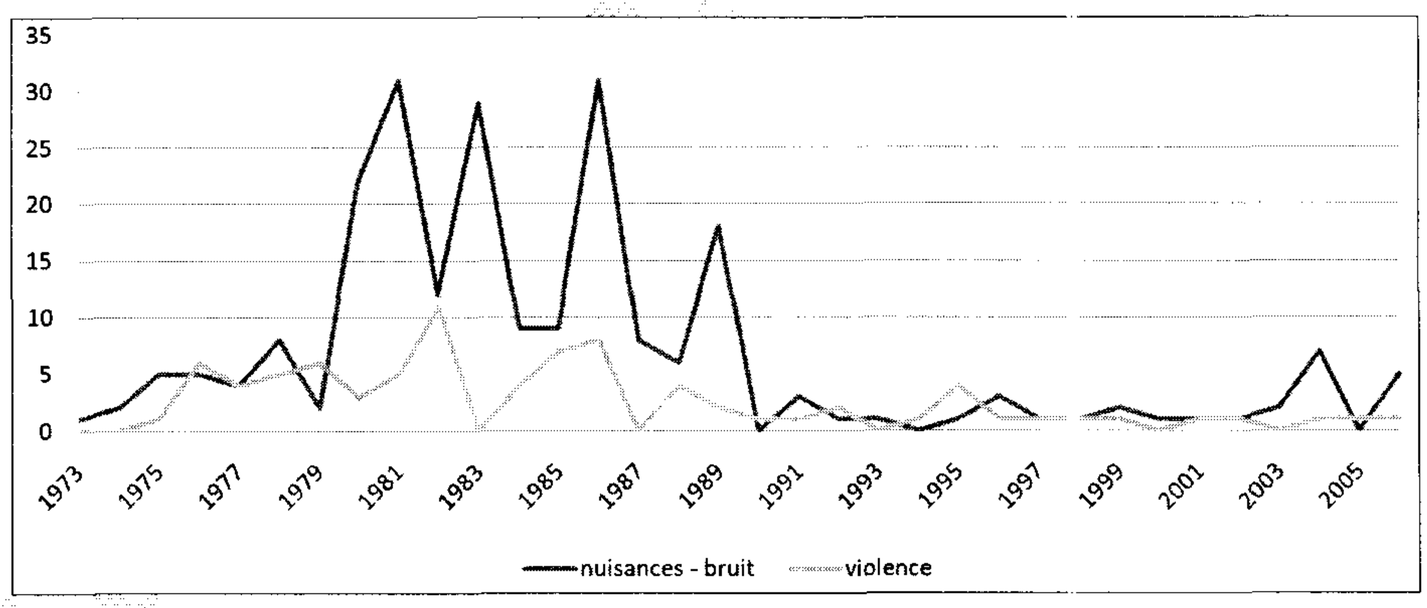


Figure 3: evolution of terrorism in Canada (Leman-Langlois and Brodeur, forthcoming).

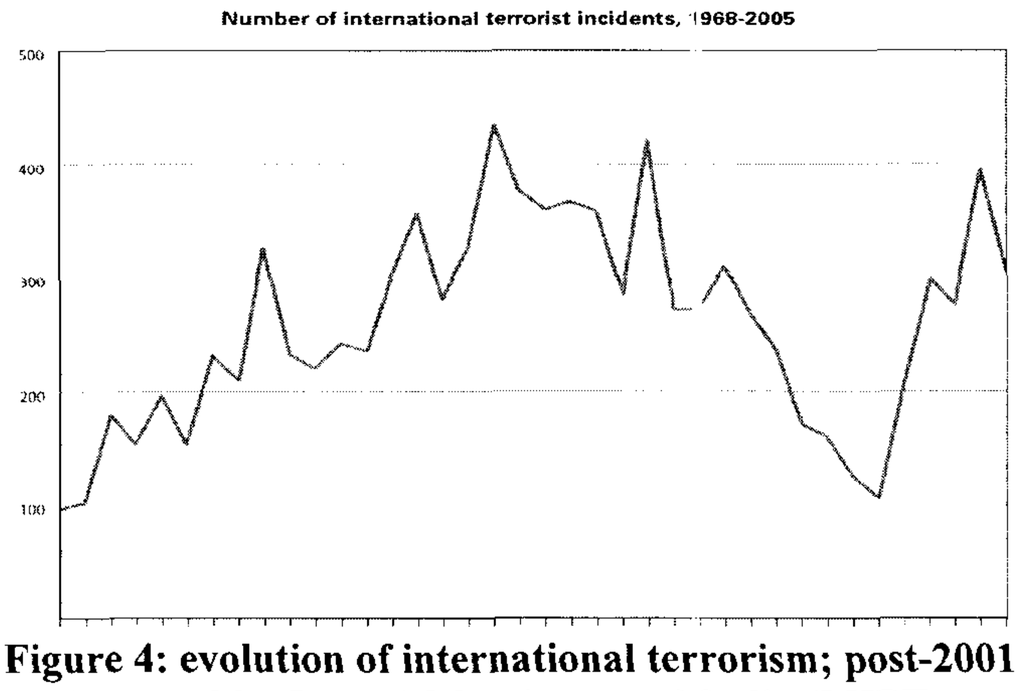


Figure 4: evolution of international terrorism; post-2001 peak caused by Iraq, Afghanistan and India (MIPT

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

On the whole, terrorism in Canada has been in decline for 15 years. International terrorism, as shown by most of the recognized databases (RAND-St. Andrews, MIPT, Iterate, etc.), is also in significant decline. The only true transnational terrorist network, al-Qaeda, has seen the end of its lifespan. Other than through their involvement in local conflicts (e.g. Afghanistan, Iraq), Western democracies have never had such low frequencies of terrorism and political violence.

Figure 3 shows the evolution of terrorism in Canada since 1973, broken down between significant violence and other acts of lesser severity ("noise"). Statistically significant high levels begin in 1980 and end in 1990. This is closely matched by RAND's or MIPT's numbers for global international terrorism.

Figure 4 presents the trend in international terrorism as measured by the MIPT. It does show renewed intensity after 2001, but these numbers have been controversial, since they include terror acts in Iraq and Afghanistan, which are only international because of the presence of a foreign invasion force. When these specific conflict zones are taken out of the database, the trend is in extremely sharp decline.

2.1 GROUP LONGEVITY AND SIZE

In our database most of the classic terrorist groups have all but stopped their activities in Canada since the mid-1990s. This includes LTTE, Hezbollah, PIRA, FARC, "Justice Department" (an animal rights group), ASALA, MEK, BKI or PKK.

Home-grown groups, such as the FLQ, Direct Action or the Sons of Freedom Doukhobor (SOF, whose status as terrorist group is disputable), have all but ceased their activities and, aside from the SOF, had extremely short life spans.

2.2 STRATEGIES USED AND FINANCIAL COSTS

Figure 5 shows the proportion of various levels of severity in terrorist acts in Canada in the last 30 years. Fewer than 10% (30) have involved loss of life, with only 2% targeting persons indiscriminately.

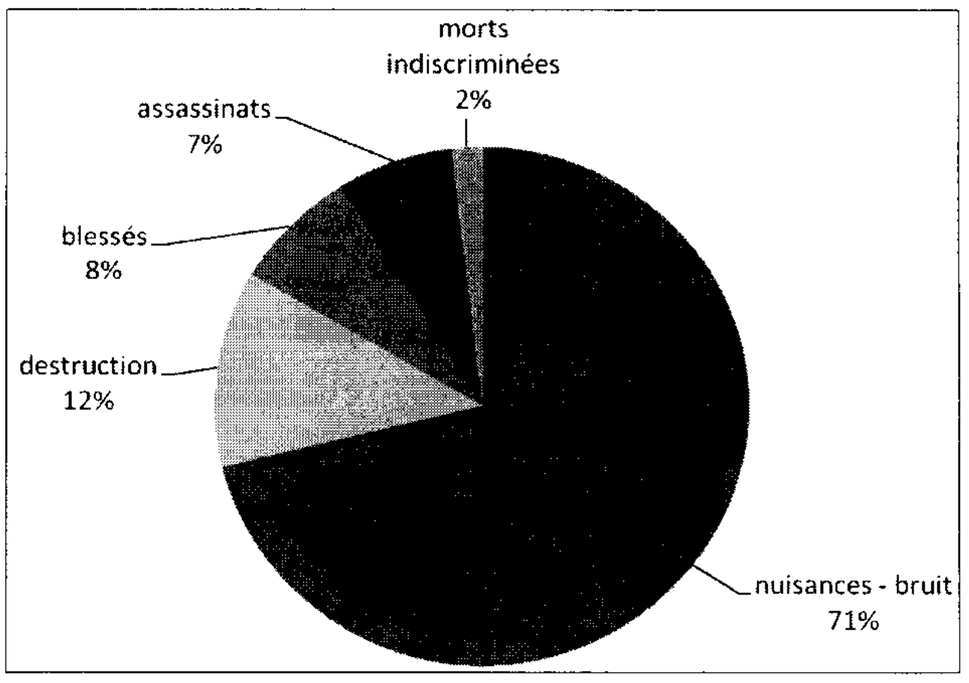


Figure 5: percentage of types of attacks, Canada, 1973-2006 (n=326; Leman-Langlois and Brodeur, upcoming).

The most expensive of these attacks, the one on Air India airliners in 1985, cost less than 3 000$ in plane tickets and was funded locally by one of the conspirators (Ripudaman Singh Malik; Malik also supported Reyat's family after is incarceration for the attack, which are added "costs"). This is also the attack witch probably required the most preparation. In almost all of the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

other recorded attacks, preparation was minimal and costs were much lower (this excludes the so-called "Toronto 18" case, which as of yet has not been sufficiently clarified to be included in our database).

2.3 INTERNATIONAL CONNECTIONS

Terrorist groups conducting primary activities in Canada do not, by and large, have significant contacts outside the country. One possible exception is Samir Ait Mohammed, deported in 2006 after 4 years in detention. According to his accomplice Ahmed Ressam, he had formulated the idea of blowing up a fuel truck in a Montreal neighbourhood he saw as predominantly Jewish. One detail o f this story is important to note:

2.4 SECONDARY ACTIVITIES AND CANADA'S ROLE IN THE GLOBAL WAR AGAINST TERRORISM

Secondary terrorist activities often involve networking beyond national borders. A few cases of logistics have been noted in the past few years, including of course financing guerrilla/terrorist groups abroad (mainly the LTTE). Mohammad "Momin" Khawaja has been found guilty of building a remote controller for detonating a bomb, which he was going to give to conspirators in the UK. Ahmed Ressam built a network in Montreal and a bomb in Vancouver in hopes of attacking LAX in 1999. His connections to French and Bosnian jihadists have been studied by many, but remain quite exceptional. Ali Adham Amhaz plotted to send Hezbollah night-vision goggles and other equipment.

Participation in "Internet Jihad" seems to be on the rise but it remains far too early to tell. The "Toronto 18" had links to Moroccan/UK citizen Younis Tsouli ("irhabi007"), webmaster extraordinaire to the likes of the late Abou Moussab Al-Zarqaoui — Tsouli's 2005 arrest in fact triggered police surveillance of the Toronto group. Saïd Namouh is presently before the courts for his involvement with the Global Islamic Media Front (GIMF), producers of the infamous "Jihad Academy."

Though none of these activities threaten Canada directly, their consequences might be disastrous. If Ressam had succeeded in his attack on LAX, impacts on Canada-US trade and cross-border travel would have been profound. Further, Canada also has a responsibility to protect its allies against terrorist attacks even in cases where such consequences are unlikely.

However, on the whole these activities are rare and low in intensity, which makes them hard to detect and control.

3 EARLY PREVENTION OF TERRORISM

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

SNA is of little help with early prevention but two important findings may be of help. First, terrorists are social beings who *learn* that using violence is a good way to fulfill a political objective, when in contact with others who already believe so. This learning process is usually referred to as "radicalization." If this is true, individuals and groups known to disseminate radical discourses must be monitored. Second, since networks are intertwined and communities are vast interconnected fields, the best way to detect radical discourse and radicalization processes is probably to be a part or this community. Traditional, "community-oriented" policing has the potential of easily fulfilling this objective. Conversely, heavy-handed police and criminal justice tactics against members of such communities are likely to precipitate radicalization processes.

4 *NETWAR*: LATE PREVENTION OF TERRORISM TROUGH DIRECT POLICE NETWORK DISRUPTION

Some of what has been discovered about overt networks and the way humans interact may be used to produce simple predictive hypotheses that can later be applied to complete fragmentary information available about a covert network. For instance, if we know that certain types of networks revolve around members who have special skills, we can infer that individuals who are in key positions of a similar covert network possess certain skills. Discovering their nature will teach investigators a great deal about what is being prepared.

This is termed "late" prevention since it intervenes after the radical group has selected a task. At that stage, attacks may be imminent.

The "netwar" mentioned in this section's title can be misleading. John Arquilla and David Ronfeldt (1996; 2002a; 2002b) have suggested that covert groups preparing criminal acts (e.g. terrorists) or actively engaged in ongoing criminal activities (e.g. organized crime groups) wilfully, knowingly organize themselves into networks because this structure is best suited to maximize efficiency and to resist government intervention. If this were true, many of the basic postulates for SNA would be violated and it would lose most of its value as an analytical tool. In fact, proper SNA cannot assume that individuals are even aware that they are part of a network — much less that they purposefully chose to become one.

It is a well-known fact that terrorist groups tend to organize in "cells," subgroups minimally connected together in order to resist detection and disruption. Ideally, the capture of one cell has no effect on the ability of the others to function. Further, the cell structure reduces problems of trust between members and simplifies recruiting new members (who are usually already known to a few cell members). This is essentially the result of the cell's smaller size. The breakdown of large groups into cells, however, introduces communications problems and makes it possible to introduce disinformation in the network of cells (this is how the release of Ingrid Betancourt was made possible). However, a willingness to organize into cells is not the same thing as claiming that the group has decided to "turn itself into a network." The group was a social network all along, it simply changed its structure. (This, assuming the observers aren't confusing their map with the actual terrain; SNA has had that effect in past research. In many cases the use of the new tool left the impression that the observed groups *had become* networks).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

With those caveats in mind, one can still think of network disruption as "netwar," a convenient way to underline the fact that the weapons and strategies involved are different when one chooses to focus on network characteristics as strategic objectives. Adopting the SNA approach to counterterrorism (or to antigang activities) involves a radical change of perception and strategy. Most obvious is the **discarding of the traditional hierarchical, crime-syndicate view of criminal or terrorist groups**. This means abandoning the familiar concepts of leaders or bosses, followers, orders, fixed structures, attributed and durable tasks or jobs for all members, strict and formalized recruitment, etc., as none of these concepts actually fits reality (Klerks, 2001).

Covert networks are fluid and short-lived structures, in constant evolution, fuelled by improvisation and opportunities, and their members are general entrepreneurs linked together by previously existing networks (Morselli, 2009). This also means that the wider the connections, the more international the networking, the looser the ties; in fact, Klerks (2001) argues that most transnational outfits are strictly opportunity structures, with extremely weak and ephemeral connections.

4.1 WHEN NETWORKS ARE KNOWN

When intelligence has managed to piece together a significant portion of data relative to individuals involved in a common task, SNA can become a part of the intelligence analysis toolbox.

4.1.1 Finding "central" actors; finding "brokers"; finding "special skills"

SNA, combined with the proper terrorism theoretical framework, can help identify individuals holding key positions in a network. Removal of these individuals through arrest or disinformation (leading other members to be suspicious of these actors) can disrupt the network. However, in many cases these arrests will not lead to spectacular cases or severe sentences, since the charges are likely to be modest: though they are indispensable, these individuals are not the "masters" of the network and their criminal offenses are likely to be only marginally serious.

4.1.2 Reduction of trust

Disinformation in the network may lead members to become suspicious and to shun other members, which disrupts network activities. This was done with the FLQ post-1970, as explained elsewhere (Leman-Langlois et Brodeur, 2005), when police managed to tap into the information flow of the network by recruiting a key informant.

4.2 WHEN NETWORKS ARE SUSPECTED

Unknown networks, merely assumed to exist because individuals rarely act alone in terrorism, must be uncovered.

4.2.1 Trawling and datamining

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

SNA, again combined with the proper terrorism theoretical framework, may help sort out data obtained through the monitoring of communications (e.g. phone records, Internet activity). The time, length, frequency and location (through cell data) of phone calls are indicative of types of relationship in a network.

4.2.2 Controlled activation

Disinformation may activate the network and reveal connections. For instance, revealing limited surveillance or secret network information may push members to act, i.e. to connect with each other in a more intensive way.

5 LATE PREVENTION OF TERRORISM THROUGH CRIMINAL JUSTICE

Most of the tactics listed above are essentially covert and do not necessarily involve the justice system. In fact many would not work if the system were used, since the publicity of arrests and trials would reveal too much of the counterterrorist strategy. In fact, not only is SNA poorly adapted to the necessities of the criminal justice system, most of its conclusions seem to question its effectiveness in terms of prevention.

5.1 ROUNDING UP NETWORK NODES

One approach is to devise ways to officially indict all, or most of the network nodes for "pre-terrorist" activities. As mentioned above, ATA provisions already criminalize many of those. Other countries, such as France, have gone further in allowing prosecution all persons even vaguely aware of the activities of the main conspirators (called "association de malfaiteurs"). Responsibility for the overall objective is also shared by all "nodes" in the network, even if only one of them had formulated the original goal. Though controversial (in France, human rights groups have asked for a moratorium on its use for terrorism cases), this approach is actually very dangerous with terrorism, a politically motivated offense, where deep networks exist and mere sympathy for the cause is often extremely common — unlike organized crime, where perpetrators are easy to identify: they continuously receive identifiable material benefits. Applied to terrorism, the penal net tends to extend well beyond the actual extremists.

The problem is that the notion of a planning, pre-terrorism phase is an extremely vague one. If the goal is to formally arrest terrorists before they actually engage in any form of concrete preparation (once these preparations are actually under way, existing Criminal Code provisions should be sufficient), an even greater set of previously legal behaviour will have to be criminalized — while the ATA is already under attack for overreaching.

5.2 CREATING NEW OFFENSES BASED ON NETWORK NODE SOCIAL FUNCTION

Though it is tempting to see it this way, SNA offers no form of "responsibility data" which might translate into criminal indictments. An actor's position within the network, however functionally important, does not reveal his or her level of implication in the criminal conspiracy. SNA is designed to provide analyses useful to sociological theory and its empirical verification; science

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

only provides generalized statements of fact about categories of individuals, with wide margins of error.

5.3 DETERRENCE

There is no evidence that terrorists are deterred by the threat of arrest and punishment. Quite the opposite: state threats and punishments are concrete manifestations of the network's discourse of oppression, injustice and humiliation, legitimizing its existence and facilitating radicalisation. Furthermore, both the severity and the certainty of the punishment (constitutive aspects of deterrence) will translate, in practice, into a presentation of terrorists as dangerous threats to Canada and/or Canadians — or to the world —, worthy of maximum government response: an unintended but particularly flattering compliment for terrorists.

CONCLUSION AND IMPLICATIONS

First and foremost, it must be remembered that SNA as applied to terrorism is in fact an array of theories, postulates and observations, many of which are yet untested or controversial. With this caveat, a few implications for justice policy can be drawn out.

1. **Guilt by association** is an extremely likely by-product of the prosecutorial use of SNA. This methodology was not invented to formally accuse persons of crimes, and does not produce "*responsibility* data." Being a member in a network is not at all like being responsible for any sort of crime.

2. The focus on **network dismantlement via criminal justice** is likely to be inefficient in terms of security — though hit has obvious benefits in terms of public image. Giving priority to arrests, whether in terms of numbers or in terms of the notoriety of those being arrested, goes against what we know about network structure and actor behaviour. In themselves, injudicious arrests may not impede network tasks, and may even help the network function more efficiently or more secretively.

3. Focus on important or **central individuals** is unlikely to adversely affect dark networks, since key players tend to lie at the periphery and limit their involvement and interactions with the other actors (Morselli, 2009; Sageman, 2008). In fact, in typical group prosecutions the severity of punishment has been shown to be inversely proportional to the centrality of the actors (Morselli, 2009: 13). In other words, the more powerful the player, the lesser the punishment.

4. SNA shows that social networks are quite different than what the term "network" has come to represent in popular use, in the media and in political discourse. **Networks are loose groupings of individuals**, based on extremely variable but generally short-lived and utilitarian, objective-oriented connections. They are not the well-organized, disciplined, focussed, responsive, command-and-control hierarchical armies of crime that we constantly hear about (Klerks, 2001). Showing that orders were issued and followed is a powerful prosecutorial tool but, from an SNA point of view, has no correspondence in reality.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5. In SNA, "groups" are called "networks" for a reason: they have a different meaning. Individual nodes are not "members" of a network in the typical sense. Therefore, any criminal law focus on **group membership** is a mistake, as it misrepresents at the same time the nature of the network, of the actors and of their connections. In that sense, the current ATA "terrorist entities list" strategy is unlikely to provide results (see Sageman, 2008).

6. Focus on **media-friendly, spectacular arrests** and the spectacle of criminal justice power against terrorists is counter-productive in the overall effort to reduce extremist networks. I agree with Sageman (2008: 153), who points out that this glorifies the terrorists, proves to their audience that they are important threats to the state. In short, it contributes to their efforts of self-aggrandizement. The 2008 Khawaja trial, with the extreme mobilisation of security (complete with snipers on rooftops) is a perfect example of everything that should be avoided at all costs.

7. This also means abandoning the practice of the spectacular press conference, involving multiple agencies and extreme claims about what was being prepared by terrorists (case in point: the Toronto 18 press conference, where the unlikely plan to *behead the Prime minister* was revealed). **Terrorist networks thrive on such magnification of the threat they represent, which helps them radicalise new members.** Terrorists are ordinary humans who happen to have been connected to a radicalizing network. Any confirmation of network discourse is a direct help to its radicalization process.

8. From a policing point of view, the most productive form of network reduction lies in the fostering of **trusting relationships in communities** rather than in surveillance. No law, no technology and no surveillance strategy can see through community groups who do not trust police. One the other hand, since many extremists self-identify before they embark on a terrorist course, many members of the community will be aware of their plans well before they are close to activation. SNA shows that closed terrorist networks begin as **overt local networks**. Trusted police agents can connect a the periphery of those networks and gather information.

9. This also means that investments in **high-tech surveillance** and additional powers of surveillance, interception, search, seizure, etc. have no preventative power against the formation of covert networks. They can, of course, be useful at a later stage, if radicalized networks can be identified.

10. Finally, increased attention to transnational connexions, especially financial transactions, given the nature of Canadian terrorism, is unlikely to be productive in preventing terrorism. The extent to which it prevents terrorism abroad is difficult to evaluate.

BIBLIOGRAPHY

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Adams, Alayne M. et al. 2006. Measuring social networks cross-culturally. *Social Networks*, 28(4): 363-376.

Arpana, Basu. 2005. *Social network analysis of terrorist organizations in India*. http://www.casos.cs.cmu.edu/events/conferences/2005/2005_proceedings/Basu.pdf.

Arquilla, John and David Ronfeldt.1996. *The advent of netwar*. Santa Monica: RAND Corporation.

Arquilla, John and David Ronfeldt 2002a. *In Athena's camp: preparing for conflict in the information age*. Santa Monica: RAND corporation.

Arquilla, John and David Ronfeldt. 2002b. *Networks and netwars: the future of terror, crime, and militancy*. Santa Monica: RAND Corporation.

Baker, Wayne E. and Robert R. Faulkner. 1993. The social organization of conspiracy: illegal networks in the heavy electrical equipment industry. *American Sociological Review*, 58(6): 837-860.

Baron, Stephen W. and David B Tindall. 1993. «Network structure and delinquent attitudes within a juvenile gang. *Social Networks*, 15(3): 255-273.

Bearman, Peter S. and Kevin D. Everett. 1993. The structure of social protest, 1961–1983. *Social Networks,* 15(2): 171-200.

Benkler, Yochai. 2006. *The wealth of networks: how social production transforms markets and freedom*. New Haven: Yale University Press.

Bernard, Russel K. et al. 1979. Informant accuracy in social network data IV: a comparison of clique-level structure in behavioral and cognitive network data. *Social Networks*. 2(2): 191-218.

Bidart, Claire and Daniel Lavenu. 2005. Evolutions of personal networks and life events. *Social Networks*, 27(4): 359-376.

Bolland, John M. 1985. Perceived leadership stability and the structure of urban agenda-setting networks. *Social Networks*, 7(2): 153-172.

Brewer, Devon D. and Bihchii Laura Yang. 1994. Patterns in the recall of persons in a religious community. *Social Networks*, 16(4): 347-379.

Brodeur, Jean-Paul and Stéphane Leman-Langlois. 2006. Surveillance-fiction: high and low policing revisited. In *The new politics of surveillance and visibility*, eds. K. Haggerty and R. Ericson, 171-198. Toronto: University of Toronto Press.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Burt, Ronald S. 1979. Innovation as a structural interest: rethinking the impact of network position on innovation adoption. *Social Networks*, 2(4): 327-355.

Buskens, Vincent. 1998. The social structure of trust. *Social Networks*, 20(3): 265-289.

Capobianco, Michael and Zbigniew Palka. 1983. The distribution of popular persons in a group. *Social Networks*, 5(4): 383-393.

Carvalho, Fernando Duarte and Eduardo Mateus Da Silva, eds. 2000. *Cyberwar-netwar: security in the information age*. Washington: Ios Pr Inc.

Castells, Manuel. 1996. *The rise of the network society*. Oxford: Blackwell.

Cross, Rob and Andrew Parker. 2004. *The hidden power of social networks*. Boston: Harvard Business School Press.

Curtis, Richard et al. 1995. Street-level drug markets: network structure and HIV risk. *Social Networks*, 17(3-4): 229-249.

Ebel, Holger et al. 2002. Dynamics of social networks. *Complexity*, 8(2): 24-27.

Electronic Frontier Foundation. 2003. EFF Review Of May 20 Report On Total Information Awareness. http://www.eff.org/Privacy/TIA/20030523_tia_report_review.php.

Erickson, Bonnie H. 1981. Secret societies and social structure. *Social Forces*, 60(1): 188-210.

Evans, John. 1994. *Criminal networks, criminal enterprises*. http://www.icclr.law.ubc.ca/Publications/Reports/netwks94.pdf.

Farley, Jonathan David. 2003. Breaking Al Qaeda cells: a mathematical analysis of counterterrorism operations (a guide for risk assessment and decision making). *Studies in Conflict and Terrorism*, 26(6): 399-411.

Fellman, Philip Vos and Roxana Wright. 2009. *Modeling terrorist networks - complex systems at the mid-range*. http://www.psych.lse.ac.uk/complexity/Conference/FellmanWright.pdf.

Fischer, Claude S. and Yossi Shavit. 1995. National differences in network density: Israel and the United States. *Social Networks*, 17(2): 129-145.

Gorman, Sean. 2005. *Networks, Security And Complexity: The Role of Public Policy in Critical Infrastructure Protection*. Cheltenham: Edward Elgar.

Hagan, John. 1997. Defiance and despair: subcultural and structural linkages between delinquency and despair in the life course. *Social Forces*, 76 (1): 119-134.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Hallinan, Maureen T. 1978. The process of friendship formation. *Social Networks*, 1(2): 193-210.

Halpin, Edward F. 2006. *Cyberwar, netwar and the revolution in military affairs*. New York: Palgrave.
Hildum, Donald C. 1986. Competence and performance in network structure. *Social Networks*, 8(1): 79-95.

Holmes, Leslie. 2007. *Terrorism, organised crime and corruption: networks and linkages*. Cheltenham: Edward Elgar.

Hunter, Saundra Mac D. et al. 1991. Identifying mechanisms of adoption of tobacco and alcohol use among youth: The Bogalusa heart study. *Social Networks*, 13(1): 91-104.

Johsnon, Jeffrey C. and Marc L. Miller. 1983. Deviant social positions in small groups: The relation between role and individual. *Social Networks*, 5(1): 51-69.

Keefe, Patrick Radden. 2006. Can network theory thwart terrorists?, *The New York Times*. http://www.nytimes.com/2006/03/12/magazine/312wwln_essay.html?_r=1.

Kick, Edward L. and Davis L. Byron. 2001. World-system structure and change: an analysis of global networks and economic growth across two time periods. *American Behavioral Scientist*, 44(10): 1561-1578.

Klerks, Peter. 2001. The network paradigm applied to criminal organisations: theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. *Connections*, 24(3): 53-65.

Krebs, Valdis E. 2002. Uncloaking terrorist networks. *First Monday*, 7(1): http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/941/863.

Krebs, Valdis E. 2008. *Connecting the dots: tracking two identified terrorists*. http://www.orgnet.com/tnet.html.

Lee, Trevor R. 1979. The resilience of social networks to changes in mobility and propinquity. *Social Networks*, 2(4): 423-435.

Leik, Robert K. and Mary Anne Chalkley. 1997. On the stability of network relations under stress. *Social Networks*, 19(1): 63-74.

Leman-Langlois, Stéphane. 2008. Le terrorisme à motif religieux au Canada, caractéristiques et évolution entre 1973 et 2006. *Criminologie*, 41(2): 9-30.

Leman-Langlois, Stéphane. 2007. Le terrorisme et l'antiterrorisme. In *Traité de sécurité intérieure*, eds. M. Cusson, B. Dupont and F. Lemieux, 199-222. Montréal: Hurtubise HMH.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Leman-Langlois, Stéphane. 2007. Terrorisme et crime organisé, contrastes et similitudes. In *Repenser le terrorisme*, eds. C.P. David and B. Gagnon, 91-110. Québec : Presses de l'Université Laval.
Leman-Langlois, Stéphane. 2006. Le 'méga-crime,' légitimité, légalité et obéissance. *Criminologie*, 39(2): 23-38.

Leman-Langlois, Stéphane. 2003. Rationalité pénale moderne et terrorisme, peut-on contrôler le 'mégacrime' à l'aide du système pénal? In *Comprendre l'acte terroriste*, eds. D. Casoni and L. Brunet, 111-119. Presses de l'Université du Québec.

Leman-Langlois, Stéphane and Frédéric Lemieux. 2007. Renseignement de sécurité et renseignement criminel. In *Traité de sécurité intérieure*, eds. M. Cusson, B. Dupont and F. Lemieux, 335-352. Montréal: Hurtubise HMH.

Leman-Langlois, Stéphane and Jean-Paul Brodeur, eds. Forthcoming. *Terrorisme et antiterrorisme au Canada*. Montréal: Presses de l'Université de Montréal.

Leman-Langlois, Stéphane and Jean-Paul Brodeur. 2005. Terrorism old and new. *Police Practice and Research*, 6(2): 121-140. Also published: 2008. A. Millie and D. Das, eds. *Contemporary issues in law enforcement and policing,* 81-104. Boca Raton: CRC Press.

Lemieux, Vincent. 2000. *À quoi servent les réseaux sociaux?.* Sainte-Foy: Les Presses de l'Université Laval.

Lemieux, Vincent. 2003. *Criminal networks*. Research and Evaluation Branch Community, Contract and Aboriginal Policing Services Directorate Royal Canadian Mounted Police. http://dsp-psd.pwgsc.gc.ca/Collection/JS62-107-2003E.pdf.

Lindelaufa, Roy, Peter Bormb and Herbert Hamersba. 2009. The influence of secrecy on the communication structure of covert networks. *Social Networks*, 31(2).

Lupsha, A. 1983. Networks versus networking. Analysis of an organized crime group. In *Career criminals*, ed. G. Waldo, 43–87. Beverly Hills: Sage.

Martin, John Levi and King-To Yeung. 2006. Persistence of close personal ties over a 12-year period. *Social Networks*, 28(4): 331-362.

Mastors, Elena and Alyssa Deffenbaugh. 2007. *The lesser jihad: recruits and the al-qaida network*. Lanham: Rowman & Littlefield Publishers.

Mcallister, Ian. 1983. Social contacts and political behaviour in Northern Ireland, 1968–1978. *Social Networks*, 5(3): 303-313.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Mcillwain, Jeffrey Scott. 1999. Organized crime. A social network approach. *Crime, Law and Social Change*, 32(4): 301–323.

Mitchell, Clyde J. 1987. The components of strong ties among homeless women. *Social Networks*, 9(1): 37-47.

Morselli, Carlo. 2009. *Inside criminal networks*. New York: Springer.

Morselli, Carlo et al. 2006. The efficiency/security trade-off in criminal networks. *Social Networks*.

Morselli, Carlo and Pierre Tremblay. 2004. Criminal achievement, offender networks, and the benefits of low self control. *Criminology*, 43(3): 773 - 804.

Napoleoni, Loretta. 2005. *Terror incorporated: tracing the dollars behind the terror networks*. New York: Seven Stories Press.

Papachristos, Andrew V. 2007. Murder by structure: dominance relations and the social structure of gang homicide in Chicago. *Social Science Research Network*. Working Paper.

Raab, Jörg and H. Brinton Milward. 2003. Dark networks as problems. *Journal of Public Administration Research and Theory*, 13(4): 413-439.

Réka, Albert et al. 2000. Error and attack tolerance of complex networks. *Nature*, July 2000, 378-382.

Ressler, Steve. 2006. Social network analysis as an approach to combat terrorism: past, present, and future research. *Homeland Security Affairs*, 2(2): 1-10.

Roach, Kent. 2002. *Did September 11 change everything? Struggling to preserve Canadian values in the face of terrorism*. Montreal: McGill Law Journal.

Ronfeldt, David et al. 1999. *The Zapatista social netwar in Mexico*. Santa Monica: RAND Corporation.

Ruef, Martin. 2002. A structural event approach to the analysis of group composition. *Social Networks*, 24(2): 135-160.

Sageman, Marc. 2004. *Understanding terror networks*. Pennsylvanie: University of Pennsylvania Press.

Sageman, Marc. 2007. *Unmasking terror: a global review of terrorist activities*. Washington: Jamestown Foundation.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Sageman, Marc. 2008. *Leaderless jihad: terror networks in the twenty-first century.* Pennsylvania: University of Pennsylvania Press.

Sarnecki, Jerzy. 2001. *Delinquent networks*. Stockholm: National Council for Crime Prevention.

Sparrow, Malcom K. 1991. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, 13(3): 251-274.

Suitor, Jill J. et al. 1997. It's about time: How, why, and when networks change. *Social Networks*, 19(1): 1-7.

Takacs, Károly et al. 2008. Collective action and network change. *Social Networks*, 30(3): 177-189.

Varese, Frederico. 2001. The structure of a criminal network examined: the Russian mafia in Rome. *Oxford Legal Studies Research Paper 21*.

Watts, Duncan J. 1999. *Small worlds: the dynamics of networks between order and randomness.* Princeton: Princeton University Press.

Watts, Duncan J. 2003. *Six degrees: the science of a connected age.* New York: W.W. Norton and Company.

Weimann, Gabriel. 1983. The not-so-small world: Ethnicity and acquaintance networks in Israel. *Social Networks*, 5(3): 289-302.

Zahab, Mariam Abou. 2004. *Islamic networks*. London: Hurst.

Zeggelink, Evelenn. 1995. Evolving friendship networks: An individual-oriented approach implementing similarity. *Social Networks*, 17(2): 83-110.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

A Discussion of the Ramifications of Terrorism Trials

by

Dr. David MacAlister

of

Simon Fraser University,
School of Criminology

A discussion paper presented to the

Department of Justice Canada

The views expressed in this report are those of the author and do not necessarily represent the views of the Department of Justice

000674

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Very little research exists regarding the impact of counter-terrorism activities on the communities from which terrorists emerge.[1] In particular, no empirical research appears to exist on the impact of terrorism trials on the communities to which the terrorists belong. The key issues addressed in this paper are as follows:

1. How have terrorism trials in Canada and abroad been received in Canadian communities that share an identity with the terrorist?
2. How do terrorism trials impact on the radicalization efforts of violent extremists and on the de-radicalization efforts of communities and governments?
3. Can public legal education, changes in legal procedure, funding for courts, or differing media strategies influence any impacts outlined in the preceding two questions?

Reception of terrorism trials in Canadian communities sharing an identity with the accused terrorist

To date, there has been no systematic collection and publication of data that directly addresses the way in which terrorism trials are received in communities sharing an identity with the accused terrorist. Information regarding the impact of terrorism trials on Canadian communities sharing an identity with alleged terrorists can only be obtained through anecdotal data and informed conjecture at this time.

A significant amount of recent speculation on terrorism has focused on Islamic terrorism. As the war in the Gulf appears to wind down, there is an increasing societal awareness that the future terrorist threat of greatest significance is likely to come from homegrown terrorists. Accordingly, future governmental efforts to combat terrorism are more likely to focus on domestic initiatives than international ones. These domestic initiatives involve the local investigation and prosecution of suspected terrorists. While Muslims living in the west have felt alienated in the recent past by the military campaigns carried out in the Gulf region, their attention is likely to turn to concern over the treatment of Muslims here at home as the focus of counterterrorism efforts turns inward. Accordingly, governments need to concern themselves with the perceptions held by the local Muslim community toward the investigation and prosecution of alleged Muslim terrorists. However, Canada's dealings with terrorism have not been confined to the Islamic context.

Major terrorism trials in Canada have affected a few select identifiable ethnic or cultural groups. Among the major terrorist incidents in Canada that resulted in trials against alleged terrorists are those involving the FLQ in the 1970s, those pertaining to the Air India/Narita Airport bombings, and of course the most recent pertaining to Muslim extremists. Terrorism is not confined to cultural or religious-based motivations. With the recent advent of various forms of "single issue" terrorism,[2] it is imperative that consideration be given to the possible positive and negative effects on those supporting these extremists that may flow from the trial of those involved in such matters.

---

[1] Jarvis and Lister, "Counter Terrorism, Citizenship and Community Cohesion," attempt to assess the scant literature on the impact of counter-terrorism tactics such as stop and search practices on identifiable minority groups, finding greater discomfort amongst the affected groups in the UK than in the US.

[2] For example, eco-terrorism, animal rights terrorism, and anti-abortion terrorism.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Separatist Terrorism: The FLQ

The October Crisis of 1970 represented the culmination of almost a decade of terrorist violence in Quebec, targeting the federal and provincial governments in that province. Terrorists advanced a separatist and socialist agenda, seeking to compel change through violence. In addition to bombing and various other acts of violence, the events of that period eventually resulted in the kidnapping of British Trade Commissioner, James Cross, and the kidnapping and killing of the provincial Labour Minister, Pierre Laporte.[3] The events of 1970 resulted in the *War Measures Act* being imposed, allowing domestic military deployment, the expansion of police powers and the curtailment of civil liberties.

Among the various trials emanating from the period, some of the most notable were the trial of Francis Simard, Paul Rose and his brother, Jacques Rose, for the kidnapping and murder of Pierre Laporte. While Francis Simard and Paul Rose were convicted and sentenced to life in prison, Jacques Rose was eventually acquitted after his first trial resulted in a hung jury and a subsequent retrial resulted in an outright acquittal.[4] Another member of the organization, Bernard Lortie, was convicted of the Laporte kidnapping and sentenced to 20 years, but was not charged in the murder.[5]

In addition to the trials of those involved in the Laporte kidnapping and killing, the FLQ members involved in the Cross kidnapping also eventually faced trial. The key principals in this kidnapping had initially managed to evade justice by taking exile in Cuba. However, several of them eventually returned to Quebec in the mid 1970s after the election of PQ government in that province. Louise Lanctot and Jacques Cossette-Trudel eventually pled guilty to the kidnapping, receiving provincial jail sentences.[6] Jacques Lanctot returned to face justice, receiving a 3 year term for his role.[7] Among others eventually returning, Marc Carbonneau received a 20 month sentence, and Yves Langlois received a 2 years less a day sentence.[8] Nigel Hamer, a participant in the kidnapping who never left the country, received a one-year jail term.[9]

The various trials flowing from the FLQ incidents appear to have had a minimal impact on the francophone community within Canada. A number of factors may have affected this outcome. First, it appears that while many Quebecers may have held some sympathy for the FLQ during the early period of their activity, the actions of the FLQ that resulted in the death of Pierre Laporte appear to have diminished support within the community.[10] Many appear to have perceived the assassination of a local government official, who had been democratically elected within the province, to be beyond the pale. Accordingly, the loss of community sympathy appears to have been accompanied by a desire to see those responsible censured for their actions.

---

[3] Crelinsten, "Internal Dynamics of the FLQ."
[4] Ibid., 64-65.
[5] Ibid., 64.
[6] Ibid., 65.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Davidson Smith, "Canada's Counter-Terrorism Experience," 87 refers to the assassination as the FLQs "most damaging mistake."

000676

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The trials appear to have been accepted by the local community as an appropriate day of reckoning for those who sought the noble objective of Quebec independence, but who went too far in their tactics. Second, in the years immediately following the FLQ's activity, the Parti Quebecois gained control of the Quebec legislature. This party advanced on a platform of Quebec sovereignty, including a call for a referendum on continued association with the rest of Canada. The democratic political process had, by the mid 1970s, come to bear on the situation in Quebec, providing a viable way forward that was not tied to terrorist violence. Most of the trials of the various participants in the October crisis did not occur until the late 1970s and early 1980s, a period in which the PQ was solidly entrenched as the provincial government in the province. Third, the trials involved the application of the normal criminal law, resulting in the application of measured penalties upon the conviction of those found culpable. Special powers played virtually no role in the process. Those found responsible for wrongdoing received penalties reflecting minimal jail time for the acts committed. Finally, it is noteworthy that the FLQ never did constitute a highly organized terrorist network. The dismantling of the FLQ was relatively easy given their lack of organization, leadership and discipline.[11]

Sikh Terrorism: Air India/Narita Bombings

In June of 1985, two airliners operated by Air India were the subject of terrorist bomb attacks. One of these aircraft was in transit from Toronto, ultimately bound for Bombay. This flight, Air India flight 182, blew up over Irish airspace resulting in the loss of the 329 lives onboard. On the same day, Air India flight 301 out of Narita Airport, near Tokyo, Japan, was in the process of being loaded with bags and passengers when a bomb exploded amongst the baggage. The bomb was in bags being transferred from those that arrived on a Canadian Pacific Airlines flight out of Vancouver. That explosion resulted in the death of two baggage handlers and the injury of four others at Narita airport.

The bombings were alleged to have been the work of a group of Sikh separatists in Canada known as Babbar Khalsa. In 1991, Inderjit Singh Reyat was extradited from England to stand trial for the Narita bombings. In that year, he was convicted on two counts of manslaughter in relation to the killing of the baggage handlers in Japan. In 2003, Reyat pled guilty to manslaughter charges in relation to the flight 182 bombing, receiving a sentence concession in exchange for his testimony against others alleged to have been involved in the plot. He remains the only person convicted in relation to these events.

In 2000, two others alleged to be involved in the Air India bombing incidents were charged with first degree murder. Ripudaman Singh Malik and Ajaib Singh Bagri stood trial on 329 counts of first degree murder. A lengthy trial spanning almost two years ensued, ultimately culminating in acquittals for both Malik and Bagri in 2005. Judge Ian Josephson was not satisfied that the Crown had met the burden of proving its case beyond a reasonable doubt. The judge appeared to be unimpressed with Reyat's testimony in that case, calling his sincerity into account. In 2006, the Crown announced Reyat was being charged with perjury in regard to his testimony during the Malik and Bagri trial. Reyat remains free on bail pending his trial on these perjury charges.

---

[11] Charters, "The Amateur Revolutionaries," 163.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The Air India airliners appear to have been targeted by Sikh extremists in an effort to retaliate against the government of India as owners of the Air India airline. This retaliation appears to have been a response to the Indian government's attack on the Sikh Golden Temple at Amritsar in 1984. The members of the Sikh group Babbar Khalsa appear to be committed to forcing the creation of a separate Sikh homeland, to be called Khalistan, in the Punjab, India.

The impact of the trials involving Reyat, Malik and Bagri appear to have had little or no negative impact on the Sikh community in Canada. Many Sikhs appear to have been appalled by the bombing incidents, perhaps due in part to the loss of many Sikh lives in the Air India bombing. The Sikh community around the world was undoubtedly horrified by the actions of the Indian army at the Golden Temple; however, the response taken by the Canadian militants responsible for the bombings appears to have attracted little approval. Today, the Sikh independence movement appears to have died down, but underlying conflicts may still prevail. Khalistan independence remains an active topic on the internet. In 2007, the Indian government formally protested a float in a parade that carried the portrayal of Talwinder Singh Parmar, an alleged mastermind in the Air India bombings, as a martyr.[12] In 2008, the Indian High Commission in Ottawa raised concerns with the Canadian government regarding pro-Khalistan independence activities in Canada.[13] None of this appears to have a direct connection to the outcome of the Reyat, Bagri or Malik trials.

Islamic Extremist Terrorism

In the years following 9/11, terrorism committed by Islamic extremists has moved to the forefront as a topic of concern amongst both the public and academia. In addition to the massive loss of life among our American neighbours, Canada was directly impacted by 9/11 itself. This is reflected in the deaths of at least 23 Canadian citizens at the World Trade Centers. In the years since then, Islamic extremism has formed the subject matter of terrorism trials, both here at home and in other western nations.

In 2006, 18 individuals belonging to a purported Islamic terrorist cell were arrested in the Greater Toronto area. The arrests, which became known as the Toronto 18, were initially lauded in the media as reflecting the breakup of an Al-Qaeda inspired terrorist cell; however, in recent months the incident has become embroiled in controversy. The roles of two informants, Mubin Shaikh and another unidentified individual, have been called into question. The implication behind the recent concern in this case is that these informants may have actually provoked the group into militant action.

A number of individuals who were originally arrested in this matter have subsequently seen the charges against them dropped, while others still await trial. To date, only one of the accused, a young offender, has gone to trial on terrorist-related offences. That individual was convicted in late 2008.[14] The accused was convicted of facilitating a terrorist group under s. 83.18 of the *Criminal Code*, a provision brought into place by the *Anti-Terrorism Act*. The case attracted attention for the concern it raised regarding the possibility of being convicted of a

---

[12] *Indo-Canadian Online*: http://indocanadianonline.blogspot.com/2007/04/india-protests-portrayal-of-terrorist.html
[13] *Thaindian News*: http://www.thaindian.com/newsportal/uncategorized/india-raises-concern-over-khalistan-activities-in-canada_10026473.html
[14] *R. v. Y. (N.)* 2008 CarswellOnt 5964 (Ont. Sup. Ct. J.), per Sproat J.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

terrorist offence based simply on one's association with others involved in a terrorist group.[15] The main concern raised by Professor Roach's critique of the case is that the "facilitating terrorism" provision does not require one to be a terrorist planning a specific terrorist act, nor be guilty of entering a terrorist conspiracy, before being convicted under this clause. Lack of knowledge that a particular terrorist activity is facilitated, or even whether any particular terrorist-related activity was foreseen or planned by the group at the time it was facilitated do not offer a defence to a charge under the relevant provisions.[16]

The most significant terrorism-related trial in recent years has been that of Mohammad Momin Khawaja. This individual was accused of involvement in bomb plots in the UK. He was convicted in October of 2008 of several offences pertaining to financing and facilitating terrorism, plus related *Criminal Code* offences pertaining to his involvement in the creation of a remote control triggering device.[17] More recently, he was sentenced to 10 ½ years in prison for these offences.[18]

Clearly, Khawaja's case involves a serious incident of an international nature, involving numerous other Islamic extremists overseas, at least one of whom have had ties to other serious terrorist cases.[19] In contrast, the Toronto 18 case has attracted considerable criticism, particularly following the release of a documentary downplaying the likelihood that those involved should be considered a serious threat.[20]

Muslim communities in Canada are affected, like the rest of Canada, by perceptions of justice flowing from individual cases. Those Muslims who have integrated into the fabric of Canadian society are concerned about violent terrorist acts committed by Muslims and non-Muslims alike. Similarly, if a trial appears to unjustly label those involved with the stigma of being a terrorist, it is as much a matter of concern for the Muslim community as it is for non-Muslims in Canadian society.

Issue-Based Terrorism

A number of specific high-profile issues have attracted organized resistance in the form of terrorist acts. Some members of various social activist groups have periodically crossed the line from protest to violent action in an effort to have their views accepted by society at large.

While many environmental activists have engaged in legitimate protest, others have more aggressively advanced their position through practices such as "spiking" trees and damaging logging equipment to stop logging operations, damaging pipelines to frustrate oil and gas development, and damaging ships involved in the whaling industry. Some animal rights protesters have engaged in acts that have been considered terrorist in nature. Among the acts in

---

[15] Roach, "The Toronto Terrorism Conviction."
[16] Ibid. Note his discussion regarding s. 83.19(2)(b) of the *Criminal Code* at 158.
[17] *R. v. Khawaja* (2008), 238 C.C.C. (3d) 114 (Ont. Sup.Ct.J.). A criticism of Justice Rutherford's earlier ruling in that case that motive is irrelevant in the definition of "terrorist activity" is provided by Plaxton, "Irruptions of Motive."
[18] *Globe & Mail* online: http://images.theglobeandmail.com/v5/content/pdf/ReasonsforSentence0312.pdf
[19] Khawaja is known to have been associated with Omar Khyam, an individual with known connections to one of the London 2005 bombers.
[20] "Unfair Dealing: The Toronto Homegrown 'Terror' Threat" Youtube Online: http://www.youtube.com/user/UnfairDealing.

000679

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

question are damage done to laboratories using animals for research purposes, the release into the wild of captive animals such as mink, and the threatened poisoning of Turkeys in grocery stores.

Among the many anti-abortion advocates are those who transcend traditional protest practices and engage in acts of violence. In Canada, several doctors who provide abortion services have been the subject of violent attacks.[21] In addition, abortion clinics have been the subject of vandalism.

The Terrorist Radicalization Process

Radicalization involves "the process of transformation of ordinary people into extremists using violence for political means."[22] It has been argued that the radicalization process in the current era differs from that of the past. Marc Sageman asserts that contemporary Al Qaeda terrorism differs from that of its origins in the 1980s, when it first came to prominence under the leadership of Osama bin Laden.[23] Furthermore, the contemporary process of radicalization is even believed to differ from that which produced those responsible for the events of 9/11. Today, potential Muslim terrorists are rarely linked directly what Sageman calls "Al Qaeda Central." This is undoubtedly because counter-terrorist strategies have made significant inroads at stymieing the ability of the organization to direct terrorist operations around the world. Today, home-grown groups appear to constitute the greatest Islamic terrorist threat. This is the nature of the group responsible for the London bombings of 2005, and it best characterizes those referred to as the Toronto 18.

Many popular beliefs regarding the causes of terrorist radicalization appear to be erroneous. It has been asserted by Sageman that active recruitment and brainwashing of potential terrorist recruits is not a common occurrence.[24] Friendship and kinship appear to be important factors in the process of joining a radical terrorist group.[25] Like-minded Muslims develop friendships in Mosques, but Sageman downplays the role of the Mosque (and also the role of Madrassas[26]) as a source of radicalization.[27] Social affiliation amongst potential members of the jihad, accompanied by the intensification of beliefs and faith may result in radicalization, but active involvement in the terrorist campaign will probably only arise if connections are made to the global jihadist movement.[28]

---

[21] At least three doctors who perform abortion services were shot in the late 1990s: Fainman, Short and Romalis. See "Sniper Attacks on Doctors Create Climate of Fear in Canada" *New York Times*, October 29, 1998. Avilable online at: http://www.nytimes.com/1998/10/29/nyregion/sniper-attacks-on-doctors-create-climate-of-fear-in-canada.html?pagewanted=all .

[22] Sageman, "A Strategy for Fighting International Islamist Terrorists," 225.

[23] Sageman, *Leaderless Jihad.*

[24] Sageman. *Understanding Terror Networks*, chapter 4.

[25] Sageman, *Leaderless Jihad*; Sageman, "Radicalization of Global Islamist Terrorists."

[26] Sagman, *Leaderless Jihad.*

[27] Ibid., 114-120. Sageman has been engaged in debate with Bruce Hoffman over the significance of such factors in the radicalization process, and the role of "Al Qaeda central" as an ongoing Muslim terrorist threat. See: Sageman, "The Reality of Grass-Roots Terrorism" and Hoffman, "The Myth of Grass-Roots Terrorism." Evans in "Understanding Madrasahs," and Bergen and Pandey in "The Madrassa Scapegoat" also downplay the role of Madrassa's in the radicalization process.

[28] Ibid., 120.

000680

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

It has been asserted that terrorism, like other forms of collective action such as insurgency and guerrilla action requires a confluence of events to act as a trigger. Anthony Oberschall has argued that this requires: (1) discontent, (2) ideology-feeding grievances, (3) capacity to organize, and (4) political opportunity.[29] To the extent that terrorism trials increase or decrease these factors, an impact on terrorist activity may be expected.

Discontent refers to widespread dissatisfaction and unhappiness for which appropriate means of relief are lacking. If this prevails, a radical solution may be viewed by many as offering promise. If it is lacking, the terrorist group will be viewed as outlaws seeking to have their personal goals fulfilled.[30]

Terrorism is fostered where there is a widely spread ideology or belief system in the community. This ideology holds public figures and the larger society responsible for the discontent, transforming those feelings into identifiable grievances. This has the effect of legitimizing the change or reforms sought by the terrorist group. Absent a legitimizing ideology, the violence is not likely to be viewed as justified, nor accepted by the community giving comfort to the terrorists.[31]

Terrorist organizations require a capacity to recruit new members, raise funds, communicate with one another, and make decisions in a structure that maintains leadership authority. This is often difficult, given the need to maintain secrecy. For Islamic terrorism, this may arise in the context of the religious infrastructure involving a key role for religious leaders and teachers in schools and Mosques,[32] or more recently, over the internet.

Political opportunity refers to the need to maintain the support of public opinion within the group, and among political allies. Outside support, often in the form of a foreign state or sponsorship by a more powerful terrorist organization provide opportunities for terrorism to be sustained.[33]

Oberschall sees the greatest hope for addressing Islamic terrorism through addressing political opportunity.[34] Minimizing or eliminating the ability of foreign states or overseas sponsors to back terrorism are seen by him as having the best promise. It is arguable that the law has a small role to play in this to the extent that it can be used to control financing of terrorist efforts. However, more recent theorizing on Islamic terrorism calls for concern over terror networks arising domestically, without significant connections to international support.[35]

---

[29] Oberschall, "Explaining Terrorism," 27-28.
[30] Ibid., 27.
[31] Ibid., 28
[32] Ibid., 28.
[33] Regional and international support structures for terrorism appears to be lacking in recent years. Terrorist groups appear to operate in relative isolation: Miller, "The Terrorist Mind: I," 124.
[34] Ibid., 36.
[35] Sageman, in "Radicalization of Global Islamist Terrorists," views the process of Muslim radicalization through a series of key factors, which he identifies as: (1) moral outrage, usually as a reaction to perceived immorality on the part of the west; (2) interpretation, whereby the moral outrage is interpreted in a way capable of fostering radicalization, typically interpreting actions of the west as part of a war against Islam; (3) resonance with personal experience, the moral outrage and interpretations attached to it are found to reflect the personal everyday experience of the individual, such as discrimination and lack of employment opportunities; and (4) mobilization through

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

If Muslim's perceive themselves as disadvantaged, discriminated against, or otherwise unfairly treated, a perception within that religious group that counter-terrorism measures will adversely impact their security can be expected.[36] Jarvis and Lister make the point that Muslims in Europe are at greater risk for these perceptions than Muslims in the U.S., since the latter are better integrated into western society.[37] Anti-terrorism measures appear to be responsible for deteriorating community relations among Muslims, particularly in those societies where Muslims are not fully integrated into the fabric of society. The conclusion that counter-terrorism measures may actually cause an increase in the likelihood of terrorism occurring[38] is clearly linked to the process of radicalization.[39]

The process through which radicalization occurs appears to be fairly complex. McCauley and Moskalenko found as many as twelve mechanisms at play in the development of political radicalization among individuals, groups and mass publics.[40] Some mechanisms have a clear impact on the individual, while others have an impact on a larger scale, affecting an entire group or population.[41] From their list of radicalizing mechanisms, it appears that criminal trials may contribute to radicalization primarily through two related mechanisms. First, the trials may establish a "political grievance" if they are perceived as unjust, whereby individuals are pulled towards radical thinking by accepting an interpretation of the terrorism trial as political and discriminatory. Secondly, "jujitsu politics" involves using counter-terrorism actions, such as military force and the invocation of special powers, as a focus of outrage to engender support for

---

networks, whereby frustration and anger is vented to others, usually through the internet where a network of likeminded individuals contact one another.

[36] Jarvis and Lister, "Counter Terrorism, Citizenship and Community Cohesion." The extent of alienation caused by aggressive counter-terrorism strategies is a major cause of concern in that it carries the potential for increasing support for terrorism within the community from which the terrorist comes, and it may thereby lend support to recruitment efforts: Lambert, "Salafi and Islamist Londoners."

[37] The perception among Muslims of a greater level of discrimination and non- belonging in Europe has also been noted by Azzam, "The Radicalization of Muslim Communities in Europe." Feelings of discontent, supplemented by a rejection of the foreign policy of many European states that has supported the invasion of Iraq, when combined with radical ideology are asserted by Azzam to present the source of the radicalization problem in Europe. Post and Sheffer in "The Risk of Radicalization" concur that U.S. Muslims are not as radicalized as European Muslims; however, they note that many U.S. Muslims remain angry over foreign and domestic policy affecting this ethno-cultural group, feeling alienated from U.S. society. Indeed, they report that 40 percent of Americans hold feelings of prejudice towards Muslims. Efforts at de-radicalization in Europe are likely to employ tactics to minimize the sense of alienation among immigrant Muslim populations: Githens-Mazer, "Variations on a Theme." This is consistent with the U.K. government's belief that lack of opportunity and inequality contribute to the radicalization process: Wither, "The United Kingdom's Campaign Against Radicalization."

[38] Ibid., 16. Some research indicates that violent retaliation after a terrorist attack increases subsequent terrorism, while arresting terrorists takes them out of circulation and legitimizes authority if they are tried in the normal criminal justice system: Nevin, "Retaliating Against Terrorists."

[39] It has been estimated by Post and Sheffer in "The Risk of Radicalization" that 80 percent of new recruits to Muslim terrorism come from those who have been "disaffected and radicalized within diaspora communities" around the world.

[40] McCauley and Mosalenko, "Mechanisms of Political Radicalization."

[41] Ibid. The authors identify the following factors: (1) Personal victimization, (2) political grievance, (3) joining a radical group – the slippery slope, (4) joining a radical group – the power of love, (5) extremity shift in like-minded groups, (6) extreme cohesion under isolation and threat, (7) competition for the same base of support, (8) competition with state power – condensation, (9) within-group competition – fissioning, (10) jujitsu politics, (11) hate, and (12) martyrdom.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the terrorist cause.[42] However, McCauley and Mosalenko's overview shows that radicalization likely arises from a number of factors that have little or nothing to do with terrorism trials.

Interpretations of the Qu'ran favourable to radicalization do not appear to reflect mainstream Muslim understanding of the sacred text.[43] It is important to note that extremist Islamic religious beliefs were identified by a group of incarcerated Muslim terrorists as the most important factors motivating them towards terrorist activity.[44]

Impact of Terrorism Trials on Radicalization into Violent Extremism

It may be argued that the risk of terrorism is perhaps best managed by organizing legislative responses to terrorism by structuring the law in a way that most closely approximates the regular criminal process.[45]

It is difficult to assess the extent to which these terrorist trials have influenced the radicalization of youth among the Muslim community in Canada. Those Imams holding anti-western views are undoubtedly inspired to critically comment upon terrorist trials involving alleged Muslim terrorists. It would come as no surprise if they were further inspired by weak cases or cases involving border-line activity. Elevating a criminal prosecution to one that has "terrorist" implications where the conduct in question is not of a clear nature may have the effect of stirring increased radicalization. However, the research remains to be done on this topic.[46]

To the extent that the invasion of Iraq has presented an impetus towards radicalization, it is arguable that trials perceived to be part of that "war" also contribute to the problem. The application of the criminal process to those alleged to be terrorists rarely treats the accused as "citizens" subject to the regular "criminal law for citizens", but rather as enemies of the state, subject to a special "criminal law for enemies", and in the U.S., it has been asserted that foreign terrorists were even treated as enemy combatants whose treatment went beyond the law under the regime prevailing at Guantanamo Bay.[47] Differential treatment may be perceived as discrimination contributing to the justification for a violent anti-state response. Those alleged terrorists coming from abroad deserve the same basic rights as Canadians when faced with criminal prosecution in this country.[48]

---

[42] The cyclical nature of terrorism and aggressive state response followed by elevated levels of terrorist activity has been well-documented in the literature. See Miller, "The Terrorist Mind: I," 134. This appears to better explain terrorist incidents than psychological factors: Miller, "The Terrorist Mind II."

[43] Loza, "The Psychology of Extremism and Terrorism."

[44] Ibid., 148. See also, Sageman, *Understanding Terror Networks*.

[45] See Lord Lloyd in his review of the UK legislation in 1996: *Inquiry into Legislation against Terrorism* (CM. 3420), discussed in Walker, "Terrorism and Criminal Justice."

[46] In one of the few reviews of research on the impact of counter-terrorism measures, Lum et al. in "Are Counter Terrorism Strategies Effective?" noted some strategies actually have the effect of increasing the likelihood of terrorist acts occurring. Their look at increasing severity of punishment found only one dated study (Landes, 1978) that attempted to assess the impact of increasing the severity of punishment for aircraft hijacking on subsequent hijackings, finding the increase in severity of sentence had no impact on frequency of this event's occurrence.

[47] Wilke, "War .v Justice."

[48] Crépeau and Jiminez, "Foreigners and the Right to Justice." Treating terrorism as a normal law enforcement problem meriting the application of the normal criminal law also finds support in Parker, "Fighting the Antaean Enemy."

000683

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The use of emergency powers in Northern Ireland, including the use of special pre-trial and trial procedures, was found to diminish confidence in the judicial process with little or no appreciable increase in public safety.[49] Indeed, many researchers found the use of emergency powers were accompanied by an increase in violence, or "backlash" effect.[50]

In Northern Ireland, de-emphasizing a militaristic response, and de-politicizing trials so as to treat terrorists in the normal criminal process was initiated in 1976.[51] Treating the wrongdoers as criminals rather than political prisoners appears to have had the effect of reducing the perceived legitimacy of these offenders among the local community. While the research on "deterrence" and "backlash" effects remains inconclusive, LaFree and his colleagues appear ready to abandon deterrence-based approaches to counter-terrorism strategies, in favour of the normal criminalization approach.[52] In the Islamic context, showing terrorists to be criminals rather than martyrs may decrease their status in the eyes of their own community,[53] thereby decreasing the impetus towards radicalization. It has been claimed that the roots of radicalism are best addressed "through the promotion of social justice and true democracy."[54]

A significant number of terrorism trials will eventually result in increased numbers of individuals subject to penal disposition. Having a significant number of terrorists in prison may eventually lead to the prison being used as a recruiting ground for new terrorists:

> Terrorists jailed for criminal activities thrive in prison. Disciplined and belonging to networks that are internally cohesive, they are free to recruit and train inmates they believe to be suited for work within a terrorist organization, and they are able to draw from a constantly regenerating pool of candidates. Local and immigrant, Muslim, non-Muslim, the bright, the dim, the violent: all are courted, all have a place in the network – provided they prove susceptible to indoctrination and radicalization.[55]

Past experience, with both IRA and Basque Separatist ETA prisoners, has shown terrorist radicalization occurs in prison.[56] As increasing numbers of terrorists are sent to prison, efforts to curb radicalization in that context need to be entertained. Initially, splitting up terrorists into different prisons may prove to be a useful tactic; however, this may not work as a long-term strategy since the numbers of those convicted and sentenced to prison may make this impossible. Efforts to disseminate a moderate message through the use of education and the employment of moderate Muslim prison chaplains may prove to be options worth exploring in the future.

---

[49] O'Connor and Rumann, "Into the Fire."
[50] LaFree, Dugan and Korte, "The Impact of British Counterterrorist Strategies."
[51] Ibid., 26. The U.K. has been criticized for employing a different approach to international terrorism post-9/11than it applied in recent years in the Northern Ireland terrorism context. It has been asserted that it should have stuck to the lessons learned from their response to the Northern Ireland situation, de-emphasizing special powers and procedures outside the normal criminal law realm: Blackbourn, "International Terrorism and Counterterrorist Legislation."
[52] Ibid., 38.
[53] Loza "The Psychology of Extremism and Terrorism."
[54] Ibid., 151.
[55] Cuthbertson, "Prisons and the Education of Terrorists," 19.
[56] Warnes and Hannah, "Meeting the Challenge of Extremist and Radicalized Prisoners."

000684

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Impact of Terrorism Trials on the De-radicalization Efforts of Communities and Governments

Effective criminal trials may have a de-escalating effect on radicalization and the cycle of violence that accompanies it. If prosecutions are not forthcoming, police and other security forces may become frustrated. They often perceive themselves to know who the terrorist threats are, even if they can not prove their identities or harmful conduct in court. A risk arises that state terrorism may displace established norms of social control provided by the normal justice system should the police take matters into their own hands. In such cases, increased tactical activity by the police may inspire an increased level of insurgency on the part of terrorists. Informants and infiltrators are a cause of great concern to clandestine terrorist groups. Heightened vigilance among terrorists may also lead to danger for former activists and acquaintances. A successful series of prosecutions may effectively diminish the ability of a terrorist group to carry out sustained, coordinated activity, particularly if key figures within the organization are brought into custody.

Various researchers have sought to outline the conditions under which terrorism ends. Ross and Gurr,[57] as well as Wilkinson,[58] have provided well-known lists of conditions that are believed to produce a reduction in terrorist activity. These factors include effective state response strategies. Successful trials may have a positive effect in pre-empting future terrorist acts through incapacitating those who are the greatest threat. They may also have the positive spin-off effect of providing public censure for the actions of the terrorist, particularly in cases where the terrorists have engaged in acts that produce harm to members of their own culture. However, the opposite effect may also result from ostensibly successful terrorism trials. As some members of a terrorist group become captured, tried and convicted, they may become martyrs and possibly become the object of further terrorist attention, since members of the terrorist organization who have managed to evade capture may take hostages in an effort to secure the release of their comrades through negotiation. This places the public at increased risk. Often, violence escalates in a cyclical fashion, as evidenced by the events in Northern Ireland over much of the last century where terrorism was often met with an aggressive state response, only to be followed by an escalation in terrorist activity.[59]

Social control efforts are likely to be accepted, even by those who are the targets of control, if they entail what is perceived to be a fair process. John Braithwaite has asserted that the Muslim world community would be less defiant and resentful about the U.S. approach to counterterrorism if they felt the U.S. acted in good faith in its middle-east dealings and showed a higher degree of social responsibility.[60] The use of criminal trials to respond to terrorism appears to stand a greater chance of achieving this objective than a response developed within a military

---

[57] Ross and Gurr, "Why Terrorism Subsides." They identify four factors: (1) preemption through imprisonment or death of terrorists, (2) deterrence through increasing the risks for terrorists, (3) burnout associated with declining commitment to the cause, and (4) backlash arising from declining political support for the terrorists' acts and objectives.

[58] Wilkinson, "Pathways out of Terrorism." He identifies six pathways out of terrorism: (1) voluntary abandonment of violence, (2) failure of a terrorist campaign, (3) an effective draconian state response, (4) a political solution, (5) a law enforcement solution, and (6) educational strategies convincing them the struggle is counterproductive.

[59] Ibid., 29-30.

[60] Braithwaite, "Pre-empting Terrorism."

000685

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

framework. To this end, the use of the "war on terrorism" analogy may be counterproductive in the de-radicalization context.

Strategies Affecting Radicalization/De-radicalization Efforts:

There is a need for evidence-based research to help identify the best counterterrorism response strategies. Very little empirical research has been carried out in this area, despite ongoing calls for the same.[61]

Public Legal Education

No evidence appears to be available regarding the impact of increasing public legal education on the perceptions of particular communities flowing from terrorism trials. However, it appears logical to assume positive benefits can accrue to increased public education on these matters. Public outreach has long been a hallmark of community policing, whereby the police have managed to improve their performance through maintaining positive relations with the public.

In regard to public outreach programs, it has been noted that efforts by London police to use negotiation skills to persuade young Muslims that al Qaeda propaganda should not be followed, carries potential as a small scale response that can have a positive effect on reducing potential radicalization at the grass roots level.[62]As part of a coherent, overall counter-radicalization strategy, police-community outreach appears to be a useful element.

More generally, government efforts to support moderate Muslims should be encouraged:

> Offering a counterweight to the different forms of radicalisation is not an easy undertaking. Undoubtedly, cooperating with moderate Muslims is extremely important. They must be supported and stimulated so they can uphold another voice. The dissemination of radical ideas must be stopped, not by simply repressing them, but by giving moderate alternatives a voice. Radical ideologies must receive a moderate and not-dogmatic answer. The 'disarmament' of the radical discourse must be done by experts, both within and outside the communities. The existing organisations and initiatives, as well as the authorities, media and educational institutions can play a meaningful role in disarming the radical discourse by promoting the circulation of democratic and moderate ideas.[63]

These efforts ought to supplement measures designed to ensure Muslim integration into the socio-economic fabric of society.[64] This is consistent with the recommendations of Rekawek, who argues that governments should "direct action and resources to preemptive cultural, economic, political, and social action which could counter the rise of terrorism."[65]

Outreach projects involving the police, and prosecutors involved in terrorism-related trials, may prove to be a valuable tool in countering radicalization. The presence of these individuals in schools and other community venues may help to disseminate a moderate message. Those involved should be careful to ensure their presence in the community does not become perceived as further exacerbating feelings of persecution and alienation which they are

---

[61] Lum, Kennedy and Sherley, *The Effectiveness of Counter-Terrorism Strategies*.
[62] Lambert, "Empowering Salafis and Islamists Against Al-Qaeda."
[63] Fraihi, "(De-)Escalating Radicalisation," 137.
[64] Ibid.
[65] Rekawek, "How 'Terrorism' Does Not End."

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

attempting to minimize. The use of government officials who are also minorities themselves may have a positive effect.

Changes in Legal Procedure

Respect for the "rule of law" in tackling terrorism is undoubtedly an important objective in minimizing the opportunities for radicalization. Canada should endeavour to maintain its legitimacy amongst the various cultures within it by treating everyone fairly and equitably. Legislation barring religious, ethnic and racial profiling would help to send a positive message of inclusion to currently disaffected minorities.[66] Ensuring that those accused of terrorism are given the same due process safeguards[67] is essential to maintaining the moral high road in the war against terrorism.[68] Campbell and Connolly draw on the lessons learned from the U.K.'s efforts in dealing with the I.R.A., asserting that the avoidance of "egregious repression" in responding to Islamic terrorist violence may be expected to reduce the likelihood of community tolerance of violent extremism.[69]

Prosecutorial strategies may have a possible impact on the effect the trial has on affected communities. Austin Turk has argued that terrorism prosecution strategies may take on one of two forms.[70] Prosecutors employ either "explicit politicality" or "exceptional vagueness" strategies when prosecuting terrorists. Explicit politicality involves clear and express use of the terrorist label in trial documents and in the acccused's portrayal to the news media. Exceptional vagueness is a strategy whereby prosecutors avoid depicting the accused as a terrorist. Instead, the offender is characterized as a traditional criminal. These differing strategies were shown by Turk to impact the trial process; however, they might also affect how the accused is perceived by their own community. More recent research by Brent Smith and his colleagues has identified a third, middle ground approach which they refer to as "subtle innuendo."[71] In this strategy, the prosecutor charges the offender as a regular criminal, but drops subtle hints during the trial that the accused is a terrorist in order to generate a desired effect with the jury.[72] While Smith and others have been conducting a fair amount of research on terrorist trials,[73] their focus has been largely confined to prosecution and defence strategies, and direct case outcomes rather than delving into the impact of differing prosecutorial strategies on the offender's community. Further research is need in this regard.

Most suspected terrorists caught in Canada should be subjected to the normal process of the criminal law:

---

[66] This is a recommendation advanced by Beutel in "Radicalization and Homegrown Terrorism in Western Muslim Communities." A call to stop racial profiling is also found in Bahdi, "No Exit."
[67] Berger, "Reflections on Khadr."
[68] Malinowski, "Restoring Moral Authority" argues that America has lost much of its moral authority in the world as a result of its post 9/11 counter-terrorism strategies, resulting in diminished reputation and influence in the world, and concomitantly adding to the perception of legitimacy with which terrorists are viewed (at 156). The need to maintain a healthy respect for civil liberties in the face of terrorism has been advanced by many legal scholars, most notably Roach, "Did September 11 Change Everything?", Toope, "Fallout From 9-11."
[69] Campbell and Connolly, "Making War on Terror?"
[70] Turk, *Political Criminality*.
[71] Smith, et al., "Prosecution and Punishment of International Terrorists."
[72] Ibid.
[73] See, for example, the recent work of Smith et al., "Prosecuting Politically Motivated Offenders," and Damphousse and Shields, "The Morning After."

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> Where the sufficiency of evidence criteria can be met, those suspected of terrorism should be prosecuted and, if guilty, punished. This would ensure that suspected terrorists are treated like other suspected criminals and entitled to the same protections and safeguards that special administrative measures, protracted and indefinite detention do not supply. Using the criminal law renders transparent any attempt to water down these safeguards, not least in respect of the standard of proof. It requires that the offence be clearly specified so that the accused know the nature of the charges laid against them.[74]

To the fullest extent possible, the normal criminal process ought to apply to terrorism trials. We can not allow a security culture to undermine our traditional respect for fundamental rights.[75] The incorporation and application of the Anti-Terrorism regime that has been brought into the *Criminal Code* contains numerous potential pitfalls. The definitions are vague, leading to a risk of casting too wide a net. The new offences add little or nothing to the existing *Criminal Code* provisions which already outlaw many acts typically associated with supporting terrorist groups.[76]

The differential treatment of accused terrorists carries the adverse potential for ostracizing, stigmatizing, and alienating members of the particular ethnic group from which the offender comes, if the law is perceived as being disproportionately applied to members of that specific ethnic group.[77] In the context of extraordinary powers available under U.S. law, Ronald Dworkin has stated:

> With hardly any exceptions, no American who is not a Muslim and has no Muslim connections actually runs any risk of being labelled an enemy combatant and locked up in a military jail. The only balance in question is the balance between the majority's security and *other* peoples' rights, and we must think about that as a matter of moral principle, not of our own self interest.[78]

There is obvious potential for the Anti-Terrorism legislation of this country to be similarly applied in a discriminatory manner.[79]

If it is accepted that the application of the *Anti-Terrorism Act* provisions carry a risk of further alienating and disaffecting members of the Muslim community, then it appears to be appropriate to apply a risk analysis to determine whether the advantages of doing so outweigh the disadvantages in choosing this course of conduct. Arguably, cases in which there is a significant likelihood of a massive level of harm that could occur from the conduct of the accused, may call for the use of the *Anti-Terrorism Act* provisions. In such a case, the benefits may outweigh the possible negative impact on Muslim views of the legitimacy of the process. However, where the risk of a terrorist act's occurrence is low and the likely harm that could be

---

[74] Zedner, "Securing Liberty in the Face of Terror," 529. In this regard, see also Lowe, "Clear and Present Danger."
[75] Toope, "Fallout from '9-11,'" Roach, *September 11*, Roach, "Did September 11 Change Everything?"
[76] See Borovoy, *Categorically Incorrect*, ch. 2. Expanding the scope of those caught by lowering the threshold of culpability has the ironic effect of increasing the numbers of those found to be rule-breakers: Welch, "Ironies of Social Control."
[77] Effective intelligence gathering and terrorist investigation will undoubtedly suffer if police are unable to retain the confidence of minority groups as a result of a perception that the law unfairly targets specific ethnic groups. See Hanniman, "Canadian Muslims, Islamophobia and National Security."
[78] Dworkin, "Terror and the Attack on Civil Liberties."
[79] See Bhabha, "Tracking 'Terrorists' or Solidifying Stereotypes," who argues the *Anti-Terrorism Act* is in contravention of the *Charter* equality guarantee. Similarly, see: Boccabella, "Profiling the *Anti-Terrorism Act*." Choudry and Roach in "Racial and Ethnic Profiling" argue that the exercise of discretion, if used to ethnically profile, should result in a *Charter* remedy due to the resultant discrimination. See also Roach, "Making Progress."

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

expected from it is low, the negative consequences of applying the *Anti-Terrorism Act* provisions likely outweigh any potential benefits that might accrue. In such circumstances, the application of the normal criminal law should suffice as a response. The difficult cases will be those that fall in between the two extremes. In such cases, discretion must be used to balance the possible positive and negative consequences before choosing a course of action.

Threat Assessment and Charge Choice

Likelihood of Occurrence

Amount of Anticipated Harm	Low	High
High	Discretionary Response	Apply Anti-Terrorism Act Provisions
Low	Apply Normal Criminal Offences	Discretionary Response

In the less serious cases, the use of the terms "terrorist" and "terrorism" in court are problematic. The possibility of these terms inflaming the Muslim community militate against any potential tactical gain in the trial or perceived public relations gain to be made by the government among the non-Muslim general public.

Funding for Courts

No evidence appears to be available regarding the impact of altering court funding on the perceptions generated regarding terrorism trials. Funding for legal aid and funding to ensure minimal trial delay may benefit the legal system in general; however, they are unlikely to have specific benefits in the terrorism trial context that do not prevail in the criminal process more generally.

Differing Media Strategies

The media have a significant impact on terrorism. Indeed, it has been argued that the sympathetic francophone media in Quebec may have exacerbated the situation in that province during the October crisis, engendering support for the FLQ and necessitating the use of extreme

000689

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

measures by the authorities.[80] Communication of the threat posed by terrorism necessarily changes over time as the dynamics of the situation change.[81]

Sageman argues that efforts need to be expended to diminish the perception among Muslims that terrorists are to be respected for their actions. This can be accomplished through media strategies that diminish the glorification of terrorist acts:

> Within this strategy of containment, it is important to neutralize the main drivers of the radicalization process: a search for glory and thrills. Terrorist acts must be stripped of glory and reduced to common criminality. Nothing is more glorious to terrorists than to go against uniformed men and women from the only remaining superpower. The fight against these terrorists must be demilitarized and turned over to law enforcement.[82]

This requires tactics designed to diminish the fame, and in some cases martyrdom, associated with terrorist acts. Government officials should avoid holding high profile press conferences after arrests have been made or trials concluded, where the terrorist nature of the alleged wrongdoing is given primacy:

> It is…important not to allocate too much importance to terrorists who are arrested or killed. Leaders must resist the temptation to hold press conferences to publicize another 'major victory' in the war on terror. These events have the undesired effect of elevating the status of terrorist criminals to that of heroes. Low-key arrests and prosecution should degrade the status of terrorists.[83]

Since terrorists seek the attention of the media,[84] and the media may play an important role in fomenting dissension among disaffected groups, media strategies need to be cognizant of this and downplay the drama of terrorist-response events.

The use of the phrase "war on terror" is also highly problematic. Exposure to such rhetoric undoubtedly adds to the likelihood of radicalization among young, impressionable Muslim youth who may interpret the phrase as a "war against Islam", thereby playing into the hands of those who seek to promote radicalization among this population. The "war" metaphor glorifies "jihad" in some circles, and is perceived by some young Muslims as signalling their way to martyrdom, confirming in their mind that their involvement in terrorist activity will produce an eternal reward should they die for their cause.

Educating the Islamic world about the true nature of western society, including Canada's core values, may be an effective element in the response to radicalization.[85] Alienation can be expected to foster radicalization, so efforts should be made to minimize feelings of alienation among Muslims.[86] The use of any terminology that can be interpreted as treating terrorist suspects as "not belonging" produces a problematic mindset among those prone to radicalization.

---

[80] Cohen-Almagor, "The Terrorists' Best Ally."
[81] Gibbs van Brunschot and Sherley, "Communicating Threat."
[82] Sageman, "A Strategy for Fighting International Islamist Terrorists" 228-229.
[83] Ibid., 229.
[84] Frey and Luechinger, "Decentralization as a Disincentive for Terror."
[85] This is identified as a key element in a counter-radicalization strategy, as outlined by Loza, "The Psychology of Extremism and Terrorism."
[86] Cilluffo, Cardash and Whitehead, "Radicalization."

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Muslim communities feel alienated by "us" and "them" terminology, since they are likely to perceive themselves as being painted with the same brush as the alleged terrorists.

Released under the Access to Information Act

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Bibliography

Azzam, M. "The Radicalization of Muslim Communities in Europe: Local and Global Dimensions" *Brown Journal of World Affairs*, 13(2) (2007): 123-134.

Bahdi, R. "No Exit: Racial Profiling and Canada's War Against Terrorism" *Osgoode Hall Law Journal*, 41 (2003): 293-317.

Bergen, P. and S. Pandey. "The Madrassa Scapegoat" *The Washington Quarterly*, 29(2) (2006): 117-125.

Berger, B.L. "The Reach of Rights in the Security State: Reflections on *Khadr v. Canada (Minister of Justice)*" *Criminal Reports* (6th), 56 (2008): 268.

Beutel, A.J. "Radicalization and Homegrown Terrorism in Western Muslim Communities: Lessons Learned from America" Minaret of Freedom Institute (2007). Available online at: http://www.minaret.org/MPAC%20Backgrounder.pdf

Bhabha, F.A. "Tracking 'Terrorists' or Solidifying Stereotypes: Canada's *Anti-Terrorism Act* in Light of the *Charter*'s Equality Guarantee" *Windsor Review of Legal and Social Issues*, 16 (2003): 95-136.

Blackbourn, J. "International Terrorism and Counterterrorist Legislation: The Case Study of Post 9/11 Northern Ireland" *Terrorism and Political Violence*, 21(1) (2009): 133- 154.

Boccabella, J. "Profiling the *Anti-Terrorism Act*: Dangerous and Discriminatory in the Fight Against Terrorism" *Appeal: Review of Current Law and Law Reform*, 9 (2003): 17-31.

Borovoy, A.A. *Categorically Incorrect: Ethical Fallacies in Canada's War on Terror*. Toronto: The Dundurn Group, 2006.

Braithwaite, J. "Pre-empting Terrorism" *Current Issues in Criminal Justice*, 17 (2005): 96-114.

Campbell, C. and I. Connolly. "Making War on Terror? Global Lessons from Northern Ireland" *Modern Law Review*, 69(6) (2006): 935 – 957.

Charters, D.A. "The Amateur Revolutionaries: A Reassessment of the FLQ" *Terrorism and Political Violence*, 9(1) (1997): 133-169.

Choudry, S. and K. Roach. "Racial and Ethnic Profiling: Statutory Discretion, Constitutional Remedies, and Democratic Accountability" *Osgoode Hall Law Journal*, 41 (2003): 1-36.

Cilluffo, F.J., S.L. Cardash, and A.J. Whitehead. "Radicalization: Behind Bars and Beyond Borders" *Brown Journal of World Affairs*, 13(2) (2007): 113-122.

Cohen-Almagor, R. "The Terrorists' Best Ally: The Quebec Media Coverage of the FLQ Crisis in October 1970" *Canadian Journal of Communication*, 25(2) (2000): 251.

Crelinsten, R.D. "The Internal Dynamics of the FLQ During the October Crisis of 1970" *Journal of Strategic Studies*, 10(4) (1987): 59-89.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Crépeau, F. and E. Jimenez. "Foreigners and the Right to Justice in the Aftermath of 9/11" *International Journal of Law and Psychiatry*, 27 (2004): 609-626.

Cuthbertson, I.M. "Prisons and the Education of Terrorists" *World Policy Journal*, 20(2) (2004): 15-22.

Damphousse, K. R. and C. Shields. "The Morning After: Assessing the Effect of Major Terrorism Events on Prosecution Strategies and Outcomes" *Journal of Contemporary Criminal Justice*, 23(2) (2007): 174 – 194.

Davidson Smith, G. "Canada's Counter-Terrorism Experience" *Terrorism and Political Violence*, 5(1) (1993): 83 – 105.

Dworkin, R. "Terror and the Attack on Civil Liberties" *New York Review of Books*, 50(17) (November 6, 2003): 37-38.

Evans, A. "Understanding Madrassas" *Foreign Affairs*, 85(1) (2006): 9-16.

Fraihi, T. "(De-)Escalating Radicalisation: The Debate within Muslim and Immigrant Communities" ch. 11 in R. Coolsaet (ed.) *Jihadi Terrorism and the Radicalisation Challenge in Europe*. Aldershot, UK: Ashgate, 2008.

Frey, B.S. and S. Luechinger. "Decentralization as a Disincentive for Terror" *European Journal of Political Economy*, 20 (2004): 509-515.

Gibbs van Brunschot, E.E. and A.J. Sherley. "Communicating Threat: The Canadian State and Terrorism" *The Sociological Quarterly*, 46 (2005): 645-669.

Githens-Mazer, J. "Variations on a Theme: Radical Violent Islamism and European North African Radicalization" *Political Science and Politics*, 41(1) (2008): 19-24.

Hanniman, W. "Canadian Muslims, Islamophobia and National Security" *International Journal of Law, Crime and Justice*, 36 (2008): 271-285.

Hoffman, B. "The Myth of Grass-Roots Terrorism" *Foreign Affairs*, 87(3) (2008): 133-138.

Jarvis, L. and M. Lister. "Counter Terrorism, Citizenship and Community Cohesion" Paper presented at the Annual Convention of the International Studies Association, San Francisco, March 26-29, 2008.

LaFree, G., L. Dugan and R. Korte. "The Impact of British Counterterrorist Strategies on Political Violence in Northern Ireland: Comparing Deterrence and Backlash Models" *Criminology*, 47(1) (2009): 17-45.

Lambert, R. "Salafi and Islamist Londoners: Stigmatised Minority Faith Communities Countering al-Qaida" *Crime, Law and Social Change*, 50 (2008): 73-89.

Lambert, R. "Empowering Salafis and Islamists Against Al-Qaeda: A London Counterterrorism Case Study" *Political Science and Politics*, 41(1) (2008): 31-35.

000693

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Levin, B. "Trials for Terrorists: The Shifting Legal Landscape of the Post-9/11 Era" *Journal of Contemporary Justice*, 23(2) (2007): 195-218.

Lowe, V. "'Clear and Present Danger': Responses to Terrorism" *International and Comparative Law Quarterly*, 54 (2005): 185-196.

Loza, W. "The Psychology of Extremism and Terrorism: A Middle-Eastern Perspective" *Aggression and Violent Behavior*, 12 (2007): 141-155.

Lum, C., L.W. Kennedy, and A. Sherley. " Are Counter-Terrorism Strategies Effective? The Results of the Campbell systematic Review on Counter-Terrorism Evaluation Research" *Journal of Experimental Criminology*, 2 (2006): 489 – 516.

Lum, C., L.W. Kennedy, and A.J. Sherley. *The Effectiveness of Counter-Terrorism Strategies.* Campbell Systematic Reviews. Rutgers, NJ: The Campbell Collaboration, 2006.

Malonowski, T. "Restoring Moral Authority: Ending Torture, Secret Detention, and the Prison at Guantanamo Bay" *Annals of the American Academy of Political and Social Science,* 618 (2008): 148 – 159.

McCauley, C. and S. Mosalenko. "Mechanisms of Political Radicalization: Pathways Toward Terrorism" *Terrorism and Political Violence*, 20 (2008): 415-433.

Miller, L. "The Terrorist Mind: I. A Psychological and Political Analysis" *International Journal of Offender Therapy and Comparative Criminology*, 50(2) (2006): 121-138.

Miller, L. "The Terrorist Mind: II. Typologies, Psychopathologies, and Practical Guidelines for Investigation" *International Journal of Offender Therapy and Comparative Criminology*, 50(3) (2006): 255-268.

Nevin, J.A. "Retaliating Against Terrorists" *Behavior and Social Issues*, 12 (2003): 109-128.

Oberschall, A. "Explaining Terrorism: The Contribution of Collective Action Theory" *Sociological Theory*, 22(1) (2004): 26-37.

O'Connor, M.P. and C.M. Rumann. "Into the Fire: How to Avoid Getting Burned by the Same Mistakes Made Fighting Terrorism in Northern Ireland" *Cardozo Law Review*, 24 (2003): 1657-1751.

Parker, T. "Fighting the Antaean Enemy: How Democratic States Unintentionally Sustain Terrorist Movements they Oppose" *Terrorism and Political Violence*, 19(2) (2007): 155-179.

Plaxton, M. "Irruptions of Motive in the War on Terror" *Canadian Criminal Law Review*, 11 (2007): 233.

Post, J.M and G. Sheffer. "The Risk of Radicalization and Terrorism in U.S. Muslim Communities" *Brown Journal of World Affairs*, 13(2) (2007): 101-112.

Rekawek, K.E. "How 'Terrorism' Does Not End: The Case of the Official Irish Republican Army" *Critical Studies on Terrorism*, 1(3) (2009): 359-376.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Roach, K. "Editorial: The Toronto Terrorism Conviction" *Criminal Law Quarterly*, 54 (2008): 157.

Roach, K. "Making Progress on Understanding and Remedying Racial Profiling" *Alberta Law Review*, 41 (2004): 895-903.

Roach, K. *September 11: Consequences for Canada*. Montreal & Kingston: McGill-Queen's University Press, 2003.

Roach, K. "Did September 11 Change Everything? Struggling to Preserve Canadian Values in the Face of Terrorism" *McGill Law Journal*, 47 (2002): 893 – 947.

Ross, J.I. and T.R. Gurr. "Why Terrorism Subsides: A Comparative Study of Canada and the United States" *Comparative Politics*, 21(4) (1989): 405-426.

Sageman, M. "The Reality of Grass-Roots Terrorism" *Foreign Affairs*, 87(4) (2008): 165-166.

Sageman, M. "A Strategy for Fighting International Islamist Terrorists" *Annals of the American Academy of Political and Social Science*, 618 (2008): 223-231.

Sageman, M. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2008.

Sageman, M. "Radicalization of Global Islamist Terrorists" Presentation to United States Senate Committee on Homeland Security and Governmental Affairs, June 27, 2007.

Sageman, M. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Smith, B., K. Damphousse, F. Jackson, and A. Sellers. "The Prosecution and Punishment of International Terrorists in Federal Courts: 1980-1998" *Criminology and Public Policy*, 1(3) (2002): 311 – 338.

Smith, B., K. Damphousse, S. Yang, and C. Ginther. "Prosecuting Politically Motivated Offenders: The Impact of the 'Terrorist' Label on Criminal Case Outcomes" *International Journal of Contemporary Sociology*, 42(2) (2005): 210 – 216.

Toope, S.J. "Fallout from '9-11': Will a Security Culture Undermine Human Rights?" *Saskatchewan Law Review*, 65 (2002): 281 – 298.

Turk, A. *Political Criminality: The Defiance and Defense of Authority*. Newbury Park, CA: Sage, 1982.

Walker, C. "Terrorism and Criminal Justice: Past, Present and Future" *Criminal Law Review*, (2004): 311-327.

Warnes, R. and G. Hannah. "Meeting the Challenge of Extremist and Radicalized Prisoners: The Experiences of the United Kingdom and Spain" *Policing: A Journal of Policy and Practice*, 2(4) (2008): 402-411.

000695

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Welch, M. "Ironies of Social Control and the Criminalization of Immigrants" *Crime, Law & Social Change*, 39 (2003): 319-337.

Wilke, C. "*War v. Justice*: Terrorism Cases, Enemy Combatants, and Political Justice in U.S. Courts" *Politics & Society*, 33(4) (2005): 637-669.

Wilkinson, P. "Pathways Out of Terrorism for Democratic Societies" in P. Wilkinson and A. Stewart (eds.) *Contemporary Research on Terrorism*. Aberdeen: Aberdeen University Press, 1987.

Wither, J. "The United Kingdom's Campaign Against Radicalization" Paper presented to the Conference on Countering Ideological Support for Terrorism: International, Theological and Interdisciplinary Perspectives" September 2006.

Zedner, L. "Securing Liberty in the Face of Terror: Reflections from Criminal Justice" *Journal of Law and Society*, 32(4) (2005): 507-533.

SECRET

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Ramification of Terrorist Trials In Canada

by

Dr. Rachad Antonius

of the
Université du Québec à Montréal,
Chaire de recherche en immigration, ethnicité et citoyenneté

with the collaboration of

Charles Dufresne

A discussion paper presented to the

Department of Justice Canada

The views expressed in this report are those of the authors and do not necessarily represent the views of the Department of Justice Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CONTENTS

Abstract ii

Executive summary iii

Key Findings iii

1. The perception of terrorism trials 1

1.1 Introduction 1

1.2 Methodology 1

1.2.1 Who do these associations represent ? 2

1.3 A case study : the Toronto 18 case 3

1.4 The perception of terrorism trials and of the security agenda 6

1.4.1 Issues of concern among Arab and Muslim communities 6

1.4.2 Interpretation and analysis of the comments we found 6

1.4.2.1 There are few detailed comments on the specifics of terrorism trials 6

1.4.2.2 The importance of the broader security agenda 7

1.4.2.3 The even greater importance of the broader political agenda 8

1.4.2.4 The importance of legislation 9

2. Radicalization and measures to address it 10

2.1 Impact on radicalization/de-radicalization 10

2.2 Strategies contributing to de-radicalization 11

000698

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ABSTRACT

This papers answers the question :

1. How have terrorism trials in Canada and abroad been received in Canadian communities that share an identity with the terrorist?
2. How do terrorism trials impact on the radicalization efforts of violent extremists and on the de-radicalization efforts of communities and governments?
3. Can public legal education, changes in legal procedure, funding for courts, or differing media strategies influence any of the impacts outlined in the proceeding two questions?

We conducted a broad survey of reactions to terrorism trials in community papers and on the websites of the associations of the communities concerned, and made use of previous interviews and discussions on this topic with community leaders. We focused on the Arab and Muslim communities. We also relied on our extensive familiarity with the debates within these communities to propose our own perspectives on the issues discussed.

The main conclusion is that while the security and political agendas that are dominant now may contribute to radicalization, because of the marginalization of some communities that result from these agendas, a fair judicial system may counteract the sense of exclusion and marginalization in these communities, and thus contribute to a de-radicalization process. The present system is not quite fair, because of the legislation introduced as part of the dominant security paradigm, that may be eroding the rights of some citizens. Some recommendations are proposed in answer to the third question.

000699

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

EXECUTIVE SUMMARY

We conducted a broad survey of reactions to terrorism trials in community papers and on the websites of the associations of the communities concerned, and made use of previous interviews and discussions on this topic with community leaders. We focused on the Arab and Muslim communities, and made use of our insights, that result from an intimate knowledge of the debates within these communities. We analyzed the Toronto 18 case as an example of what is wrong in the system, relying on opinions that are well argumented and widely held in the communities concerned. We also reported on the issues that are discussed within these communities, and that have to do with the way terrorism-related matters are handled at the level of security and at the level of Justice. The analysis below reflects how terrorism-related issues have been received by the concerned communities, rather than our own assessment of terrorism trials.

Key Findings

We started with a case study in order to ground the general remarks that follow. The Toronto 18 case presents all the symptoms of a system that is risking of loosing its credibility in the eyes of rights-oriented advocacy groups and individuals, and in the eyes of the Muslim and Arab communities. Many associations have increasingly and consistently expressed the feeling that this was a fabricated crisis, in which some misguided youth were led by CSIS informants into doing things they would never have sought of doing by themselves. Basically, the positions taken by these associations are characterized by mistrust.

The fundamental issues raised by these analyses are the following. 1. The theatrical announcement of the arrests, which contributed to the propagation of a stereotyped image of Muslims. 2. The role of the informants. They were people with problems (drugs and money), their testimony was unreliable, and they acted more like *agents provocateurs*, than informants. 3. The process itself was problematic because of the conditions of detention of the suspects, because of the lack of credibility of the witnesses, and because of the abrupt interruption of preliminary hearings. In may respects, the case looks like a fabricated case where young men were pushed into criminal activities by moles that went far beyond their role.

The following issues were raised in the documents we consulted.

1.Trials (Terrorist trials verdicts, "Toronto 18", Operation Thread, Maher Arar & "Syria 4", Adil Charkaoui, Abousefian Abdelrazik). **2. Background** (Canada's human rights reputation, Canadian human rights legislation, Rise of islamophobia, Ethnic profiling, Profiling at borders, No-fly lists profiling, Immigration legislation). **3. Canadian government foreign policy** (Influences by foreign governments, Influences by diasporas in Canada, Conservative government foreign policy, Government foreign policy statements). **4. Antiterrorist legislation** (Antiterrorist legislation, Antiterrorist legislation safeguards). **5. Security and police investigations** ("Culture of impunity" in security, Cooperation with foreign security agencies, CSIS practices, CSIS visits, RCMP antiterrorist activities, RCMP antiterrorist statements, Informers, Security certificates). **6. Arrests and detentions** (Bail terms, Arrests, Treatment of inmates, Judicial due process, Civil rights and judicial laws and rules). Illustrations of statements concerning these issues can be made available in an annex, but are too voluminous to be part of this report.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The conclusions that emerge from the material examined are the following : 1. There are few detailed comments on the specifics of terrorism trials on the part of Muslim and Arab associations. The tendency is to denounce racial profiling and unfair treatment. 2. The importance of the broader security agenda. It is the security agenda, rather that the judicial procedures as such, that is the main source of injustices. 3. The even greater importance of the broader political agenda. This agenda means that some political forces which are seen as legitimate in the Arab societies are treated like terrorist entities, in contrast with European countries which differentiate between the military and political/social wings of the political forces in question. Moreover, Canada's position on the Israeli-Palestinian conflict is seen as being unfair, and as being a factor behind the politicization of the security agenda. 4. The importance of legislation. Anti-terrorist legislation, and Security Certificates are seen as facilitating racial profiling and unjust treatment of some communities.

On the issue of radicalization, we believe that, while it may have roots in the political cultures of some societies, it results much more from the global injustices in the Middle East and is exacerbated by Western policies. It is a global phenomenon. It results from a sense of marginalization and injustice, and it is determined much more by the dominant political orientation than by the lack of outreach programs. Fair judicial processes in Canada could play a crucial role in countering the sense of marginalization, and therefore in diminishing radicalization. The case of the Arar Commission is a case in point.

Counterbalancing radicalization is not mainly a question of outreach. Outreach activities can be extremely productive when they are backed by a rights-based approach and by a fair system, free of racial profiling. Many voices in the legal community, especially among jurists in universities and in civil liberties associations believe this is not the case. They say that the delicate balance that must be attained between security and rights has been tilted in favor of security. They assert that a rights-based approach has a stronger potential for guaranteeing security at the long run, by its potential to win the hearts and minds of the communities where radicalization takes place.

Public legal education is certainly helpful, in order to explain the safeguards for fundamental liberties found in the present legislation. The new security legislation has introduced changes in legal procedures that are strongly criticized. Changes must be made to return to the procedures that were in place before the security paradigm became dominant.

Funding for courts is addressed with a word of caution. Recognizing the right to be different should not mean that people should be subjected to different rights. The other caution is that training activities on Arab or Islamic cultures should not be the responsibility of institutions that are in conflict with these cultures. As for media strategies, we would say that the over-mediatization of arrests and of security procedures, given the present state of the media, plays a very negative role and it reinforces the feeling of alienation among Arab and Muslims. This feeling of alienation and marginalization is a main factor of radicalization.

We also make a recommendation of outreach activities by the Department of Justice (rather than the security agencies), focused on the specific work of the DoJ. In spite of some of the difficulties involved, we believe that the legal education that will result is well worth the effort and that it could play an important role in countering radicalization.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

1. THE PERCEPTION OF TERRORISM TRIALS

1.1 Introduction

This discussion paper aims at answering the following questions:

1. How have terrorism trials in Canada and abroad been received in Canadian communities that share an identity with the terrorist?
2. How do terrorism trials impact on the radicalization efforts of violent extremists and on the de-radicalization efforts of communities and governments?
3. Can public legal education, changes in legal procedure, funding for courts, or differing media strategies influence any of the impacts outlined in the proceeding two questions?

1.2 Methodology

For this paper, we conducted a broad survey of reactions to terrorism trials in community papers and on the websites of the associations of the communities concerned, and made use of previous interviews and discussions on this topic with community leaders. We focused on the Arab and Muslim communities. We surveyed the materials on the Web sites of eight Arab/Muslims associations and periodicals covering a period of up to six years (2003-2009). The Muslim associations surveyed are the Canadian Council on American Islamic Relations (CAN-CAIR), the Canadian Islamic Congress (CIC), the Canadian Muslim Union (CMU), the Muslim Canadian Congress (MCC). Two Arab associations were surveyed : the Canadian Arab Federation (CAF), and the National Council On Canada-Arab Relations (NCCAR). We also looked at two community periodicals that express perspectives emanating from the Maghrebi community in Montreal, Atlas Medias Montreal, and Maghreb Canada, which are published in French. We also consulted some academic works on the 'war on terror'. The analysis below reflects, then, how terrorism-related issues have been received among these associations, rather than our own assessment of terrorism trials.

In the case of associations, the material surveyed consisted of articles by board members, association members or outside researchers, open letters and petitions to government officials, news releases (excluding releases pertaining to association activities), articles from mainstream news media, reproduced on the associations' websites, presenting facts and analyses related to our topic. The assumption here was the associations were in agreement with the broad views presented in these articles. In the case of periodicals, we looked at the articles by journalists or outside researchers that were promoted as representing the points of view of the association. We also consulted some websites devoted to a particular issue (for instance the Toronto 18 or the Charkaoui case). We also referred to intensive interviews, both formal and informal, we had in our previous research, with leaders in the Arab and Muslim communities.

All in all, over two thousand items were accessed on the selected Web sites. Of these, more than one hundred were directly related to the object of this study. We found relatively little material on

000702

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the terrorism trials *per se*, but a lot more on the security agenda more generally, a fact that is significant from our analytical point of view, as explained further down.

Part of the perspective presented below is our own perspective, developed to link all the partial information we had and to develop a coherent view of the issues involved.

1.2.1 Who do these associations represent ?

Since we are talking about Arab and Muslim communities, it is useful to remember that although there is a very strong link between Islamic and Arab identities, the two should not be confused. Even if, globally, the very vast majority of Arabs are Muslims (85 % approximately), only 20 % of Muslims are Arabs. The proportion of non-Muslims among Arabs is greater in Canada than in the Arab world, as the first wave of Arab migration to Canada was made of Christian Arabs. The latter are also affected by Canadian security policies, but to a lesser degree than Arab Muslims. Their organized leadership tends to be less oppositional concerning the security agenda, and less critical of Canadian foreign policy. Finally, there is a deep ideological and political debate, among Muslim Arabs, about whether they should identify primarily as Muslims or primarily as Arabs. Although secular political trends retain some strength in Arab societies and Arab diasporas, they are less visible than Arab Islamic political trends.

The vast majority of community associations are not very vocal on political issues : they tend to be oriented towards social or religious activities. When they do take a stand on political issues, this is done in very general terms rather than on specific policy issues. This is even more true on the issue of terrorism and political violence, which is seen as being a delicate issue that can get people into trouble. This dominant attitude has been transposed from the countries of origin, where it reflected, partly, a fear of political repression, that has been transformed into a political culture by virtue of which it is more desirable not to get involved politically, and to leave politics to activists. The silent majority, however, may tacitly support a given political orientation, even if it does not get involved directly.

The sources we have chosen reflect, in our opinion, a majority orientation *among community activists* in the Arab and Muslim communities. They are the one who speak up on the issues of concern to this report, and they provide, in some cases, articulate analyses and opinions. In this respect, they all have some degree of legitimacy among the communities involved. The vast majority of Arab and Muslim citizens feel strongly that racial profiling may affect them, and they may be critical of security policies, but they would not get involved politically to challenge such policies. Therefore, focusing on the groups we have chosen gives us a good picture of the range of opinions found, but the assessment of the relative popularity of each of the various trends will remain a guess, but a well-informed guess.

To be a little more specific, so as to allow for a better interpretation of our findings, we would like to point out that neither the Arab nor Muslim communities in Canada have one single, representative national umbrella organization uniting most of them on a common platform. Nothing comparable, for instance, to the Canadian Jewish Congress. Therefore, Arab or Muslim communities in Canada do not speak with one voice.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

However, there is a near-consensus on some issues: the first is that they oppose terrorism and religious or state violence, but they consider some political forces to be liberation movements rather than terrorist organizations, even if they may be critical of some of the policies of such movements, and of the way these movements resort to political violence. Most of them also feel that Canadian Arabs and Muslims are a minority subject to discrimination and harassment, and that the Canadian security agenda is applied in a way that is unfair to Arabs and Muslims. There is also a majority opinion to the effect that Canada has adopted foreign policy positions that lack neutrality or that are hostile to Arab and Muslim political interests on the international scene. A very small minority trend supports Canadian positions on political issues concerning the Middle-East.

We must also point out to the political and ideological diversity within Arab and Muslim communities, in addition to ethnic and religious diversity. For instance, the members of the Canadian Islamic Congress (CIC) devote an important part of their activities on questions relating to religious practices, while these questions are totally alien to other organizations. The Muslim Canadian Congress (MCC), for instance, advocates 'the separation of religion and state in all matters of public policy', and it considers that the CIC is a fundamentalist organization that should be denounced. Few, in the Arab and Muslim communities, would agree with the MCC on this last assessment, although many would agree that the CIC is a conservative, religiously-oriented organization, with a leadership that is outspoken on political issues. While the MCC used to be an important voice in alerting the Muslim community to the dangers of fundamentalism, it has lost some of its credibility in the eyes of many Muslims and Arabs because of its lack of nuance in its criticism.

Some organizations (CAN-CAIR, CIC, CAF) follow closely a number cases that they consider to be human rights cases, and they monitor lapses in judicial due processes, or the activities of CSIS or the RCMP. Other organizations, and the MCC in particular, are practically silent on these matters or only refer to them in very general terms. The MCC is explicit in its support of the repression of fundamentalism, and it is very supportive of efforts in this direction. Some of these differences have probably as much to do with the objectives and ideological orientation of each association as with their resources (or lack of), enabling them to follow various dossiers.

1.3 A case study : the Toronto 18 case

The Toronto 18 case presents all the symptoms of a system that is loosing credibility in the eyes of rights-oriented advocacy groups and individuals, and in the eyes of the Muslim and Arab communities. Many associations (except the MCC) have increasingly and consistently expressed the feeling that this was a fabricated crisis, in which some misguided youth were led by CSIS informants into doing things they would never have sought of doing by themselves. Basically, the positions taken by these associations are characterized by mistrust.

In his chapter in *Law and Liberty in the War on Terror* (Andrew Lynch, Edwina MacDonald, and George Williams, Eds., The Federation Press, 2007) , Ben Saul discusses the question of motive in the definition of terror, and remarks that "There are, however, no bright lines in the debate between human rights advocates on one side and national security types on the other." (p.29).This cleavage goes much further than the definition of motives, and it includes the overall assessment of the security agenda and its implementation.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

We will refer particularly to two analyses : that of Professor Michael Keefer (University of Guelph), titled : *The Toronto 18 Frame-up : Fraud and Fear-Mongering in the 'War on Terror'* (www.globaloutlook.ca) and the latest book of Professor Shereen Razack (Ontario Institute for Studies in Education), *Casting out : The Eviction of Muslims from Western Law & Politics* (U. of Toronto Press, 2008). Both provide well-documented, and well-articulated analyses of what is wrong with the security paradigm of the Canadian state. One may disagree with some of the generalizations made in the first paper, but the evidence is there, and it would be difficult to brush it aside.

The fundamental issues raised by these analyses are the following.

1. The theatrical announcement of the arrests. The ceremony to announce the arrest was impressive (I happened to comment on it live, from the Toronto Studios of CBC, on the Saturday following the arrests). All the chiefs of intelligence and police services were there, and they solemnly announced that they had uncovered a major plot that threatened Canada, its parliamentary system, and its Prime Minister. The fact that they were ready to move right away to prosecute the suspects contrasted with the Security Certificates cases, and cast more credibility on the arrests. In the following days, the suspects, many of whom were in their teens, were brought to the Brampton court in shackles, with fully equipped snipers on the roof and helicopters flying above the court house. In retrospect, now that we know the role of the two informants, and the quality of the evidence, it is clear that the intelligence gathered by the security services did not justify this theatrical staging.

2. The role of the informants. Two aspects of their role stand out : the informants were people with problems (drugs in one case, money in both) whose testimony was unreliable. The other aspect that stands out is that the informants went far beyond their role of informants and acted more like *agents provocateurs*, providing ideas, tools and financial means to a bunch of misguided youth. It now appears that the suspects had, by themselves, neither the expertise, nor the tools, and probably not even the ideas to do what they were accused of doing. All these were graciously provided by the informants. The following quote by Professor Keefer reflects a feeling that is widely shared not only by the Muslim and Arab communities, but also by a much broader sector of the rest of the Canadian public that is concerned about civil liberties : 'Without the work of Mubin Shaikh, it's arguable that nothing that could plausibly be identified as a "Toronto 18" group would have existed; and it seems clear that only the entrepreneurial intervention of the second mole made it possible to claim that members of the group were seriously planning acts of terrorism'. However, on March 24, 2009, Ontario Superior Court Justice John Sproat upheld the guilty verdict of one of the youth, saying that the process was not one of entrapment. In addition, even if it had been a situation of entrapment, it should be said that these youths had the readiness to be led by the informants, which raises the issue of radicalization that will be discussed below.

3. The process itself. The conditions of detention of the suspects, in the early weeks of their detention and may be later, seem to be unacceptable : they seem to have undergone sleep deprivation[1]. The fact that many allegations were dropped also shows that these allegations were not supported by reliable evidence. CSIS (and may be also the prosecution) probably knew that the

[1] We have not checked this information from independent sources, and we mention it with caution.

000705

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

evidence was not strong, since they had hired the informants. The abrupt halting of the preliminary hearing before Shaikh's testimony could be cross-examined is also a problem from the point of view of guaranteeing a fair trial. Finally, the staying of charges against four of the adult suspects, including the suspected ring leader, in April 2008, is extremely significant and shows that the case may be collapsing. The guilty verdict against of one of the youth has also been received critically, for even if the young man did behave in ways that constitute criminal offenses because of their intent, he was pushed to do it by the informants. The role of the informants makes it impossible to know with a minimal degree of confidence whether there were criminal intentions other than the ones proposed and facilitated by the informants.

4. The interpretation of the trial. If the case is so weak, or even manufactured and framed-up as some observers believe, why did CSIS pursue it in the first place and why did it stage such a theatrical performance ? In retrospect, given the information we now have, this 'security show' seems even more grotesque. This is indeed puzzling because, from our experience in the various advisory committees we participated in, many individuals and some of the leadership in the security apparatus do not seem to be prejudiced at the individual level. But a system can be prejudiced by the implicit assumptions and representations that are at its core, and by the broad political agenda that presides over it. This is the line we want to reflect on.

We can propose three possible levels of explanation. One is found at the level of representations, i.e. the set of implicit conceptions of the 'Muslim Other' that presides over our interpretation of empirical observations. Media representations play an important role there, but also some of the academic work that is done about Muslims, in particular in the networks of security studies, also reflects this prejudice. In other words, it is a prejudice that is shared by an important part of the decision-making political elite, which sees everything related to terrorism from within a prejudiced framework. The analyses of Shereen Razack mentioned above, specially in her first chapter, are helpful to see through the intertwined set of ideas and empirical data that relate to this issue. Another level is that of the political agenda. The desire to cast Muslims as a danger in order to serve some foreign policy objectives is not to be discounted. This paper is not the appropriate place to conduct a critical analysis of Canadian foreign policy in the Middle-East, but it is certainly a very relevant aspect of the issues we are discussing. The necessity to justify by all means the 'war on terror', the Canadian presence in Afghanistan, the American war occupation of Iraq are part of the political background that frames the dominant views of issues related to the danger of Islamic terrorism. The signing of a *Declaration of Intent to enhance cooperation in the area of public safety* between Canada and Israel in March 2008 is one indication that Canada sees security issues that relate to the Middle East largely from an Israeli perspective. This, in spite of the fact that on the Department of Foreign Affairs website, Israel is clearly identified as an occupying power, that the Fourth Geneva Convention of 1949 applies in the territories occupied by Israel in 1967, and that some of the Israeli actions are contrary to the Geneva Convention. A third set of explanations can be found at the level of the immediate interests served by such arrests, but we cannot speculate on such interests. It is important to say that it is the partial collapse of the case that leads us to search explanations. If there was a real danger of the magnitude that was portrayed in the media, on the basis of the behavior of the security apparatus, these questions would be less relevant.

000706

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

1.4 The perception of terrorism trials and of the security agenda

We have found no comprehensive study on terrorism trials in general, or on that terrorism trial in particular (the Toronto 18 case) on the websites of Arab and Muslim associations. However, we found a lot of partial remarks that allow us to draw some conclusions.

1.4.1 Issues of concern among Arab and Muslim communities

The following issues were raised in the documents we consulted. We organized them in the following categories:

1.Trials (Terrorist trials verdicts, "Toronto 18", Operation Thread, Maher Arar & "Syria 4", Adil Charkaoui, Abousefian Abdelrazik).

2. Background (Canada's human rights reputation, Canadian human rights legislation, Rise of islamophobia, Ethnic profiling, Profiling at borders, No-fly lists profiling, Immigration legislation).

3. Canadian government foreign policy (Influences by foreign governments, Influences by diasporas in Canada, Conservative government foreign policy, Government foreign policy statements).

4. Antiterrorist legislation (Antiterrorist legislation, Antiterrorist legislation safeguards).

5. Security and police investigations ("Culture of impunity" in security, Cooperation with foreign security agencies, CSIS practices, CSIS visits, RCMP antiterrorist activities, RCMP antiterrorist statements, Informers, Security certificates).

6. Arrests and detentions (Bail terms, Arrests, Treatment of inmates, Judicial due process, Civil rights and judicial laws and rules).

On each of these issues, we have compiled illustrations of opinions found in the sources consulted, but their volume makes it difficult to include them in this report. We could provide them as an annexed separate document if this is desired.

1.4.2 Interpretation and analysis of the comments we found

We propose the following general conclusions from our investigation, and propose our interpretation of what they actually tell us.

1.4.2.1 There are few detailed comments on the specifics of terrorism trials

Terrorism trials as such have not received a lot of comments on the web sites of community associations and newspapers. Detailed positioning on trials such as those of the Toronto 18, for instance, have rather been found on dedicated websites expressing the views of specialized advocacy groups, and generally written by academics. For community associations, it is the security agenda in general that has been receiving all the comments that concern terrorism. This

000707

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

may be due to several broad reasons:

a. Several cases where terrorism was an issue were not treated within the criminal code or within antiterrorist legislation. The Security certificates provide an illustration of this state of affairs, as they are treated within immigration law.
b. On issues of terrorism, Arab and Muslim associations tend to get involved only to the extent they feel the treatment of the case is unfair, and their demands are usually that due legal process should be followed. We have found no comments, for instance, on the Ahmed Rassam case. Most understand that terrorism is a serious matter and that the existence of *real* terrorism cases that are linked to the community would be devastating. But they are worried that some cases will be treated like terrorism cases without sufficient evidence, and that some political forces in the Muslim or Arab countries are designated as 'terrorist' and criminalized for political reasons rather than on the basis of objective criteria.
c. These worries are reinforced by the existence of cases where racial profiling, rather than hard evidence, was at the origin of the case. Most Arab, Muslim, or other observers 'read' this situation as a manifestation of negative stereotypes and sometimes as a political choice. As a consequence all cases where hard evidence is not presented within a reasonable amount of time, are considered to be cases of racial profiling. Reference to the principle 'innocent until proven guilty' is often at the basis of their advocacy work, and they sometimes lament that when it comes to Muslim suspects, the working principle seems to be 'guilty until proven innocent'. When community associations express their concerns, it is precisely because the case has not been subjected to the usual legal norms: accusations are not filed, or else the evidence is not made available to the defendant, thus not permitting a fair trial.
d. The advocacy work of community associations tends to be situated in a broader context, as they associate with (non-ethnic) civil liberty associations and dedicated advocacy groups.
e. As a result, the detailed analyses and positioning with respect to the specifics of a given trial as such (discussions of the judicial process, of the arguments of the prosecutors and the defense) are usually done within these specialized advocacy groups, which tend to transcend ethnic or religious boundaries. Arab and Muslim associations become in this situation members in larger coalitions that are not led by them. The arguments and criticisms presented by Arab and Muslim organizations are very close to those presented by these specialized advocacy groups.

1.4.2.2 The importance of the broader security agenda

One aspect of the positioning of Arab and Muslim associations is more fundamental than the others, and it has to do with the security agenda. By security agenda, we mean the legislation and all the measures that are justified by security concerns, that precede, accompany and follow the judicial procedures. The security agenda also includes the conceptual framework that frames such measures, their very justifications, and the way they are put into practice. In studying the discourse of Arab and Muslim associations, we have indentified a number of the measures they criticize, listed further down.

What it is seen to be problematic, then, is the security agenda much more than the legal procedures of terrorism trials as such. It is when the security agenda justifies a departure from normal judicial proceedings that a sense of injustice is felt. For instance, surveillance and intelligence gathering

000708

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

activities (interrogation of imams or of activists, sometimes at their workplace; longer interrogations at the borders for people believed to be Arabs or Muslims; etc.) are perceived as fundamental breaches of human rights when they are done without sufficient reasons that are based on evidence. They are then seen as a form of racial profiling, that derive from a hostility to Arab culture or to Islam, or at best from ignorance. As a consequence, the arrests of certain individuals without due process is seen as a manifestation of racial profiling. The issue of islamophobia comes out again and again as an important factor behind racial profiling in most discourses emanating from Arab or Muslim groups on the security agenda. Islamophobia in this case is seen not just as the result of a lack of knowledge about Islam, but as the result of political lobbying aimed at de-legitimizing political struggles that refer to Islam as a political idiom or as a political ideology.

This situation is more problematic than it seems, because it gives rise to unjustified fears by Muslims and Arabs. In the presence of some cases of racial profiling (the Arar case being highly mediated), every case where the proof is incomplete is seen as a case of racial profiling, and it is attributed to islamophobia. Even when there are good reasons to suspect someone, they are not taken seriously by Arab and Muslim organizations as long as a full proof of guilt has not been given, and they insist that the principle 'innocent until proven guilty' should not be reversed to 'guilty until proven innocent' when it comes to Muslim suspects.

1.4.2.3 The even greater importance of the broader political agenda

In the eyes of most Muslim and Arab associations, the political agenda that is behind the security agenda is also seen as problematic, and as more important than the latter. It is the political agenda that explains and justifies why some groups and some activities as framed as 'terrorist'. On this point, Canada differs from several European countries that distinguish between the social and political wings of some groups such as Hezbollah on one hand, and their military wings on the other hand. Most European countries do not criminalize the social and political branches of Hezbollah, whereas Canada does. For many associations and observers, it is the political agenda that explains why the security agenda is applied the way it is.

This issue vibrates differently in the case of Arab and Muslim associations on one hand, *versus* associations related to other communities such as the Sikh or Tamil communities. This is because of the Israeli-Palestinian conflict is a 'local' issue in Canada, as one of the sides is much closer to the hearts and minds of the Canadian political and intellectual elite. From the point of view of Muslims and Arabs, the Canadian government is seen as having played a negative role that is not in line with its international legal obligations (see Antonius, R., 2002 : *The Relevance of the Principles of International Law to the Resolution of the Israeli-Palestinian Conflict*, available on www.ieim.uqam.ca/spip.php?mot14&debut_archive=150). This issue is and will remain a contentious issue as long as international law will remain ignored in the search for a just and peaceful political settlement in Israel-Palestine. Our remarks on this point concern the security agenda as it applies to individuals or groups involved in Middle-Eastern politics.

The desire to harmonize Canadian and US policies, both for reasons of ideological and political proximity and for reasons of commercial interests, is also seen as a factor determining the political agenda, especially in its security dimension. The US security agenda is perceived in very negative terms in the Arab and Muslim community. The popularity of books that are critical of the Global

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

War on Terror is significant. Let us mention for instance *Good Muslim, Bad Muslim: America, the Cold War, and the Roots of Terror* (New York, Pantheon Books, 2004), by Columbia University professor Mamdouh Mamdani, *The War on Error: Real Stories of American Muslims* (Fayetteville, University of Arkansas Press, 2007), by Melody Moezzi, etc. These books are quite serious and do not fall in the genre of *conspiracy theories*. Some other books raise questions concerning the failure of the security apparatus in the US and the incoherence and contradictions of the official answers, but fall short of asserting that the crisis was fabricated by the US. Such is *The War on Truth; 9/11, Disinformation and the Anatomy of Terrorism* (Northampton, MA, Interlink Publishing Group, 2005) by Nafeez Mosaddeq Ahmed. Others, finally, clearly fall in the trap of conspiracy theories. We mention this because these books have a large audience among Arabs and Muslims, who tend to adopt a critical attitude towards the political agenda that informs Canadian and American Middle East policies. This attitude is reinforced by cases where Muslim suspects are considered guilty before the proof is properly established, and this situation makes Muslim and Arabs vulnerable to conspiracy theories, because they tend not to trust official explanations and justifications when it comes to the Middle East. This then becomes the framework within which many of them evaluate security policies in Canada.

Based on our familiarity with the political opinions in the Arab and Muslim communities, our feeling is that the dominant assessment of the Barak Obama administration is cautiously critical, as changes towards the Middle East as seen to be more cosmetic than real. This remains to be seen.

1.4.2.4 The importance of legislation

Serious criticism has been addressed to the way the security agenda was translated into legislation. This criticism was centered around two issues : The Security Certificates, and the Anti-terrorism legislation. Arab and Muslim organizations have pointed out that this legislation is unfair as it opens the door to arbitrariness, but detailed criticism has come essentially from the community of jurists in universities and in civil liberty associations.

As this report is addressed to the Department of Justice, we feel that the technical aspects of this legislation and the problems they raise have been discussed at length elsewhere, they are known by the readers of the report, and they are beyond the competence of the author of this report. We will simply point to the work of respected jurists such as Kent Roach, François Crépeau, Peter Leuprecht, Warren Allemand and others. We just want to say that these critical analyses are discussed within intellectual and political circles in the Arab and Muslim communities. They confirm a deep feeling, shared by many in these communities, that this legislation opens the door to racial profiling and unfair treatment. This is why the dominant political and security paradigms are so important : they explain not only the legislation itself but also they shed light on the problems that arise from putting this legislation into practice.

000710

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

2. RADICALIZATION AND MEASURES TO ADDRESS IT

2.1 Impact on radicalization/de-radicalization

We will accept, for this discussion, the following definition of radicalization :

> Radicalization is a process, not an end unto itself, and it does not necessarily lead to violence. After all, ever political spectrum by definition has its own 'extremes'. (*Radicalization, violence, and the Power of Networks*, A summary of the ideas presented at the Global Futures Forum Conference in Brussels, October 2-4, 2006)

This definition says implicitly that radicalization is the process that gets individuals and groups to move to the extreme of a political spectrum, an extreme that means that the political ends they pursue are taken as absolute, often justifying extreme means to attain these ends, thus paving the way for the use of violence. A preventive approach leads us to think that one way to avoid political violence is to avoid radicalization as one of its facilitating factors. We understand that this is the meaning of radicalization that is of concern to the Department of Justice Canada.

Radicalization/de-radicalization is a multi-level process which depends on many factors. At the global level, the most important one is the foreign policies of Western states, including Canada, that support injustices in Arab and Muslim societies. This factor cannot be addressed by goodwill and expert legal opinions : these are widely available, but it is a question of balance of power. A moving testimony of this state of affairs is provided by the recent book : *Warum Tötest Du, Zaid ?* (Why do you kill, Zaid ?) by Jürgen Todenhöfer (Munich, C. Bertelsmann, 2008), where the author explains the journey of a young Iraqi from an anti-war attitude and a positive evaluation, at first, of American intervention, to a situation where he joins the Iraqi violent resistance against the American occupation of Iraq (a resistance which is quite different and opposed politically to the terrorist Al Qaeda networks in Iraq). The story of Zaid is an emblematic illustration of a radicalization process. The situation in Afghanistan and in Palestine are other examples where Western policies promote radicalization. In the case of Palestine, Western systematic opposition to the application of international law to resolve the conflict peacefully and on a just basis is a major cause of radicalization at the global level.

However, in order for this sense of injustice to be translated into radicalization and eventually into political violence, some ideological conditions must exist. The rise of political Islam, at the global level, is one such condition, and the factors leading to its growing importance cannot be reduced to foreign intervention, even if it is facilitated by it. We believe that radicalization at the Canadian national level is a reflection of this global radicalization.

The way terrorist or terrorism-related trials are handled may work towards reducing radicalization efforts in more than a marginal way : by ensuring that the rule of law is applied, that fair trials are conducted and that the outcome of the trials are the result of objective and universally applied principles rather than racial profiling, a very strong message is sent to the candidates for

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

radicalization, that Western normative and legal systems cannot be reduced to strategic interests in the Middle-East.

In other words, the current dominant political and security agendas can do little to reduce radicalization because they do not address the fundamental causes of radicalization. In a way they contribute to the radicalization process. However, the judicial sphere can play a major role in reducing radicalization, if it succeeds in sending the message that this is a country where civil and political rights, and more generally all human rights, are protected. For instance, the way the Arar case was handled by the Arar Commission played a major role, in our opinion, in sending this strong message, thus contributing to a sense that this is a fair country. We believe that the contribution of the Arar Commission to de-radicalization is enormous and it should not be underestimated. In contrast, the Toronto 18 case played a negative role because the legal procedures have been dominated – some would say hijacked – by the security agenda.

2.2 Strategies contributing to de-radicalization

The third question to be answered in this report is the following : Can public legal education, changes in legal procedure, funding for courts, or differing media strategies influence any of the impacts outlined in the proceeding two questions?

We want to submit the idea that counterbalancing radicalization is not only, or mainly, a question of outreach. Outreach activities can be extremely productive when they are backed by a rights-based approach and by a fair system, free of racial profiling. Focusing on outreach is implicitly based that we are doing the right thing, and it is now a matter of explaining it to the targeted public. But what if we were not doing the right thing ?

One pre-requisite to successful outreach activities is that the legislation be fair, and that its implementation be fair as well. Many voices in the legal community, especially among jurists in universities and in civil liberties associations believe this is not the case.

Therefore, the first thing to do in order to facilitate de-radicalization is to review the legal framework and to question the security agenda that informs it. Many voices in the legal community say that the difficult, and delicate, balance that must be attained between security and rights, has been tilted in favor of security. They assert that a rights-based approach has a stronger potential for guaranteeing security at the long run, by its potential to win the hearts and minds of the communities where radicalization takes place.

In spite of this word of caution, we believe that an outreach program about rights-based approaches to security, and about the legal processes used to deal with terrorism-related issues is absolutely important to counter radicalization. Such programs do exist, but they could certainly be enhanced and broadened.

The first effects of such a program can be seen in the fact that even those who criticize the security agenda, in the Muslim and Arab communities, do so using the language of rights, and promote it within their constituencies. This is a fundamental requirement of a rights-based culture, which is itself, to a great extent, an antidote to radicalization. Once a culture of human rights is internalized

000712

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

and promoted in a community, this gives cultural tools to the members of the community to resist processes of radicalization.

Public legal education is certainly helpful, in order to explain the safeguards for fundamental liberties found in the present legislation. But such education will also mean that some tough questions are asked, and that changes in present legislation be made. Concerning legal procedures, we would argue that the new security legislation has itself introduced changes that are strongly criticized. So, if changes are to be made, they must be made to return to the procedures that were in place before the security paradigm became dominant.

Concerning the funding for courts, we can speak of training sessions on intercultural competence, with a word of caution. Being open to other cultures should not be an excuse to essentialize them. Recognizing the right to be different should not mean that people should be subjected to different rights. Unfortunately there has been cases (not having anything to do with security) where courts have excused criminal behavior on account that it was culturally accepted in a community. The other caution we would like to make is more political, and admittedly delicate. Given the agreement between Canada and Israel on security matters, it would be very unfortunate if Israeli security services were called in to train Canadian security services about Arab or Islamic cultures. Given what is happening in the Middle East, this would only reinforce stereotypes and racial profiling.

As for media strategies, we would say that the over-mediatization of arrests and of security procedures, given the present state of the media, plays a very negative role and it reinforces the feeling of alienation among Arab and Muslims. This feeling of alienation and marginalization is a main factor of radicalization.

Our most important recommendation, however, is the following. Outreach activities by the Department of Justice, rather than the security agencies, should be conducted with the concerned communities, and if possible, on specific issues. We understand that it may be delicate to discuss the details of on-going trials. But it may be useful to conduct training sessions, for instance, on the judicial processes used in terrorism cases, explaining both the legislation, and the way it is implemented. Details of a specific case could be discussed to the extent they are already public, in order to bring into the discussion elements that have been overlooked in the public debate. For instance, many aspects of the security certificates cases are not brought up in the discourse of civil liberties associations, and we feel they are absolutely relevant.

We see three possible types of target audiences, and sessions with each of the three could be planned.

a) The community associations, in particular the ones that are involved in advocacy work.
b) Associations of lawyers from these communities, or even ad-hoc groups of lawyers from the concerned communities.
c) The various civil liberties associations and advocacy groups (which are not tied to a community in particular) which have acted on issues related to the security agenda or to terrorism (for instance, the *Ligue des droits et libertés* in Montréal).

Such training sessions could put to task the representatives of the DoJ, as the dialogue should be a two-way dialogue if it is done seriously. But be believe it is well worth the effort.

000713

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Extreme Expression and its Regulation

by

Professor Jamie Cameron

of
York University,
Osgoode Hall Law School

A discussion paper presented to the

Department of Justice Canada

The views expressed in this report are those of the authors and do not necessarily represent the views of the Department of Justice Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Executive Summary

This short discussion paper considers extreme expression in some of its settings: specifically, those of hate and discriminatory expression, hateful and defamatory religious expression, and terrorist expression. Its goal, in doing so, is to review and comment on existing provisions in Canadian law, as well as to consider measures which have been proposed or adopted elsewhere. It concludes that Canada's laws, as presently constructed, do not reveal troubling gaps in this area of regulation. Moreover, the consequences for expressive freedom – and constitutionality of doing so – would have to be carefully considered in the case of any extensions to the regulatory framework for extreme expression.

Disclosed

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

A framework for discussion

This short paper places difficult questions about whether, when, and how to regulate extreme expressive activity into a framework for discussion. Issues which are complex and difficult arise in a context of ongoing tension between freedom of expression and its permissible limits. As it is not possible to provide a comprehensive analysis within the project mandate of 3-6000 words, this paper proposes only to review and comment briefly on diverse regulatory options which have been adopted, in Canada and elsewhere, in response to extreme or extremist expression. The terms of reference for this project take the form of three questions:

1. How is terrorism similar or dissimilar to hate crimes? What are the legal and/or philosophical advantages or drawbacks of linking the two concepts?
2. What elements of Canada's anti-hate legislation can be used to counter violent extremists? Why, or why not, are each of the elements either not used or are seen as being more, or less, effective?
3. How do the debates over the utility of recent laws regarding freedom of expression and religious extremism in other countries (such as the UK) and internationally (such as at the UN) relate to the social and political reality we experience in Canada?[1]

These terms of reference flag questions about current Canadian law, but also signal a concern – or at least raise a query – about whether existing laws include or cover expressive activities that could or should be regulated. Of particular interest there are measures which address expression that targets religions, religious practices, and

---

[1] Department of Justice, Research and Statistics Division; Terms of Reference for a project titled, A Discussion of Freedom of Expression in the Context of Anti-Terrorism and Anti-Hate Crime Policy (January 2009). I would like to thank those from the Department of Justice, as well as my colleagues Professors Arthur Cockfield and Barbara Perry, who participated in the discussion session in Ottawa on March 17, 2009. I would also like to thank Rishi Hargovan, Osgoode Hall Law School LL.B. (2010) for providing research assistance on this project.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

members of religious groups, and expression that encourages, promotes, advocates, or glorifies terrorist activities.

Though readers will be familiar with the *Charter of Rights and Freedoms* (the "*Charter*"), a brief overview is provided, both to set the framework for discussion and to serve as a reminder that the *Charter* places limits on the government's authority to regulate expressive activity that do not constrain the actions of other states. Then, the three main sections of the paper, in order, consider extreme expression under the *Criminal Code* and *Canadian Human Rights Act*[2] (the "*CHRA*"), extreme religious expression (*i.e.*, defamation of religions, religious hatred, and religious vilification), and, finally, terrorist expression. In discussing the current criminal law and human rights legislation, the first part focuses on the relationship between hate expression and terrorist expression, and considers whether human rights legislation is an appropriate instrument for regulating expressive activity. The second part asks whether the absence of a law that is specific to extreme religious expression represents a gap in Canada's regulatory framework. A final section on terrorist expression looks briefly at anti-glorification laws and the internet as a tool for terrorist recruitment.

The paper's key points are then summarized in a conclusion which runs along the following lines: first, Canada's failure to adopt certain measures does not reveal a troubling gap in its response to extreme expression; and, second, measures which have been adopted or proposed elsewhere (*i.e.*, including at the UN) are of doubtful constitutionality under the *Charter*. In the absence of evidence to suggest that harmful

[2] R.S. 1985, c.H-6.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

expressive activities are currently unregulated the status quo, which consists of anti-terrorism and hate propaganda provisions, provides an adequate response to the problem of extreme expression in Canada at this point in time.[3]

Constitutional considerations

The *Charter* is necessarily the starting point in any discussion of restrictions on expressive freedom.[4] Such restrictions are constrained by the *Charter* and must satisfy a standard of justification under section 1's concept of reasonable limits. To that it should be added that the *Charter*, and section 2(b), distinguish Canada from other jurisdictions like the United Kingdom ("UK") and Australia, neither of which has an analogous system of constitutional rights, and both of which have adopted measures to deal with extreme activities that have intrusive consequences for expressive freedom.

For present purposes, it is sufficient to reference four principles which bear on the constitutionality of limits on expressive activity. First is the freedom principle, which proposes a broad, inclusive and egalitarian approach to section 2(b) and guarantees that "everyone can manifest their thoughts, opinions, beliefs, indeed all expressions of the heart and mind, however unpopular, distasteful or contrary to the mainstream".[5] This principle is reflected in *Irwin Toy*'s definition of expression as "any attempt to convey

---

[3] "Adequate", in this context, does not reflect my opinion of the current law but is instead a neutral or more objective description of the way existing provisions balance the competing interests in protecting expressive freedom and preventing harm.
[4] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11.
[5] *Irwin Toy Ltd. v. Quebec*, [1989] 1 S.C.R. 927 at 968.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

meaning".[6] In granting section 2(b) a generous interpretation the Supreme Court also indicated that there is an exception for "violent forms of expression",[7] but defined it narrowly as "expression communicated directly through physical harm".[8] Under that approach, which has consistently been followed in the jurisprudence, all expressive activity which attempts to convey meaning is *prima facie* protected by the *Charter*; it does not matter whether it is valuable or not, and nor is it relevant – for purposes of section 2(b) – that the activity may be harmful.

Freedom is not absolute under the *Charter*, and is subject to those reasonable limits that are demonstrably justified in a free and democratic society, under section 1. Second, then, is the harm principle, and its recognition that the state may prohibit or punish "harmful" expressive activities. How harm should be defined is not free from difficulty, especially where a causal connection between the activity in question and an identifiable harm cannot be established. Under one approach, which – at one end of the spectrum – would maximize the *Charter*'s protection of expressive freedom, a narrow conception requires evidence of particularized harm (*i.e.*, imminent violence, incitement, a concrete or empirical link between words and action) before expressive activity can be regulated. At the other end of the spectrum a broader conception avoids the risk that expressive activity might cause harm and allows the state to regulate, absent evidence of harm, and in circumstances where expressive activity may "harm" the community at

---

[6] *Ibid.* (also stating, at 969, that "if the activity conveys or attempts to convey a meaning, it has expressive content and *prima facie* falls within the scope of the guarantee").
[7] *Ibid.* at 970 (stating that "[w]hile the guarantee of free expression protects all content of expression, certainly violence as a form of expression receives no such protection").
[8] *R. v. Keegstra*, [1990] 3 S.C.R. 697 at 732.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

large, in generalized and indeterminate ways (*i.e.*, by desensitizing the community or promoting attitudinal change).

The third and fourth principles engage the concept of proportionality and are concerned with the manner of regulation.[9] Together, they ensure that any limit on constitutionally protected activity satisfies prescribed standards of proportionality. The third principle requires precision in the scope of the regulation to avoid unnecessary interference with expressive freedom. It focuses on the question of definition, including the breadth of the regulation and whether it catches protected activity, or more expressive activity than is necessary to meet the regulatory objective (*i.e.*, of preventing harm).[10] The fourth principle addresses proportionality through a form of "big picture" balancing, which asks whether the salutary benefits of a regulation outweigh its deleterious consequences for expressive freedom.[11] It is at this stage that concerns about self-censorship, and the chilling or silencing effects of prohibiting certain kinds of expression, are taken into account.

The Supreme Court of Canada has not consistently required direct or empirical evidence of harm in upholding a variety of provisions which prohibit and criminalize various forms of offensive expression (*i.e.*, hate propaganda, discriminatory expression, obscenity, defamatory libel, tobacco advertising, child pornography). Even so, section 2(b) places powerful constraints – ones which are political as well as legal in nature – on on the government's authority to interfere with expressive freedom. As the debate

---

[9] See *R. v. Oakes*, [1986] 1 S.C.R. 103 (creating the proportionality test under section 1 of the *Charter*).
[10] This part of the analysis references the minimal impairment requirement of the proportionality test.
[11] And this is the final element of the proportionality analysis.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

surrounding the anti-terrorism laws confirms, any extension of criminal prohibitions into the realm of political, religious, or ideological expression and belief is, and will be, controversial. Restrictions on certain types of expression (*i.e.*, religious expression) have been contentious in jurisdictions without constitutional guarantees, like the UK (which has human rights legislation that does not confer full constitutional authority on the judiciary) and Australia (which as yet has no bill of rights).

Extreme hate expression: the *Criminal Code* and the *CHRA*

In responding to provisions which prohibit extreme expression, the Court has upheld measures but at the same time defined the permissible scope of regulation with care, to avoid undue interference with expressive freedom. Almost twenty years ago the Court upheld the *Criminal Code*'s hate propaganda provision[12] as well as section 13 of the *CHRA*;[13] both times the result was determined by a margin of four votes to three. But it also invalidated the *Code*'s false news provision, in the context of Ernst Zundel's holocaust denial campaign,[14] and more recently re-iterated that the *Code*'s concern is with the problem of extreme expression and the intentional promotion of hatred.[15] This part of the paper has two objectives: one is to comment briefly on the relationship between hate expression and "terrorist expression"; the other is to discuss section 13 and its ongoing role in regulating discriminatory expressive activity.

Hate propaganda and terrorist expression

---

[12] *R. v. Keegstra* , *supra* note 8.
[13] *Canada (Human Rights Commission v. Taylor*, [1990] 3 S.C.R. 892.
[14] *R v. Zundel*, [1992] 2 S.C.R. 731.
[15] *Mugesera v. Canada*, [2005] 2 S.C.R. 91; see also the lower court ruling in *R. v. Ahenakew*, 2009 SKPC 10 (February 23, 2009).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To begin, it is worth noting that Canada's anti-terrorism laws target terrorist *activity* and not terrorist *expression*.[16] Anti-terrorist provisions which seek to prevent as well as to punish terrorism in Canada are based on a distinction between acts and omissions which are criminalized, and expressive activities, which are excluded from the scheme. Accordingly, this paper does not consider terrorist activities or the *Code*'s anti-terrorism provisions, but limits its discussion to the question of terrorist expression. Whereas hate propaganda has a statutory definition and is a recognized species of expressive activity, there is no statutory definition – or common understanding – of terrorist expression. The reason may be, in part, because terrorism is action-oriented and is identified, in particular instances, by its program of action. In considering that difference, this part of the paper suggests why hate propaganda provisions do not respond to the problem of terrorist expression (to the extent there is one). Later, the paper returns to the question in a section that discusses measures that target particular forms of terrorist expression.

The *Criminal Code*'s hate propaganda provision criminalizes expressive activity that targets an identifiable group in a way that willfully promotes hatred, and in circumstances which do not fall within any of the statutory defences.[17] In upholding the provision, the Supreme Court of Canada emphasized the elements that minimize the interference with expressive freedom: one is a requirement of intention on the part of the

---

[16] See section 83.01(1.1) of the *Criminal Code*, 2001, c.41, ss.4, 126(3), which states that the *expression* of a political, religious or ideological *thought, belief or opinion* does not come within the definition of a "terrorist activity" for purposes of the anti-terrorism legislation (emphasis added). See discussion *infra*, "Terrorist expression…"

[17] *Criminal Code*, section 319(2) (defining the offence), (3) (prescribing defences) , and 318(4) (defining "identifiable group" as "any section of the public distinguished by colour, race, religion, ethnic origin or sexual orientation") R.S.C. 1985, s.27 and S.C. 2004, c.14, s.1.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

speaker; a second is a definition of hatred that is narrow and focuses on the extreme nature of the expression; and a third is, again, an interpretation of "promoting hatred" which requires a high degree of blameworthiness on the part of the accused. The gravamen of the offence, then, is the hateful targeting of those who belong to a group that is identified by one of the statutory criteria.

Hate propaganda and terrorist expression might overlap in a way that would bring terrorist expressive activity into the terms of section 319. For instance, terrorists and terrorist organizations may target groups which are protected by the *Code*'s hate propaganda provisions (*i.e.*, when the object of the terrorism is an identifiable group). Though not described as such, the Ku Klux Klan might be thought of as "domestic terrorists" and, by the same token, hate propaganda might be found in the agenda of terrorist organizations engaged in campaigns which include race or ethnic hatred or cleansing. Despite the incidence of overlap in some cases, it should not be assumed that provisions that are designed to deal with the hateful targeting of identifiable groups can respond to the extreme expressive activities of terrorist organizations.

In this it is important to consider the harm in each instance, and to recognize that hate propaganda and terrorist expression may be harmful in different ways. In *R. v. Keegstra*, the Supreme Court of Canada held that hate propaganda is harmful for two reasons: first, members of the target community suffer direct harm when they are the objects of hatred; and second, the community at large also sustains harm in the form of a

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

risk that the hate monger's message might affect societal attitudes toward members of the target group.

Terrorist expression, by comparison, has the different goal of persuading its audience of the validity of a program of action, and even of seeking converts to the cause. At a minimum its objective is to generate sympathy or support and, in many cases, it serves more actively as a tool of recruitment. Though hate propaganda also seeks converts, terrorist expression is in a least some cases a call to action. Terrorist expression may be less harmful than hate propaganda when it merely solicits sympathy and support (*i.e*, this is the difference between the mere support of or agreement with terrorist causes and the willful promotion of hatred); at the same time it can be more insidious than hate propaganda (*i.e.*, when the activity is a call to action, a form of conscription by words).

This discussion is pursued again in the section below, which returns to the question of terrorist expression in the context of the UK's anti-encouragement offence. For the moment, the point is that it is awkward, both in concept and practice, to treat terrorist expression as though it is hate propaganda, or to view the hate propaganda provisions as an adequate substitute for a measure that defines and addresses terrorist expression (if, indeed, such a provision is necessary).

<u>Extreme discriminatory expression</u>

Generally, the purpose of human rights instruments – provincial as well as federal – is to address discriminatory practices in access to various services and opportunities

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(*i.e.*, housing, employment). In addition, many codes in Canada treat discriminatory expression as a human rights violation. Under section 13 of the *CHRA* it is a discriminatory practice to use the telephone or internet to communicate any matter that is "likely to expose a person or persons to hatred or contempt on the basis of any of the prohibited grounds of discrimination".[18] Recently, complaints initiated at four human rights commissions (Canada, Ontario, British Columbia, and Alberta) arose from two instances of alleged Islamophobia. One was an online version of Maclean's magazine which, on October 20, 2006, published an excerpt titled "The Future Belongs to Islam" from a book by Mark Steyn; the other concerned an article in the Western Standard magazine, which discussed and published the "Danish cartoons".[19]

Though the complaints failed, these and other proceedings prompted two questions: one is whether anti-discrimination human rights laws should continue to play a role in regulating expressive activity, and the other is whether modifications to human rights proceedings are called for at this point in time. The Canadian Human Rights Commission (the "CHRC") commissioned answers to these questions from Professor

---

[18] R.S. 1985, c.H-6. Under section 3(1) of the *CHRA*, the prohibited grounds of discrimination are race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability and conviction for which a pardon has been granted".

[19] Complaints were brought and adjudicated by human rights commissions in Ontario and at the federal level, as well as in Alberta and British Columbia. See Commission Statement Concerning Issues Raised by Complaints Against Maclean's Magazine, http://www.ohrc.on.ca/en/resources/news/macleans (Ontario Human Rights Commission statement issued on April 29, 2008, condemning media coverage that contributes to Islamophobia and promotes societal intolerance towards Muslim, Arab and South Asian Canadians). The other commission decisions are *Canadian Islamic Congress v. Rogers Media Inc.* (20071008); Canadian Human Rights Commission (June 25, 2008); *Edmonton Council of Muslim Communities v. JMCK Western Publishing Corp.* (S2006/05-042); Alberta Human Rights and Citizenship Commission (August 1, 2008); and *Elmasry and Habib v. Roger's Publishing and MacQueen (No. 4)* 2008 BCHRT 378 (October 10, 2008).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Richard Moon, whose report was released in October of 2008 (the "Moon Report").[20] He recommends the repeal of section 13 of the *CHRA* and, in the alternative, suggests substantial modifications to that provision.[21] In brief, Professor Moon maintains that any attempt to remove prejudicial and discriminatory expressive activity from public discourse would require extraordinary intervention by the state. He concludes that censorship is an ineffective and inappropriate response to expressive activities which stereotype or discriminate against those on the *CHRA*'s list of prohibited grounds of discrimination.

Professor Moon argues that the law should only regulate extreme expression which "threatens advocates or justifies violence against the members of an identifiable group".[22] Though he does not state precisely what he means by these terms, Moon's concern with extreme expression that is linked to violence proposes a conception of harm that is closer to incitement than *Keegstra*'s definition of harm.[23] In addition, he sees extreme expression (defined, in the *CHRA* in terms of hatred or contempt) as a matter which falls within the jurisdiction of the criminal justice system, and does not fit comfortably in the human rights code mandate of regulating discriminatory practices.[24] Alternatively, Professor Moon recommends modifications to the *CHRA* which would limit its focus to hate speech (*i.e.*, he proposes that the reference to "contempt" be

---

[20] Report to the Canadian Human Rights Commission Concerning Section 13 of the *Canadian Humans Rights Act* and the Regulation of Hate Speech on the Internet, by Professor Richard Moon (October 2008).
[21] *Ibid.* at 33-40.
[22] *Ibid.* at 1 (Summary of Recommendations).
[23] Whether the regulation of extreme expression should adopt a more speech-protective standard – under the *Criminal Code* as well as under any human rights legislation – is a question that cannot be adequately addressed within the scope of this paper.
[24] *Ibid.* at 28 (stating that a ban on hate speech may be seen as an extension of the criminal law prohibition on the advocacy and threat of violence which is justifiable to prevent the risk of violence against members of an identifiable group).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

removed from section 13), add a requirement of intention (*i.e.*, he would target expression which threatens, advocates, or justifies violent action against members of a group) and thereby limit section 13's application to the most extreme expression, and modify the process for investigating complaints.

What emerges from the Moon Report are choices about the purpose and nature of regulation in this area. One conception is that the state can and should regulate prejudicial and discriminatory views under provisions like section 13 and through the agency of human rights commissions. Another conception would limit the state's intervention to extreme expression which threatens violence, and treat this type of expressive activity as a criminal justice issue. In between is a third conception which would retain section 13 but bring its criteria for the regulation of expressive activity more into line with criminal law definitions. It is not within the mandate of this paper to comment further on the options presented by the Moon Report, other than to say that making a choice requires an analysis that sets the salutary benefits of section 13 off against its deleterious consequences for expressive freedom.[25]

Defamation of religion(s), religious hatred, religious vilification, and blasphemous libel

[25] The salutary side of the balancing includes the benefits that derive from enforcing section 13, as well as the symbolic and deterred value of a provision which recognizes the harm caused by certain kinds of discriminatory expression and provides a remedy for its targets. The deleterious consequences for expressive freedom include the nature of the scheme itself (*i.e.*, how complaints are brought and then managed), the actual costs to expressive freedom when complaints succeed, the chilling and silencing effects of section 13, and its ineffectiveness as a regulatory mechanism.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The defamation of religion(s) – with particular reference to "islamophobia" – has been a matter of rising debate in recent years. The UK and some Australian states have led the way, to some extent, by enacting religious hatred and religious vilification legislation.[26] Most recently, on March 27, 2009, the United Nations Human Rights Council passed a resolution condemning the "defamation of religions"; though couched in terms which would protect all religions, the defamation resolution explicitly supports the censorship of negative commentary about Muslims, Muslim minorities, and Islam.[27] For that reason, the resolution is extremely controversial.[28]

As noted above, recent months have drawn attention to human rights complaints arising from commentary that offended members of the Muslim community. Though all the complaints were dismissed, the Ontario Human Rights Commission issued a statement which, in *obiter*, identified and decried what it described as widespread Islamophobia in the media and in other outlets of public debate in Canada.[29] In light of measures adopted elsewhere and the concerns raised by this group of complaints, the question is whether Canada should also consider a specific provision for expressive activities which target religions or their adherents.

---

[26] The Australian states are Queensland, Tasmania, and Victoria, and the legislation is cited in Rex Tauati Ahdar, "Religious Vilification: Confused Policy, Unsound Principle and Unfortunate Law" (2007) 26(2) U. of Queensland L.J. 293, n.2.

[27] See Appendix A (attaching a copy of the Resolution).

[28] See Laura MacInnis, "U.N. body adopts resolution on religious defamation", March 26, 2009 http://www.reuters.com/article/worldNews/idUSTRE52P60220090326 (explaining that 180 secular, religious, and media groups urged diplomats to reject the resolution because it "may be used in certain countries to silence and intimidate human rights activists, religious dissenters and other independent voices" and reporting that Canada's representative had declared that "It is individuals who have rights, not religions," … and that "Canada believes that to extend (the notion of) defamation beyond its proper scope would jeopardize the fundamental right to freedom of expression, which includes freedom of expression on religious subjects."); see also "Chilling Thoughts at the UN", *Globe & Mail* Editorial, March 30, 2009 at A12.

[29] *Supra*, note 19.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

As noted above, "religion" is one of the grounds which defines an identifiable group for purposes of the hate propaganda provisions in the *Criminal Code*.[30] In addition, religion and religious belief are among the prohibited grounds of discrimination in federal and provincial human rights legislation across the country.[31] The sole prohibition in current Canadian law that is specific to religion – the offence of blasphemous libel – is limited in scope by its focus on Christianity, and cannot serve as a general prohibition against religious hatred.[32] In the UK, the offence was specifically aimed at attacks on the Church of England, and the selective focus of the offence became problematic over time – making the crime anachronistic until it was abolished by the UK Parliament in 2008.[33] Vestiges of the offence also exist in other jurisdictions, where it is mainly dormant.[34] In Canada, the last prosecution under section 296 took place in 1936 and it is argued that the offence has fallen into (legal) "desuetude".[35] Though the provision has not been tested under the *Charter* it is unlikely to survive constitutional scrutiny.

Statutory models abroad address the problem of religious hatred in egalitarian terms. A prime example is the UK's *Racial and Religious Hatred Law 2006*,[36] which was enacted to address specific gaps in the law: the common law offence of blasphemous libel (which remained in existence at the time) singled out the Church of England and did

---

[30] *Supra*, note 17.
[31] See *e.g. CHRA*, *supra* note 2.
[32] Section 296 provides as follows: "Every one who publishes a blasphemous libel is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years". R.S.C. 1985, c.C-46.
[33] Jeremy Patrick, "Not Dead, Just Sleeping: Canada's Prohibition on Blasphemous Libel as a Case Study in Obsolete Legislation" (2008) 41 U.B.C. L. Rev. 193 at 207.
[34] *Ibid.* at 207-14.
[35] *Ibid.* at 242-47 (discussing the doctrine of desuetude).
[36] *Racial and Religious Hatred Law, 2006*, c.1 (U.K.)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

not protect other religions from being blasphemed; in addition and more importantly, the UK's then existing race hatred law revealed troubling anomalies. Specifically, attacks on religious adherents could only be prosecuted where the religious targets were a *race* for purposes of the legislation. In other words, it was an offence to stir up hatred against Jews or Sikhs, who met the "race" criterion, but not against members of other religions – such as Muslims or Christians – who lacked a cohesive racial characteristic and were excluded from the statute's protection.[37] Meanwhile, and though the UK legislation was designed to provide a corrective, religious vilification laws have been enacted in at least three Australian states.[38]

Even in the absence of a constitutional guarantee like section 2(b) of the *Charter*, the U.K. and Australian laws have attracted intense criticism. The literature suggests that these laws are problematic for at least three key reasons: 1. it is impossible to separate extreme expression about a religion from extreme expression about its adherents; 2. in the realm of religion belief is equated with truth, and truth is equated with belief; and, 3. the self-censorship and the chilling effect which accompany many restrictions on expressive freedom are magnified in this context by the dynamics of religious discourse.

It is one matter for the state to protect members of religious groups from being targeted by hate speech because of their religious beliefs, and quite another for the state to protect particular religions – their institutions, practices, and beliefs – from attack and

---

[37] See Kay Goodall, "Incitement to Religious Hatred: All Talk and no Substance?" (2007) 70(1) M.L.R. 89 at 93 (explaining why incitement to hate Jews, Sikhs or Gypsy travelers falls within the race hatred provisions, but incitement to Muslims or Christians does not).

[38] A decision in the state of Victoria which quickly became a *cause célèbre* is *Catch the Fire Ministries Inc. v. Islamic Council of Victoria Inc.* [2006] V.S.C.A. 284.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

criticism. Though commentators agree that it would be unacceptable for the state to prohibit criticisms of religion, the problem is that an attack on religion may be indistinguishable from an attack on adherents who follow and practice its creed. In other words, it may be difficult to comment freely – and vehemently – on religion without at the same time targeting, offending, or harming its adherents. In that, the publication of "The future belongs to Islam" by Maclean's magazine may be a case in point. For that reason, these measures have been described as a new form of blasphemy law.[39] Yet more troubling than the religious hatred and religious vilification provisions is the March 2009 UN resolution, which would prohibit the defamation of *Islam* as well as of Muslims and Muslim minorities.

A second concern is that religion – as a matter of faith and belief in the absolute truth of religious creed – lends itself to extremist expression. It is in the nature of religious faith to indoctrinate, proselytize, convert, and – on some occasions and in some cultures – to practise intolerance. Those who hold the faith are believers in the truth of their religion – its origins, hegemony, tenets, and practices. Non-believers and those who follow other faiths may be seen as purveyors of sin, as enemies, as evil incarnate or the devil. Religious views are strongly held and expressed; religion has been and can be an

---

[39] See Joel Harrison, "Truth, Civility, and Religious Backgrounds: The Contest Between Religious Vilification Laws and Freedom of Expression (2006) 12 Auckland. L. Rev. 71 at 77 (stating that the argument that a person's fundamental belief system can be criticized without causing offence to or vilification of that person is fallacious); Ahdar, *supra* note 26 at 309 (quoting a line from a judgment in *Catch the Fire* that "[i]t is essential to keep the distinction between hatred of beliefs and hatred of their adherents steadily in view"); and Anthony Jeremy, "Practical Implications of the Enactment of the Racial and Religious Hatred Act 2006" (2007) 9 Ecc. L.J. 187 at 188 (stating that there is "a clear distinction between criticism of a religion and the practices of its followers on the one hand, and using threatening language to incite hatred against members of that religion" and adding that "the Act protects people, not the tenets, beliefs or practices of their religion").

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

inflammatory force. For that reason it is dangerous and unseemly for the state to enter into the fray of deciding what is religious truth, and regulating who is entitled to say what – either on behalf of, or against, particular religions and their followers.

Definitions are part of the problem here: the broader the regulation, the greater the consequences for free expression. Issues which are important in this context include the scope of the regulation (*i.e.*, what the threshold of harm is and how extreme the expression must be); what is protected (*i.e.*, whether a distinction – and a fine line – should be drawn between attacking a religion, which might be permissible) and attacking its adherents (which is not); and how the offence is measured (*i.e.*, whether the speaker can only be prosecuted for intending to cause hatred or whether it is enough that the communication was likely to cause hatred, or had the tendency to cause hatred).

A third and overriding concern in this area is that regulations which protect religion and religious groups will set up an unhealthy dynamic of censorship, self-censorship, and contests between groups which will place a chill on public discussion of important questions of public interest (*i.e.*, about religious practice, religious culture, and religious institutions). These laws also have salutary benefits, both because of their symbolic importance and because they may have the civilizing effect of deterring the gratuitous slurring of unpopular or minority religions. Yet to deter is also to silence or chill those whose expressive activities may not be illegal, and to remove their voices from public debate. As one commentator put it: "[t]he state is enlisted in religious arguments, becoming complicit in a process of legal silencing undertaken by rival

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

minority groups, engaging with them in debates of truth and falsehood, good and evil. … [F]reedom of expression is crucial in the area of religious debate. It represents the idea that a responsible citizenry must decide these questions of faith and truth themselves".[40] And, to excerpt another author at greater length:

> Various forms of teaching, evangelism and proselytism that include robust criticism or denunciation of other faiths become a dangerous exercise. Such forceful speech may now be construed by the secular authorities as nothing less than that of an illegitimate instance of religious vilification. The prudent course then is to exercise self-censorship; dilute the message or perhaps abandon the speech altogether. … Yet society can recognize and support religious minorities and express its disapproval of bias and prejudice in ways other than a potentially draconian law that stifles religious expression generally. The mere existence of such laws may have a deterrent effect but it may be the wrong one. Some religionists may now be deterred from robustly arguing the merits of their faith.[41]

There is no gap, at present, in Canadian law. Hatred against a group that is identified by its religion is prohibited by the *Criminal Code*'s hate propaganda provisions, and religious groups are also protected from being victimized by hateful and contemptuous expression – at least for now – by the federal government's human rights legislation. A defamation of religions or religious vilification provision need not, and should not, be entertained at this time, at least not without careful study and consideration of the competing considerations at stake (*i.e.*, the salutary benefits, or value added to present law, and the deleterious consequences for expressive freedom, as discussed at length in the literature).

Terrorist expression: advocating, encouraging, and glorifying terrorism

---

[40] Jeremy, *supra* note 39 at 95.
[41] Ahdar, *supra* note 26 at 297.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canada's post 9-11 anti-terrorism legislation focused on the prevention and punishment of terrorist activities, and excluded mere expression from the scheme.[42] The constitutional sensitivity around regulations which touch on activities which may be protected by the *Charter* is reflected in the debate about the definition of terrorist activity – the motive element[43] – and its invalidation, albeit at a lower court level, in *R. v. Khawaja*.[44] At present, Canada does not have provisions which either define or prohibit "terrorist expression", separate and distinct from "terrorist activity". One such measure that has been adopted elsewhere is the UK's "encouragement of terrorism" offence.

The offence has palpable consequences for expressive freedom, and has been enormously controversial as a result. Under the heading *Encouragement etc. of terrorism*, the *Terrorism Act, 2006* defines the elements of the offence in terms of statements which are *likely* to be understood by some or all of the members of the public to whom it is published, as a *direct or indirect encouragement or other inducement* to the commission, preparation, or instigation of acts of terrorism.[45] Though subjective *mens rea* is required for this offence, and can take the form either of intent or recklessness, other parts of the definition are less rigorous. For instance, the statutory concept of encouragement includes *every* statement which *glorifies* the commission or preparation of terrorist offences – *whether in the past, in the future, or generally* – and which *could* reasonably be understood as glorifying conduct and setting it up as a standard for

---

[42] See *supra*, note 16.
[43] Section 83.01(1) defines "terrorist activity" as "(b) an act or omission, in or outside Canada, (i) that is committed (A) in whole or in part for a political, religious, or ideological purpose, objective or cause …."
[44] (2006), 214 C.C.C. (3d) 399 (invalidating that provision). See generally, Ben Saul, "The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient or Criminalising Thought?" in Andrew Lynch, Edwina MacDonald, George Williams, *Law and Liberty in the War on Terror* (Australia: The Federation Press, 2007) 28-38.
[45] *Terrorism Act, 2006*, section 1, c.11 (U.K.) (emphasis added).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

emulation.[46] It is irrelevant under the statute whether the statements relate to particular acts of terrorism (*i.e.*, they could simply glorify a terrorist leader or a terrorist ideology), and it is also irrelevant that the statements may not result in any encouragement or inducement of terrorist offences.[47]

In this way, the UK legislation regulating "terrorist" expression places extraordinary restrictions on expressive freedom. Initially, the encouragement offence was certified *Human Rights Act*-compatible by Lord Carlile, whose independent review concluded that the proposal was "a proportionate response to the real and present danger of young radically minded people *being persuaded towards terrorism* by apparently authoritative tracts wrapped in a religious or quasi-religious context".[48] Yet within the space of a year the House of Lords/House of Commons Joint Committee on Human Rights concluded, to the contrary, that the encouragement offence was inconsistent with the UK's obligations under the Council of Europe Convention on the Prevention of Terrorism. Specifically, the Joint Committee concluded as follows:

> [T]he combination of the breadth of the definition of "terrorism", the vagueness of "glorification", and the lack of a requirement that there be at least a danger that an act of terrorism will result, makes the encouragement of terrorism offence in section 1 of the Terrorism Act 2006 incompatible with the requirement in Article 12 of the [above-mentioned] Convention that the establishment of any new offence of public provocation to commit a terrorist offence be compatible

---

[46] *Ibid.*, section 1(3) (emphasis added).
[47] *Ibid.*, section 1(5).
[48] Proposals By Her Majesty's Government for Changes to the Laws Against Terrorism, Report by the Independent Reviewer, Lord Carlile of Berriew Q.C. at para. 23 (October 2005) (emphasis added); available at http://security.homeoffice.gov.uk/news-publications/publication-search/prevention-terrorism-act-2005/lord-carlile-fourth-report.pdf?view=Binaryhttp://security.homeoffice.gov.uk/news-publications/publication-search/prevention-terrorism-act-2005/lord-carlile-fourth-report.pdf?view=Binary

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> with the right to freedom of expression, and proportionate to the legitimate aim pursued.[49]

That report was followed, one month later, by a report of the International Commission of Jurists which, in its "Response to the European Commission Consultation on Inciting, Aiding or Abetting Terrorist Offences" wrote critically of the UK's encouragement offence,[50] and recommended that any EU incitement law be subject to definitional restrictions aimed at containing regulatory overreach and its adverse consequences for expressive freedom.[51]

The purpose of the UK's anti-encouragement offence is to prohibit expressive activities which may serve as a recruitment tool for terrorist organizations and terrorist causes. Yet, both as worded in the *Terrorism Act, 2006* and in concept, the offence is problematic. As the Joint Committee on Human Rights and the International Commission of Jurists – as well as NGOs[52] and scholars[53] – have pointed out, the offence has

---

[49] House of Lords, House of Commons Joint Commission on Human Rights, "The Council of Europe Convention on the Prevention of Terrorism" (January 22, 2007) at 17; available at http://www.statewatch.org/news/2007/jan/coe-conv-on-terr-jhrc-report.pdf.

[50] As the ICJ explained, at page 16 of the report, "[t]he very wide definition of encouragement of terrorism, when read with the definition of terrorism in UK law, results in a criminal offence of very uncertain scope, which is likely to be difficult to apply in practice, and which is open to discriminatory application against the UK Muslim community". The report also voiced concerns about the *mens rea* requirement for the offence, and in particular, the prospect of convicting a person for recklessly encouraging terrorism: "the requirement only of recklessness as to whether some members of the public could be indirectly encouraged to terrorism, has the potential to disproportionately interference [sic] with freedom of expression rights and to have a chilling effect on political speech"; *ibid*; available at http://www.icj.org/IMG/EC_Questionaire_final.pdf.

[51] *Ibid.* at 19. Those conditions include a requirement of subjective intent to incite an act of terrorism, a causal link to a violent act of terrorism or an imminent risk of such an act, and a link to a sufficiently precise definition of terrorism to meet the standard of legal certainty; a further condition, in the view of the ICJ, is that incitement offences must not "criminalize justification or glorification of terrorism where it amounts to explanation or discussion of the circumstances leading to terrorism, or debate on the causes of terrorism or the ideology of groups linked with terrorism".

[52] See, *e.g.* Article 19, Global Campaign for Free Expression, "The Impact of UK Anti-Terror Laws on Freedom of Expression, Submission to ICJ Panel of Eminent Jurists on Terrorism, Counter-Terrorism and Human Rights"; available at http://www.article19.org/pdfs/analysis/terrorism-submission-to-icj-panel.pdf

[53] See, *e.g.* Kent Roach, "Must We Trade Rights for Security? The Choice Between Smart, Harsh, or Proportionate Security Strategies in Canada and Britain" 27 Cardozo L. Rev. 2151 (2005-2006)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

repressive implications for expressive freedom generally, and also raises the prospect that minority communities and causes might either be targeted or silenced by the self-censoring effects of provisions which have undeniable chilling effects.

In the spring of 2009 the Canadian Tamil community staged mass demonstrations, in Toronto and in Ottawa, to protest the treatment of Tamil civilians in Sri Lanka as the civil war of many years duration in that country reached its apparent endpoint. The flag of the LTTE (Liberation Tigers of Tamil Eelam or "Tamil Tigers"), which has been declared a terrorist organization in Canada and elsewhere, was displayed at these demonstrations. Though it was not against the law for demonstrators to do so, the public display of this flag attracted significant attention and negative commentary. [By way of aside – as it is tangential to the point under discussion – it is well settled that symbolic conduct is constitutionally protected by the first amendment under the U.S. Constitution; more problematic and less settled in the jurisprudence is whether the first amendment protects the right to engage in expressive activity anonymously, and would render anti-masking provisions – which were aimed at least initially against the domestic terrorism of the KKK – unconstitutional. [54]] Whatever might be said, in any case, about the Tamil Tigers, the Canadian Tamil community, or the circumstances of Tamils in Sri Lanka – and this is just one example – an anti-glorification or anti-encouragement offence, along

---

[54] See *Stromberg v. California*, 283 U.S. 359 (1931) (red flag display); *Tinker v. Des Moines School Dist.*, 393 U.S. 503 (1969) (black armband protest against the Vietnam War by public school students); *Texas v. Johnson*, 491 U.S. 397 (1989) (flag desecration); and *Virginia v. Black*, 538 U.S. 343 (2003) (cross burning). Meanwhile, many states have anti-masking legislation and it has recently been reported that an agent from the Joint Terrorism Task Force in the US arrested an animal rights activist who wore a mask while participating in a protest against the circus; available at http://www.greenisthenewred.com/blog/mask-felon/417/

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the lines of the UK model, would have significant consequences for expressive freedom in Canada.

If every idea is an incitement[55] then every idea is somewhat harmful too, in the sense – at a minimum – of causing offence, displeasure, or discomfort. Returning to the earlier concept of a spectrum, harm can be plotted along a continuum, with passive expressions of sympathy for an idea or cause at one end, and incitement – a veritable call to arms – at the other. There could be widespread or even complete agreement that the incitement at one extreme should be criminalized and also that the mere sympathy for a cause at the other should not; yet it is not so easy to specify the harm that might be associated with other points along the spectrum – which may include glorifying, ennobling, supporting, encouraging, advocating, promoting, and inducing etc. – with any degree of (causal) certainty. Without attempting to propose a threshold for harm, this paper simply points out that neither the *Charter* nor a healthy democratic regard for expressive freedom would permit the regulation of expressive activity that supports terrorist causes or organizations, without evidence that the activity is sufficiently harmful to justify the state's intervention. Absent a pressing justification (*i.e.*, evidence that glorification is an effective recruitment tool in Canada) it is difficult to see how a provision which criminalizes the encouragement, glorification, or justification of terrorism – even one which is narrowly defined – could survive constitutional scrutiny.

---

[55] See *Gitlow v. New York*, 268 U.S. 625 (1925) (*per* Justice Oliver Wendell Holmes Jr., dissenting).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

As noted above, the primary concern with this type of terrorist expression is that it might be an effective tool for recruitment into terrorist activities.[56] The UK's legislation prohibiting the encouragement and glorification of terrorism also includes provisions which address the distribution of terrorist publications, by electronic means or otherwise.[57] In noting how far the UK legislation goes, it is important to emphasize that these offences do not depend on a causal connection between the dissemination of terrorist publications and acts of terrorism; nor is the successful recruitment of converts to terrorist causes an apparent element or factor in the definition of these offences.[58]

A recent policy report by the International Centre for the Study of Radicalisation and Political Violence (ICSR) addresses the use of the internet by political extremists and terrorists as a radicalization and recruitment tool. The report, titled, "Countering Online Radicalisation: A Strategy For Action", concludes that although extremists make extensive use of it, the internet is relatively ineffective as a recruitment mechanism.[59] This does not mean it is not problematic as it serves extremist causes in other ways; instead it casts doubt on the internet's capacity to recruit converts which, the report says, are more typically drawn in through social contacts, networks, and other forms of communication.[60] The report also reviews the options for regulation and provides a

---

[56] See Olivier Roy, Ál Qaeda in the West as a Youth Movement: The Power of a Narrative" (Brighton: MICROCON Policy Working Paper 2, 2008) (discussing the roots of radicalization).

[57] *Terrorism Act, 2006*, *supra* note 45, sections 2 and 3.

[58] Compare the Moon Report, *supra* note 20 at 24 (stating that "under most accounts of freedom of expression, the state is not justified in restricting expression simply because it causes harm ... by persuading its audience").

[59] "Countering Online Radicalisation: A Strategy for Action" (ICSR, 2008) http://www.icsr.info/news-item.php?id=21

[60] The International Centre for the Study of Radicalisation and Political Violence ("ICSR") was formed in January 2008 as a partnership between four academic institutions: King's College London; the University

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

number of recommendations.[61] Once again, the limited point here is that, whether defensible or not under its own constitutional arrangements, the UK legislation – and the ease with which it brushes respect for expressive freedom aside – would not be acceptable under Canada's *Charter of Rights and Freedoms*, where regulatory responses to extreme expression are subject to requirements that the harm be demonstrated and the measure be proportional.

Conclusion

At present, Canada's regulatory framework for extreme expression is focused on the hate propaganda provisions of the *Criminal Code* and the *CHRA*'s prohibition against discriminatory expressive activity. Measures specifically addressing attacks on religions and their adherents have not been adopted. In the case of religion, extreme expression which promotes hatred, or which causes hatred or contempt toward identifiable religious groups, is currently covered by the *Code* and the *CHRA*. Religion-specific measures in other jurisdictions have been controversial and in Canada – albeit depending on the wording of any such provision – would have serious consequences for expressive freedom. The case for such a measure has not as yet been made out. Otherwise, the merits of preserving or repealing the *CHRA*'s prohibition on discriminatory expression will depend on policy considerations which are beyond the scope of this paper. Finally,

---

of Pennsylvania; the Interdisciplinary Center Herzliya (Israel); and the Jordan Institute of Diplomacy; http://www.icsr.info/

[61] Primary among them is the conclusion that removing or blocking extreme content on the internet will do little – on its own – to solve the problem; more to the point, the focus should be on the individuals who produce, publish, and disseminate this material and should take the form of strategic prosecutions. The report also emphasizes that government measures alone are not sufficient to counter the problem of "online radicalization" and suggests ways that non-state actors (*i.e.*, online communities, the media) can play a role in helping to deter and decrease the incidence of extreme online expression.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

any regulation of terrorist expression must be preceded by preliminary steps which not only would articulate the nature of the problem and the need for regulation, but would also propose a definition which identified what terrorist expression is.

* Jamie Cameron, Professor of Law, Osgoode Hall Law School, York University.

CSIS-SCRS
DISCLOSED

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Selective Bibliography

Cases and decisions

Canada (Human Rights Commission v. Taylor, [1990] 3 S.C.R. 892

Canadian Islamic Congress v. Rogers Media Inc. (20071008); Canadian Human Rights Commission (June 25, 2008)

Catch the Fire Ministries Inc. v. Islamic Council of Victoria Inc. [2006] V.S.C.A. 284

Commission Statement Concerning Issues Raised by Complaints Against Maclean's Magazine, http://www.ohrc.on.ca/en/resources/news/macleans

Edmonton Council of Muslim Communities v. JMCK Western Publishing Corp. (S2006/05-042); Alberta Human Rights and Citizenship Commission (August 1, 2008)

Elmasry and Habib v. Roger's Publishing and MacQueen (No. 4) 2008 BCHRT 378 (October 10, 2008)

Gitlow v. New York, 268 U.S. 625 (1925)

Irwin Toy Ltd. v. Quebec, [1989] 1 S.C.R. 927

R. v. Ahenakew, 2009 SKPC 10 (February 23, 2009)

R. v. Keegstra, [1990] 3 S.C.R. 697

R. v. Oakes, [1986] 1 S.C.R. 103

R v. Zundel, [1992] 2 S.C.R. 731

Stromberg v. California, 283 U.S. 359 (1931)

Texas v. Johnson, 491 U.S. 397 (1989)

Tinker v. Des Moines School Dist., 393 U.S. 503 (1969)

Virginia v. Black, 538 U.S. 343 (2003)

Reports and submissions

Article 19, Global Campaign for Free Expression, "The Impact of UK Anti-Terror Laws on Freedom of Expression, Submission to ICJ Panel of Eminent Jurists on Terrorism,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Counter-Terrorism and Human Rights; available at http://www.article19.org/pdfs/analysis/terrorism-submission-to-icj-panel.pdf

"Countering Online Radicalisation: A Strategy for Action" (ICSR, 2008); available at http://www.icsr.info/news-item.php?id=21

House of Lords/ House of Commons Joint Commission on Human Rights, "The Council of Europe Convention on the Prevention of Terrorism" (January 22, 2007); available at http://www.statewatch.org/news/2007/jan/coe-conv-on-terr-jhrc-report.pdf.

International Commission of Jurists, "Response to the European Commission Consultation on Inciting, Aiding or Abetting Terrorist Offences" (February 16, 2007); available at http://www.icj.org/IMG/EC_Questionaire_final.pdf

Proposals By Her Majesty's Government for Changes to the Laws Against Terrorism, Report by the Independent Reviewer, Lord Carlile of Berriew Q.C. (October 2005); available at http://security.homeoffice.gov.uk/news-publications/publication-search/prevention-terrorism-act-2005/lord-carlile-fourth-report.pdf?view=Binaryhttp://security.homeoffice.gov.uk/news-publications/publication-search/prevention-terrorism-act-2005/lord-carlile-fourth-report.pdf?view=Binary

Report to the Canadian Human Rights Commission Concerning Section 13 of the *Canadian Humans Rights Act* and the Regulation of Hate Speech on the Internet, by Professor Richard Moon (October 2008); available at http://www.chrc-ccdp.ca/publications/report_moon_rapport/toc_tdm-en.asp

Articles

Rex Tauati Ahdar, "Religious Vilification: Confused Policy, Unsound Principle and Unfortunate Law" (2007) 26(2) U. of Queensland L.J. 293-316

Laura K. Donohue, "Terrorist Expression and the Future of Free Expression", 27 Cardozo L. Rev. 233-341 (2005-2006)

Kay Goodall, "Incitement to Religious Hatred: All Talk and No Substance" (2007) 70(1) M.L.R. 89-113

Joel Harrison, "Truth, Civility, and Religious Battlegrounds: The Contest Between Religious Vilification Laws and Freedom of Expression" (2006) 12 Auckland U. L. Rev. 71-96

Anthony Jeremy, "Practical Implications of the Enactment of the *Racial and Religious Hatred Act 2006*" (2007) 9 Ecc.L.J. 187-201

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

David Nash & Chara Barkalis, "Incitement to Religious Hatred and the 'Symbolic': How will the *Racial and Religious Hatred Act 2006* Work?" (2007) 28(3) Liverpool Law Rev.

Jeremy Patrick, "Not Dead, Just Sleeping: Canada's Prohibition on Blasphemous Libel as a Case Study in Obsolete Legislation" (2008) 41 U.B.C. L. Rev. 193-248

Kent Roach, "Must We Trade Rights for Security? The Choice Between Smart, Harsh, or Proportionate Security Strategies in Canada and Britain" 27 Cardozo L. Rev. 2151 (2005-2006)

Olivier Roy, Ál Qaeda in the West as a Youth Movement: The Power of a Narrative" (Brighton: MICROCON Policy Working Paper 2, 2008) (discussing the roots of radicalization)

Ben Saul, "The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient or Criminalising Thought?" in Andrew Lynch, Edwina MacDonald, George Williams, *Law and Liberty in the War on Terror* (Australia: The Federation Press, 2007)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Released under the Access to Information Act

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The Continuum of Fear
Hate Crime/Terrorism

by

Dr. Barbara Perry

of the

University of Ontario Institute of Technology,
Criminology, Justice and Policy Studies

A discussion paper presented to the

Department of Justice Canada

The views expressed in this report are those of the author and do not necessarily represent the views of the Department of Justice Canada.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Contents

Abstract iii

Highlights iv

Introduction 1

A continuum of fear? 1

Relevance and utility of hate crime legislation 5

Canadian policy in the global context 8

Bibliography 14

Public Safety Canada
Sécurité publique Canada

000747

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Abstract

In what follows, I explore the connections between hate crime and terrorism, observing that the two phenomena are located on a single continuum, differing largely in scale, rather than kind. In light of the noted similarities, then, I turn to the question of the as well as the utility of Canadian hate crime legislation for responding to terrorism. I argue that hate crime legislation generally has not proven effective in its intended context, and for this and other reasons is not a viable counter-terrorism mechanism. I conclude by contrasting Canada's relatively ambivalent approach to the contemporary threat of terrorism, to the more strident policies that have been proposed or enacted in other Western nations.

Security Classified / Protected

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Highlights

A continuum of fear?
Starting with Donald Black's identification of a number of defining characteristics of terrorism, I compare hate crime and terrorism according to:

- Intimidation
- Grievance
- Recurrence
- Methods
- Mass Violence
- Agents of Terrorism
- Capacity to organize
- Covert operations

The comparison leads to the conclusion that terrorism and hate crime share similarities of kind, but not necessarily of scale. They tend to be closely aligned in terms of motives and methods, and in terms of the ways in which they affect not just immediate victims but a broader community. However, terrorism can generally be said to be on a much larger scale in terms of organization and direct impacts (i.e., *mass* violence).

Relevance and utility of hate crime legislation
The conclusions drawn from the first part of the paper suggest a corresponding affinity between statutory responses to hate crime and terrorism. However, I argue that hate crime provisions are relatively weak mechanisms for the prevention and prosecution of terrorists. Such legislation has had little impact on hate crime, so there is little likelihood that it would be any more successful in the context of terrorism. The key reasons for my assessment are:

- Limited range and enforcement of hate crime legislation
- Lack of deterrent capacity
- Lack of fit with terrorist motives and modus operandi
- Difficulty of balancing equality provisions with freedom of expression

Canadian policy in the global context
There is considerable fear among scholars and human rights advocates that post-9/11 counter-terrorism legislation poses particular problems for freedom of expression. Globally, recent, thinly veiled provisions and proposals that would target Muslims in particular are especially problematic in this respect. After listing several such examples, I offer a brief critique of "glorification of terrorism" provisions. I look then at how Canada has positioned itself viz. its peers, and conclude that our approach has been somewhat muted, and in fact, might be characterized as ambivalent. I conclude by arguing that militaristic and punitive responses to terrorism are insufficient without attempts to understand the motives of perpetrators, and then building bridges across communities.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Introduction

The terrorist attacks of September 11, 2001 on US soil redefined for North Americans, in particular, the reality of terrorism. What had heretofore been restricted to "fringe" groups of right wing extremists, or something that happened "over there," suddenly became something much larger, much more threatening, and much closer to home. The events of that day shifted terrorism from the periphery to the centre of the public consciousness. The question that is posed – is there grounds for assuming parallels between terrorism and hate crime – may thus seem odd to some. How, you might ask, can something that accounts for so much death and destruction be compared to something that is, in contrast, relatively minor in its effects? One possible response is to suggest that the two phenomena exist along a single continuum of fear and intimidation, differing in degree rather than kind. It is even possible that hate crime itself may evolve into a concentrated campaign of intimidation, at which point it may very well itself constitute terrorism.

Another effect of the 9/11 terror attacks is that they drew attention away from the more typical white domestic terrorist – such as Timothy McVeigh and members of right wing extremist groups. Now the terrorist is defined by his brown skin, and his Muslim religion (Jaggar, 2005). The "evil-doers" are, according to the rhetoric, indisputably the Muslim Other. Canadian anti-terror legislation has encapsulated this by defining terrorism according to the "political, religious or ideological" motives of those perpetrating the violence, thereby serving to "legitimize the somewhat inevitable focus on Muslims" (Stribopolous, 2004: 75). Just as the "war on drugs" has by and large been a war on black men and women, so too has the "war on terror" become a war on Muslims.

In what follows, I explore the connections between hate crime and terrorism, as well as the utility of Canadian hate crime legislation for responding to terrorism. I conclude by contrasting Canada's relatively ambivalent approach, to the more strident policies that have been proposed or enacted in other Western nations.

A continuum of fear?

To date, much of the scholarship around terrorism has come from the disciplines of political science, international relations, or law. Sociologists and criminologists have come to the game very late, but have nonetheless begun to make substantial contributions to our theoretical understanding of terrorism and counter-terrorism (Turk, 2004; Deflem, 2004; Black, 2004). Sociological frameworks that have fruitfully been applied have alternately conceptualized terrorism as a social construct; as political violence; as collective violence; as communication; as social organization; as learned behaviour; and as social control (Black, 2004; Turk, 2004). It is the latter model that I find most useful, especially in thinking about the connections between terrorism and hate crime. Such an understanding enables us to see that terrorism, like hate crime, is an exercise of power intended to constrain and contain its victims. Interestingly, Alison Jaggar offers a definition of terrorism as control which closely mirrors my own definition of hate crime. According to her, terrorism

> is the use of extreme threats or violence designed to intimidate or subjugate governments, groups, or individuals. It is a tactic of coercion intended to promote further ends. . . .Its threats or violence are aimed directly or immediately at the bodies or belongings of innocent civilians, but these are typically terrorists' secondary targets; the primary targets of terrorists are the governments, groups, or individuals that they wish to intimidate (Jaggar, 2005: 209).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Compare this to my definition of hate crime:

> It involves acts of violence and intimidation, usually directed toward already stigmatized and marginalized groups. As such, it is a mechanism of power, intended to reaffirm the precarious hierarchies that characterize a given social order. It attempts to recreate simultaneously the threatened (real or imagined) hegemony of the perpetrator's group and the "appropriate" subordinate identity of the victim's group. . . . The intent of ethnoviolence is not only to subordinate the victim, but also to subdue his or her community (Perry, 2001: 10).

The parallels inherent in these definitions already draw us toward the likely conclusion that the two phenomena are similar in nature if not in scope. To further this analysis, I turn to Donald Black for insight into untangling this puzzling web that links – potentially – hate crime to terrorism. In a series of recent articles, Black has articulated an account of terrorism as a form of social control in response to deviant behaviour. Immediately, this resonates with hate crime, which I have characterized as a means of constraining and punishing those who dare to step outside the boundaries of what is deemed their "appropriate" place, defined according to their location on any number of relational hierarchies – race, gender, religion, or sexual orientation for instance (Perry, 2001). Black's utility does not end there, however. Following from his core definition of terrorism, Black identifies a series of characteristics that might be said to define terrorism. First, the definition: "terrorism is unilateral self-help by organized civilians who covertly inflict mass violence on other civilians" (Black, 2004: 10). Heuristically, the seven derivative elements, identified and described below, provide a useful tool by which to systematically contrast hate crime with terrorism. I have also integrated related elements of terrorism as identified by Jaggar's account (2005). Arguably, hate crime mirrors terrorism on most dimensions, departing largely on questions of scale rather than kind. It is important to keep in mind throughout that the difficulty of this task is increased by the diversity of what we understand to be "terrorists." They are not homogeneous – there are, for example, those motivated by political aims, those motivated by anti-statism, and those motivated by racism. Thus it is difficult to generalize. Where possible, then, I indicate the type of terrorist organization to which I refer, as well as drawing distinctions between different types of organizations.

First and foremost, there is no doubt that the intent of both terrorism and hate crime is to *intimidate* and instil fear. As the opening definitions suggests, perpetrators of both operate with the aim of terrorizing their targets – individual and collective – into submission. Moreover, this intimidation is not only – or even primarily – targeted at just the immediate victim. Rather, in both cases, the goal is to terrorize secondary victims. In the case of hate crime, the secondary targets are members of the victim's community – other Jewish people, or other Asian people, for example. The objects of terrorism are generally much broader, in that they include a nation's people and/or their governing body.

Related to the motive is, of course, the impact. Hate crime generally has the effect of polarizing a national or local citizenry. It can pit neighbour against neighbour; it certainly instils inter-cultural hostility, thus threatening the stability and unity of a community – whether local or national. Terrorism can have a similar effect where the perpetrators are members of some identifiable group of "others." But, as we saw with the 9/11 attacks, terrorism can also have the opposite effect of drawing a threatened community together, uniting rather than dividing them internally. Here, the fear is of the "outsider" not the neighbour. Hence, the dramatic outpouring of patriotism that included the blossoming of

000751

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

American flags across the US, and the singing of *God Bless America* during the seventh inning stretch of major league baseball games.

What motivates these attempts to intimidate is what Black refers to as a "*chronic grievance*." This is a useful characterization as it does not assume political or religious or economic or any other pre-ordained impetus. Rather, it leaves the ideological basis of the grievance open to account for myriad instigating factors. Looking at the "work" of terrorists like White Aryan Resistance, for example, the grievance might be what they perceive as lax immigration law or loss of white male privilege. In a similar way, hate crime offenders are typically reacting against what they perceive to be threatening behaviour on the part of their victim(s). Levin and McDevitt (2002; 1993) include a retaliatory motive in their typology of hate crime offenders, based on their observation that a notable proportion of offenders reported that their offence was a response to a prior (perceived or real) offence perpetrated against them.

However, there is an important distinction in the nature of these "grievances." Hate crime offenders are largely motivated by bias, animosity or fear of the target community. Terrorists, on the other hand, are animated by more structurally grounded grievances, derived from an interpretation of a social order as itself illegitimate. There is a world of difference between the hate crime offender who attacks an individual Brit because he thinks the British are "arrogant snobs," and the IRA operative who attacks the British state as part of the wider agenda of throwing off the yokes of oppression. Both Christian and Islamic extremists are waging a battle to "maintain or restore a social order based on the fundamentals of faith, family and community against a rootless world order of abstract markets, mass politics and a debased sacrilegious 'tolerance'" (Rosenfeld, 2004: 26). But this need not reflect religious animus so much as the aim of imposing an alternative religious world view.

Terrorism has been characterized by many commentators as *recurrent*, thus amounting to "campaigns of terror." Terrorists might strike any target at any time. Much the same can be said for hate crime. For many targeted communities, it also represents a sustained assault. It is normative; it is endemic in a broader culture that maligns and stigmatizes the Other. Unlike most typical "street crime," violence motivated by racial or gender or religious animus, for example, is not a "one off" event. Rather, for many victims it represents an ongoing pattern of harassment and brutality. Consider the case of "move-in" violence, in which people of colour, in particular are often subject to ongoing vandalism, verbal harassment, arson, even death threats until they see no option other than to leave otherwise "white" communities.

Similarly, there are parallels in the *methods* of terrorism and of hate crime. For instance, terrorism is typically directed at symbolic targets – as in the case of the Twin Towers and the Pentagon on 9-11. For the attackers, these were indisputable symbols of American greed, arrogance and power. Hate crime, too, is often directed toward such symbolic targets. While most is interpersonal violence, bias motivated property offences generally strike "institutions," such as mosques, or gay bars – proxies for the community in question. Such assaults instil a particularly intense fear, since they are often the heart of the community, typically sites of safety and community rather than of violence.

Moreover, as Mark Hamm stresses, it is important to remember that both terrorism and hate crime are at root criminal events: murder, bombing, hostage taking, etc.. In his recent book, *Terrorism as Crime*, Hamm (2007) unpacks his relatively simple thesis – that terrorism is "ordinary" criminal behaviour, carried out for "extraordinary" purposes. Similarly, hate crime is also simply criminal behaviour, inspired by a unique set of motivating prejudices. From a

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

legal perspective, the term hate crime assumes the commission of a criminal offence, a violation of an existing criminal code. The hate crime designation may only be applied where a "predicate offence," or underlying crime is committed, as a result of bias or prejudice.

Where terrorism and hate crime part ways with respect to methods is in terms of scale. Clearly, the impact of terrorist attacks is much more extensive, such that it constitutes *mass violence* – multiple victims, even into the thousands. It often constitutes mass murder, in which the impact is immediate and dramatic. Hate crime, by contrast, typically involves a single immediate victim, or perhaps two or three at most. On rare occasions – as in Marc Lepine's anti-feminist assault – there may be a higher toll. However, this is uncommon.

There is considerable debate in the literature as to who is to be included in our understanding of the *agents of terrorism*. Some would exclude state terror. Yet this has constituted the bulk of terrorist activity historically. Terrorism has long been executed by or on behalf of states. How can one *not* class as terrorism South African apartheid, or the Nazi holocaust? The U.S. government has itself been complicit in global terrorist activities, as in its support for Nicaraguan "contras." Even now, states continue to engage in criminal, terroristic acts directed at their own populations (e.g., Taliban), or those of threatening nations (e.g., Israel and Palestine).

Nonetheless, in a departure from historical trends, a great deal of modern terrorism is instigated by non-state agents – a phenomenon that Hamm (2007) refers to as the privatization of terrorism. Contemporary terrorism is as likely to be motivated by political, religious, or even economic concerns as it is defence of a state or way of life. Anti-state terrorism (e.g., The Order) has not declined, and religiously motivated terrorism (e.g., Al-Qaeda) has in fact increased in the last half century.

An important distinction to draw in this context, however, is that the relationship between offenders and their targets is not necessarily the same in both hate crime and terrorism. While it is not unknown for members of marginalized communities to commit bias motivated violence against more powerful targets, the opposite is much more typical. That is, hate crime tends to involve more powerful actors seeking to retain their relative position. It is "top down" violence. In contrast, a great deal of non-state terrorism runs in the opposite relational direction, or "bottom up." It is violence perpetrated against powerful targets by less powerful agents. The 9-11 terrorists could hardly have chosen a stronger target, whether in economic or military terms.

Typically, terrorists sport membership in identifiable bodies with the "*capacity to organize*: recruitment, fund-raising, leadership, internal communication, and decision-making" (Oberschall, 2004: 28). This accurately describes such "traditional" terrorist groups as Al-Qaeda and the Irish Republican Army. These generally have a formalized structure and chain of command, as well as access to material and financial resources that facilitate their operation. So, too, by definition, do organized hate groups. The Klan is a classic example, having as it does a rigidly structured hierarchy, and depending on the specific clavern, access to substantial financial support. However, this begs the question of whether members of such groups are terrorists, or hate crime offenders. The members may be, but are not always, both. Moreover, most hate crime offenders are not members of terrorist organizations. Even in the most vocal and vitriolic hate groups, a relatively small number of people are engaging in a limited - albeit vicious - number of violent acts perpetrated against minority groups and against the state. Most estimates suggest that organized hate groups are responsible for little

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

more than 10 to 15% of all hate crime (Levin and McDevitt, 2002; 1993). The vast majority is committed - singly or in groups - by people who are not directly connected to any organized form of hate.

Finally, terrorist organizations carry out their strategies *covertly*, whereby they operate underground. Clearly, this is the case for organizations like Al-Qaeda, or the IRA. So, too, does this describe the activities of so-called hate groups. For example, beginning in the 1980s, Louis Beam, a long time Klansman and virulent racist, was the architect of the militia movement's strategy of "leaderless resistance," which was an attempt to enhance the invisibility of white supremacist and anti-state activists. Beam learned from his experiences with the Klan the danger of traditional lines of leadership and communication. "Leaderless resistance" advocates phantom cells and individual action as a means of defeating state tyranny. In contrast, individual hate crime offenders often diverge from these patterns. In fact, they are often very keen to be seen or at least to be known for their "prowess" in gay-bashing, or anti-Semitic arsons. It is important for them that they consolidate their own identity in visible and thus accountable ways.

Comparatively, then, terrorism and hate crime are at least close cousins. One might say they run along the same continuum of intimidation and fear. They differ largely in degree rather than kind. Yet how is this assessment useful? On the one hand, it encourages us to take hate crime seriously. It could easily evolve into terrorism, as it does among organized hate groups, for example. Yet this point is typically obscured "when attacks on non-government targets, such as abortion clinics or members of unpopular or stigmatized religions, ethnic, racialized, sexual minorities, immigrants or gypsies are defined as 'hate crimes,' thus suggesting that such attacks are no more than expressions of personal prejudice" (Jaggar, 2005: 204). As I've argued above, the intent of hate crime is not only or even primarily intimidation of an individual, but of their community.

Conversely, this assessment of the parallels between hate crime and terrorism allows us to see the latter in somewhat more familiar and comprehensible terms. Hate crime is a phenomenon about which we are beginning to learn a great deal. Such knowledge may, in fact, enable us to better understand the dynamics and motivations of terrorism as well. Again, it shares the same continuum as hate crime, while clearly occupying the extreme end of the scale.

Relevance and utility of hate crime legislation

Intuitively, one might expect that because hate crime and terrorism are closely related, they are then similarly amenable to the same sorts of legislative controls. It is worth noting that the same piece of legislation that heightened security measures against suspected terrorists – the *Anti-Terrorism Act* (hereafter *ATA*) – also embedded a two new pieces of hate crime legislation: a bias motivated mischief provision (S.430.4.1), and a provision that allows the deletion of online hate materials (S.320.1). Ironically, the provisions of the *ATA* that threatened to restrict civil liberties and human rights were justified with claims that the new hate crime legislation broadened protections for vulnerable groups. As Kent Roach (2003: 57) observes, "even illiberal definitions of terrorism and strong police powers would now be defended in the name of human and equality rights." Indeed, an attempt was made to make the whole bill more palatable with reference to its commitment to defending the rights of all, in spite of the fact that S.430.4.1 was but a small gesture embedded within a much larger slate of provisions with the potential to leave all Canadians "less free" in many respects.

000754

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

There are a number of related limitations to the use of hate crime legislation. First is the relative dearth of hate crime legislation. In contrast to the breadth of US legislative initiatives, Canada has relatively few statutory tools with which to confront hate crime. In 1970, Criminal Code amendments recognized as criminal offences promotion of genocide (S.318), public incitement of hatred likely to lead to breach of the peace (S.319.1), and wilful promotion of hatred (S.319.2) when directed against specified "identifiable groups." Somewhat distinct from these provisions is S.718.2, a sentence enhancement statute (recall also the new provisions noted above that were embedded in the *ATA*). We could also include here S.13 of the Canadian Human Rigths Act, which defines as discriminatory and subject to civil remedy, hate speech communicated via telephonic or Internet communication.

Thus, aside from the mischief provision in the *ATA*, there is no legislation that defines particular acts as "hate crimes" in and of themselves. If the state should choose to prosecute terrorist activity under the criminal code, there are plenty of more aggressive options to choose from. Hate crime legislation is relatively toothless in comparison to the array of criminal code offences that might be invoked: murder, arson, conspiracy, perhaps even sedition. And added to these, of course, are the many new criminal code provisions of the 2001 *Anti-terrorism Act*. Interestingly, there is an emerging consensus among many Western scholars that the post-9/11 anti-terrorism legislation was largely unnecessary in light of pre-existing means by which to respond to terrorists(Rogers and Ricketts, 2002; Roach, 2002; Hamm, 2007). Even the Council of Europe admitted that "normal" criminal laws in most countries were sufficient to handle crimes committed in the name of religion.

An additional problem is that, in spite of existing legislation around hate crime, very few cases have made their way to the courts. The HCCWG (2006) identified, between 2001 and 2006, 80 charges against 46 individuals under S.319.2 (wilful promotion of hatred; none of the other provisions had been invoked); only seven of these resulted in convictions. Use of the sentencing enhancement provision has been similarly rare: "The Working Group is aware of 28 judicial decisions . . . in which sentencing courts have considered evidence that hate, bias or prejudice constituted the whole or some part of the offender's motivation," and in only 17 was it deemed that these factors motivated the offence (HCCWG, 2006: 4-5). A more recent paper presented by Austin Lawrence (2009) suggests, however, that the HCCWG may have under-estimated the rate of prosecution. For the same period, he identified 5 convictions under S. 318, and more than 80 under S. 319. While higher, Lawrence's figures still reflect a reluctance to prosecute hate crime if one considers that, in 2006, for example, there were 892 hate motivated crime reported to police (Lawrence, 2009).

The explanation for the rarity of hate crime prosecutions arises from constraints in two key areas: prosecutorial and police decision-making. Prosecutors face a difficult tension in balancing "hatred" against free speech protections, and find it exceedingly difficult to "prove" motive. Additionally, prosecutors rely on decisions made by police who have tremendous discretion in whether to report or investigate an incident. There is ample scholarly evidence to suggest that police are hesitant to do either, often because of lack of training, or because of their uneasy relationships with victim communities (Bell, forthcoming; 2002; Nolan, et al., forthcoming). There is no reason to believe that they will be any more eager to pursue apparent terrorist activity under hate crime legislation, especially in light of the myriad other criminal code offences that are much easier to investigate, "prove," and prosecute.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Lack of police or prosecutorial commitment to hate crime legislation, then, is one limitation. In addition, is the question of deterrence through such statutes as the sentencing enhancement provision of S718.2. There is little evidence to suggest that hate crime legislation – or most criminal legislation for that matter – has any deterrent effect *domestically*. Add to that the fact that the terrorism the policy makers have in mind is that which is committed by foreign nationals, and this becomes even more problematic. On the one hand, potential terrorists likely have no idea what legislation exists. And nor would they care if they did. Given the structure and organization of contemporary terrorists, they assume that they will not be caught, either because their plans are so well thought out, or because they plan to die in action as was the case with the 9-11 terrorists and the dozens of recent suicide bombers across the Middle East. Either way – through capture or death – terrorists become martyrs. Legislation is a weak inoculant against fervently held ideals.

One might also question the relevance and utility of hate crime legislation to terrorism. Among the key statutes are those addressing incitement to hatred and to genocide. Incitement provisions simply do not fit the motives, or even the modus operandi of terrorists. Recall the argument raised earlier that terrorists operate covertly. Rarely do they speak out publicly, expressing their position or intent. Terrorists don't generally proselytize or announce their intentions beyond a cadre of recruits; rather they act on their principles with relatively little fanfare until the moment of action. It is only then, typically, that their message is revealed, when they "take credit" for terrorist incidents. Exceptions here might be white supremacist organizations that openly express their racism, or other biases in the context of their websites. Here, then, S.319.2 might have some value, and S.320.1 could come in especially handy. It is conceivable, for example, that posts such as the following taken from the World Church of the Creator website could be subject to the latter provision:

> WE BELIEVE that the White Race, its Biological and Cultural Heritage, is now under attack by our mortal racial enemies: Jews, niggers and the mud races. WE BELIEVE that RAHOWA (RAcial HOly WAr) . . . is the only road to the resurrection and redemption of the White Race (World Church of the Creator, online).

Clearly, this illustrative quote promotes both hatred, and perhaps even genocide and could thus be subject to "deletion." However, this is an American based site. What jurisdiction does Canada have? Indeed, there are myriad jurisdictional and technical limitations on any state's ability to regulate such expression (see Perry and Olsson, forthcoming; Moon, 2008).

Moreover, extremists generally take up arms against a state for what amount to political reasons – not out of bias, or a desire to exterminate a people. Of course, there are exceptions as in Rwanda or Darfur, but these are not the norm among contemporary terrorists. Typically, the behaviour of terrorists – white supremacists excepted – does not share the characteristics noted by Justice Dickson in *Keegstra*: "To promote hatred is to instil detestation, enmity, ill-will and malevolence in another." Again, this is the essence of white supremacist and perhaps some contemporary Islamic fundamentalist rhetoric. Other classes of terrorists – eco-terrorists, or separatist groups for example – are not inspired by animus, but by political motives. In either case, hate speech prosecutions may have less impact than conspiracy provisions, for example, in that the latter does not rest on establishing motive, only intent.

Finally, hate speech provisions generally are controversial at best – and most Canadian legislation amounts to hate speech restriction. The corresponding debate has clearly been

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

more prolonged and turbulent in the US, due in large part to the sanctity of libertarian values embedded in the First Amendment. There, the chronology of policy and politics around hate speech began nearly a century ago, in the 1920s (Walker, 1994) when the American Civil Liberties Union was first established. Since that time, policy makers and justices have had to grapple with the uneasy balance between the equality provisions of the 14th Amendment, and free speech protections of the 1st Amendment. The latter has typically prevailed. To support the privileging of expression over equality, proponents generally argue that the "offensiveness" of hate speech is not sufficient reason to restrict its use as it does not typically rise to the level of threat. Proponents of regulation of hate speech counter that there is harm inherent in offensive speech acts, to the extent that they silence those to whom such speech is directed.

In Canada, argues Richard Moon (2008), arguments for freedom of expression tend to be grounded in the values of truth, democracy, and individual autonomy. This lies uneasily with human rights doctrine, and with other existing hate speech provisions intended to "promote equality, tolerance and the dignity of the person" (Canadian Human Rights Act, S.13). Courts and public policy makers face a long and unpredictable struggle to balance the competing values. Prosecution of terrorists under such provisions, then, would be predicated on very uncertain ground. Moreover, this tension and uncertainty further undermines the deterrence effect noted earlier, such that "It is far from clear that targeting speech is rationally connected to preventing terrorism. Any effectiveness of targeting speech that advocates terrorism is likely to be minimal, especially when compared to the obvious harms caused to freedom of expression" (Roach, 2006: 2184). I will say more about this below in my discussion of global policies.

Canadian policy in the global context

The potential for restrictions on freedom of expression have also been central to the debates on anti-terror legislation. Indeed, the Office for Democratic Institutions and Human Rights (hereafter ODIHR, 2007: 220) boldly states that "Freedom of expression is particularly vulnerable to becoming a casualty of counter-terrorism measures." Freedom of expression is crucial to the functioning of a democratic state. It is recognized by most western nations, and is given international prominence in Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which reads:

> 1. *Everyone shall have the right to hold opinions without interference.*
> 2. *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
> 3. *The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
> *(a) For respect of the rights or reputations of others;*
> *(b) For the protection of national security or of public order ("ordre public"), or of public health or morals."*

Yet there are many who argue that contemporary anti-terrorism legislation compromises freedom of expression. Post-9/11, we find ourselves in what Stephen Toope (2002; 290) has characterized as a "security culture," that he argues has resulted in

000757

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> Atavistic cries of more spending on 'defence,' even in the absence of specific goals, ill-considered and sometimes draconian legislation to fight terrorism, and round-ups of vaguely suspicious individuals (often relying on ethnic or religious profiling).

Within such a regime, there is the potential for rights to take a back seat to security. Indeed, "counter-terrorism *per se* is being used as a justification for restrictions on free speech . . . counter-terrorism, in and of itself, is being presented as a proportionate and necessary justification for the interference" (ODIHR, 2007: 220). We are by now familiar with Bush and Blair's insistence that we should all be prepared to sacrifice some rights to protect ourselves from the threat of the "evil doers."

This descent began early on, in the immediate aftermath of the attacks in New York and Washington, when western nations rushed to implement new counter-terrorism policy. Many countries around the world persist in their consideration of anti-terror policies and reform thereof, many of which resuscitate the debate around the balance between security and restrictions on human rights, and especially freedom of expression. Below is a small sampling of proposals and provisions that have arisen across the Western world:

- establishment of "sect observatories" that would enable the identification and subsequent banning of "dangerous" cults and sects (France, Belgium, Austria);

- criminalization of "mental manipulation," or teachings that would result in "psychological dependency" (France);

- state proposals to require daily recitation of the Pledge of Allegiance (US);

- banning of religious groups if they "oppose international understandings" (Germany);

- banning of "conspicuous" religious symbols and dress (France; Quebec;

- conferral of citizenship would require by law citizenship ceremony, swearing allegiance and evidence of rudimentary understanding of English (UK);

- provision banning the "glorification of terrorism" (UK; UN Security Council Resolution 1624); and

- related to the above, "fomenting, justifying or glorifying terrorist violence in the furtherance of particular beliefs." These are attended by a provision to exclude or deport those deemed "not conducive to the public good" (UK).

What many of these provisions share is the conflation of terrorism with "outsider" status, and with religion, specifically, with Islam. They reflect the uncritical acceptance of the popular mythology of the "Muslim-as-terrorist," which highlights the stereotypes of the "crazed," "religiously fanatical" Muslim. Consequently, in what amounts to religious vilification, Muslims of all sects and moderation are increasingly treated as though they are proponents of terrorism or as terrorists themselves. As Davis (2002: 16) warns, "this association of religion with terror . . . and its ability to engender fear in the hearts of Americans in combination with

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

legislation and policy changes that enable expanded powers of government surveillance, has ominous implications for the nation's religious traditions."

Kent Roach (2001; 2003) makes a similar point. He argues that legislation creating new terror related activities is part of a lengthy trend toward a "narrative" or "memorial" style in criminal law, whereby the desire to recognize "tragic cases" trumps the commitment to rational and coherent legal principles. Canada joined other nations in exploiting the panic created by 9/11 to further a developing law and order agenda (for more on the moral panic associated with terrorism, see Rothe and Muzzatti, 2004; and Kappeler and Kappeler, 2004). Roach is especially concerned that in the specific case of counter-terrorism provisions,

> We ignored criminal law principles because we wanted to denounce Islamic fanaticism. . . . A criminal code that denounces certain religious or political motives as extreme in criminal law, however, runs the risk of alienating our diverse and multicultural citizenry (Roach, 2003: 28).

Moreover, there are elements of risk embedded in many of these policies, specifically with respect to their implications for freedom of expression. Extensive criticism has been directed toward recent endeavours to ban "glorification of terrorism." Particular concern has been raised about the breadth of the notion of "glorification," which might be taken to refer to sympathy, or even understanding of the motives of terrorists. For example, in the aftermath of 9/11, for example, American academics were taken to task for public statements urging people to try to comprehend the ways in which US foreign provides some incentive for the attacks. It is conceivable that, under glorification provisions, such statements would have been sanctionable. Yet clearly, they fell far short of incitement or encouragement of violence, or even of anti-American hatred. Glorification – or *apologie* – is difficult if not impossible to link causally with subsequent action. It is, rather incitement that constitutes direct exhortation to engage in violence and/or terrorism. Loose usage of terms like glorification

> is likely to result in the criminalization of perfectly lawful statements, including, in the current climate, statements that seek to initiate debate around the issue of suicide bombers and offensive, insulting or abusive statements by Muslim leaders who are critical of the liberal western way of life. This is likely to have a serious chilling effect on freedom of expression in places such as mosques or at campaign rallies (Global Campaign for Free Expression (2006: 7).

A related risk is that the militaristic response constituted by the "war on terror" is counterproductive, both domestically and internationally. At home, even the muted rhetoric of Canadian claims-makers has fuelled anti-Muslim sentiment and activity. The *ATA*, in this sense, has not protected one and all; it has left its primary targets vulnerable to demonization and discrimination. Globally, it is conceivable that the reaction has created vast resentment in the Middle East, with a consequent rise in radicalism, thereby making terrorism more rather than less likely. Returning to Donald Black, with whom I started this analysis, I accept his contention that it is important to recognize that terrorists will define the social control of terrorism as deviant – and therefore punishable - behaviour (Black, 2004: 13). More directly, Turk (2004: 348) contends that

> Destroying the "infrastructure of terrorism" may temporarily deter the threat, but its ideological sources are reinforced by what is easily (and sometimes accurately)

000759

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> construed as a disproportionate and indiscriminate assault on people whose culpability has not been proven.

Indeed, as civilian casualties rise, and as towns and villages are devastated by US led assaults, anger and bitterness have spread across many parts of the Middle East. Hard line strategies that trample the rights of people at home and abroad do not ensure national security. On the contrary, they undermine it. Military force and legal constraint are insufficient to the task of eliminating terrorism, and may in fact exacerbate it, especially if they take the form of the silencing legislation discussed herein:

> The suppression of expression that falls short of incitement to violence may not only be problematic legally but may also be counter-productive in that it can seem to lend the views expressed a legitimacy that they would not attract if they were expressed openly. It can also lead to a sense of alienation through depriving parts of the community of a legitimate means of expressing their views which may tend to push them further towards more radical forms of protest or create an environment which is more susceptible to terrorists' discourse (ODIHR, 2006: 3).

A similar conclusion is reached by Kent Roach (2006: 2178), who suggests that the imposition of speech restrictions "may also be a counterproductive anti-terrorism strategy if they confirm and broaden false perceptions that the present war against terrorism is a war against Islam." We have seen this even in Canada, where the array of newly introduced provisions "does not expose potential terrorists and fails to increase national security. On the contrary, it undermines national security while harming Arabs, Muslims, and other racialised groups by heightening their vulnerability and reinforcing their exclusion from Canadian society" (Bahdi, 2003: 294). In a Justice Committee hearing leading up to passage of the bill, Dr. Mohamed Elmasry (Canadian Islamic Congress) denounced it, arguing that it would make Muslim Canadians "the most targeted group in the country." His sentiments were echoed by the Congress' lawyer, Rocco Galati, who said "You might as well delete the Constitution from our landscape." Galati went on to say that ". . . it just repeats the historical injustices against a racial or religious minority that we've seen throughout Canadian history" (CBC News Online, 2001). Subsequent events have borne out their fears that the legislation would further enable the stigmatization and persecution of Muslims.

A 2005 CAIR-CAN report documents extensive experiences in which law enforcement agents (CSIS, RCMP, police) "approached" or "contacted" Arabs and Muslims, often with no explanation for the contact. In fact, of the 467 respondents, 8% had been contacted – the bulk of whom (84%) were Canadian citizens; among those who were not directly contacted, nearly half (43%) knew at least one other Canadian Muslim who had been (CAIR-CAN, 2005). Moreover, 19% of those who had been contacted indicated that this was not a single event, but characterised by multiple contacts. Equally intimidating were the questionable tactics used by law enforcement agents. Among the practices identified were discouraging legal or other third party assistance; aggressive and threatening behaviour; threats of arrest; problematic and suggestive questions (e.g., attitudes toward or knowledge of such things as jihad, Al-Qaeda, or loyalty to Canada *as opposed to* loyalty to their religious faith); improper identification; attempts to recruit participants as informants; and interrogation of minors. Some respondents were subject to many of these tactics; many were aware of others who shared similar experiences. The ultimate result of these patterns is to increase the alienation and mutual distrust between Muslims and law enforcement agents. Ultimately, in the "war on terror," engendering such distrust is counterproductive. It

000760

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

reduces the willingness of affected communities to cooperate with law enforcement, even if they did become aware of evidence of terrorists or terrorist activity in their midst.

Yet there is another side of the story. Clearly, as noted above, Canadian Muslims have not been spared the consequences of suspicion and its resultant discriminatory treatment. But these patterns notwithstanding, it is still accurate to say that Canada's post-9/11 response to terrorism has been tempered relative to that of peer nations like the US, the UK and Australia. By and large, Canada has remained immune to such blatant attempts to contain and control Muslim speech and behaviour. The notable exception has been in Quebec, where debates have raged around wearing of traditional religious garb (leading to a provincial royal commission inquiry). At the federal level, however, the Canadian path has been relatively tempered. In fact, Canada's reaction has been characterized by something akin to ambivalence. There is little evidence of the sort of "cowboy rhetoric" for which George W. Bush has become so (in)famous. Indeed, then Prime Minister Chretien drew criticism for his observation, made in the summer of 2002 that "the Western world is getting too rich in relation to the poor world . . . we're looked upon as being arrogant, self-satisfied, greedy and with no limits . . . You cannot exercise your powers to the humiliation of others" (*Globe and Mail*, Sept. 11, 2002). Chretien's acknowledgement of the structural underpinnings of terrorism were criticized as anti-American and as lending support to terrorists – a reminder of Bush's famous caveat that "you're either with us or against us."

Interestingly, recent events underscore Canada's relative reluctance to engage in the type of fear mongering evident in so many other Western nations. Here, the courts have begun the process of whittling away at the counter-terror legislation introduced 8 years ago. The Ontario Superior Court struck down references to "political, religious, or ideological" motives as unconstitutional. Courts have also demanded the release of non-Canadian terror suspects held without charge. And critics in the House were able to halt the renewal of the 2001 anti-terrorism bill, and with it, its provisions for preventative arrest and investigatory hearings – neither of which have actually been used by Canadian authorities to date. Highly publicized events here – the inquiry into the Air India crash, for example – would have provided fodder for vitriolic calls for greater security and more legislative control in the US or UK. However, such has not been the case in Canada. Politicians have not, for the most part, exploited these occasions to further a similar agenda here. Even *Maclean's* magazine – hardly a left wing publication – has suggested that Canada's reaction to the "terrorist threat" has been "muted." The magazine quotes the Mississauga-Streetsville MP Wajid Khan (L) as saying that "our foreign policy is a little different, our Canadian values are a little different . . . we're not as aggressive" (*Maclean's*, July 19, 2005). Khan's is an apt summary of the Canadian approach.

An illustrative example demonstrating the somewhat muted and ambiguous treatment of anti-terror legislation is found in the international provisions for "glorification of terrorism." A Parliamentary Subcommittee report in 2007 recommended the adoption of a "glorification of terrorism provision" (Subcommittee on the Review of the *Anti-Terrorism Act*, 2007a), but with very little fanfare and with no apparent consequence. The government response was simply to indicate that it would "carefully consider whether such an offence ought to be created, bearing in mind the *Canadian Charter of Rights and Freedoms* (*Charter*) and the policy implications" (Subcommittee on the Review of the *Anti-Terrorism Act*, 2007b). There

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

were even two dissenting opinions on the Commons Committee, who resisted such a provision on the bases that existing hate propaganda and incitement provisions were sufficient, and significantly, that the glorification proposal would violate freedom of expression. Moreover, the Senate subcommittee did not support the recommendation. To date, no action has been taken on the recommendation. Rather than take the opportunity to engage in "anti-terror" posturing so characteristic of other Western nations, Canadian politicians appear to be treading lightly in this area.

We are well advised to "stay the course" of moderation rather than succumb to the rhetorical flourishes of the likes of Bush and Blair. Chretien was, perhaps, on the right track when he called attention to global inequalities in wealth and power as precursors to terrorism. He is one among a few world leaders who have called for an understanding of the political and economic – not just religious foundations of the terrorism perpetrated by Islamic extremists. Understanding and responding to the underpinnings of terrorists' "chronic grievances" is an important first step, in that it allows the building of "an environment which is not conducive to terrorist recruitment or the acceptance of justifications put forward by terrorists for their actions" (ODIHR, 2006: 3). Recent work on "counter-radicalization might be especially relevant here, in that it highlights the need to take "positive measures" that seek to counter the polemics of radical messages (Stevens and Neumann, 2009). Related to this, I close with a final example of the ways in which the Canadian response excels relative to its peers:

> It has created a Cross Cultural Roundtable on National Security Issues, and in the wake of the London bombings, both Canada's Public Safety Minister and its Prime Minister met with Imams, who had agreed to a statement condemning the bombings. Smart strategies based on working with prominent Muslims who condemn terrorism and extremism may be more effective than divisive prosecutions of extreme speech, especially speech that may attempt to explain and justify terrorism as opposed to speech that promotes hatred towards identifiable groups (Roach, 2006: 2179).

000762

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Bibliography

Bahdi, Reem (2003). No Exit: Racial Profiling and Canada's War Against Terrorism. *Osgoode Hall Law Journal*. 41(1-2): 293-316.

Bell, J. (forthcoming). Policing and surveillance. In F. Lawrence (Ed.), *Responding to Hate Crime*. New York: Praeger.

Bell, J. (2002). *Policing Hatred*. New York: New York University Press.

CBC News Online (2001). *Muslims, Arabs denounce Canada's anti-terror bill*. November 6, 2001. www.ottawa.muslim.net/Newsarticles/feature_cbc_terrorbill.htm. Retrieved May 12, 2006.

Canadian Council on American-Islamic Relations (2005). *Presumption of Guilt: A National Survey on Security Visitations of Canadian Muslims* http://www.caircan.ca/downloads/POG-08062005.pdf

Davis, D. (2002). The dark side to a just war: The USA PATRIOT ACT and Counterterrorism's potential threat to religious freedom. *Journal of Church and State*, 44(1): 5-17.

Black, D. (2004). Terrorism as social control. In M. Deflem (ed.), *Terrorism and Counter-terrorism: Criminological Perspectives* (pp. 9-18). Boston: Elsevier.

Global Campaign for Free Expression (2006). The Impact of UK Anti-Terror Laws on Freedome of Expression. London. http://www.article19.org/pdfs/analysis/terrorism-submission-to-icj-panel.pdf.

Globe and Mail, PM says U.S. attitude helped fuel Sept. 11. Sept 11, 2002.

Hamm, M. (2007). *Terrorism as Crime. New York: New York University Press.*

Harding, C. (2002). International terrorism: The British response. *Singapore Journal of Legal Studies*, 2002: 16-29.

Hate Crimes Community Working Group. 2006. *Addressing Hate Crime in Ontario*. Toronto: Attorney General and Minister of Community Safety and Correctional Services.

Jaggar, A. (2005). What is terrorism, why is it wrong, an could it ever be morally permissible? *Journal of Social Psychology*, 36(2): 202-217.

Kappeler, V., and Kappeler, A. (2004). Speaking of evil and terrorism: The political and ideological construction of a moral panic. In M. Deflem (ed.), *Terrorism and Counter-terrorism: Criminological Perspectives* (pp. 175-197). Boston: Elsevier.

Lawrence, Austin (2009). Anti-Black Hate Crime Statistics. Anti-Black Hate Crime Forum, Ottawa, March 9, 2009.

000763

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Levin, J. (2002). *Hate Crimes Revisited: America's War Against Those Who Are Different.* Boulder CO: Westview Press.

Levin, J. and McDevitt, J. (1993). *Hate Crimes: The Rising Tide of Bigotry and Bloodshed.* New York: Plenum Press.

Maclean's (2005). Oops – Ottawa has suddenly realized we may have a security problem. July 1. www.macleans.ca/article.jsp?content+20050725_109489_109489.

Moon, R. (2008). *Report to the Canadian Human Rights Commission Concerning Section 13 of the* Canadian Human Rights Act *and the Regulation of Hate Speech on the Internet.* Ottawa: Canadian Human Rights Commission.

Nolan, J., Bennett, S., and Goldenberg. P. (forthcoming). Hate crime investigations. In F. Lawrence (ed.), *Responding to Hate Crime*. New York: Praeger.

Office for Democratic Institutions and Human Rights, (2007). *Countering Terrorism, Protecting Human Rights: A Manual.* Warsaw: ODIHR.

Office for Democratic Institutions and Human Rights, (2006). *Human Rights Considerations in Combating Incitement to Terrorism and Related Offences.* Vienna: OSCE/CoE Expert Workshop - *Preventing Terrorism: Fighting Incitement and Related Terrorist Activities.*

Oberschall, A. (2004). Explaining terrorism: The contribution of collective action theory. *Sociological Theory*, 22(1): 26-37.

Perry, B., and Olsson, P. (forthcoming). Cyberhate: The Globalization of Hate, *Information and Communications Technology Law.*

Perry, B. (2001). *In the Name of Hate: Understanding Hate Crimes*. New York: Routledge.

Roach, K. (2006). Terrorism, globalization and the rule of law: Must we trade rights for security? The choice between smart, harsh, or proportionate security strategies in Canada and Britain. *Cardozo Law Review*, 27 : 2151-2201.

Roach, K. (2003). *September 11: Consequences for Canada.* Montreal and Kingston: McGill-Queen's University Press.

Roach, K. (2002). Canada's new anti-terrorism law. *Singapore Journal of Legal Studies*, 2002: 122-148.

Roach, K. (2001). The dangers of a Charter-proof and crime based response to terrorism. In R. Daniels, P. MacKlem, and K. Roach (eds.), *The Security of Freedom: Essays on Canada's Anti-terrorism Bill* (pp. 131-147). Toronto: University of Toronto Press.

Rogers, N., and Ricketts, A. (2002). Fear of freedom: Anti-terrorism laws and the challenge to Australian democracy. *Singapore Journal of Legal Studies*, 2002: 149-175.

Rosenfeld, R. (2004). Terrorism and criminology. In M. Deflem (ed.), *Terrorism and Counter-terrorism: Criminological Perspectives* (pp. 19-32). Boston: Elsevier.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Rothe, D., and Muzzatti, S. (2004). Enemies everywhere: Terrorism, moral panic, and US civil society. *Critical Criminology*, 12: 327-350.

Stevens, T., and Neumann, P. (2009). *Countering Online Radicalisation: A Strategy for Action*. London: International Centre for the Study of Radicalisation and Political Violence

Stribopoulos, J. (2004). Response. In T. Gabor (ed.), *The Views of Canadian Scholars on the Impact of the* Anti-Terrorism Act (pp. 73-80). Ottawa: Department of Justice Canada.

Subcommittee on the Review of the *Anti-Terrorism Act*, 2007a. *Rights, Limits, Security: A Comprehensive Review of the* Anti-Terrorism Act *and Related Issues.* Ottawa: House of Commons. http://www2.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&Parl=39&Ses=1&DocId=2798914&File=0.

Subcommittee on the Review of the *Anti-Terrorism Act*, 2007b. *Government Response to the Seventh Report of the Standing Committee on Public Safety and National Security.* Ottawa: House of Commons. http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3066235&Language=E&Mode=1&Parl=39&Ses=1&File=18#A2.

Toope, S. (2002). Fallout from '9-11': Will a security culture undermine human rights? *Saskatchewan Law Review*, 65: 281-298.

Turk, A. (2004). Sociology of terrorism. *Annual Review of Sociology*, 30: 271-286.

Walker, S. (1994). *Hate Speech: The History of an American Controversy*. Lincoln NE: University of Nebraska Press.

Unclassified

000765

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Security, Terrorism and Governance Team Meeting
Minutes of the September 20, 2011 Meeting

Below is a brief synopsis of the brainstorming session, which was held on September 20, 2011 between members of the Security, Terrorism and Governance Team (STG) and Derek Wade of the Research and Statistics Division (RSD).

Present: Karine Bolduc, Glenn Gilmour, Dorette Pollard, Derek Wade.
Absent: Regrets received from Doug Breithaupt

A. OUTSTANDING BUSINESS from meeting of June 22, 2011:

Agenda Item 1 – 2010-2011 STG Research Projects:

1. Research on Foreign Domestic Implementation of Nuclear Terrorism Conventions (CPPNM Amendment and ICSANT):
   → Karine reported that this research project was completed months ago and the final paper will be posted to the "S" drive in due course.

Agenda Item 2 – 2011-2012 Potential STG Research Projects:

- Dorette mentioned that the calls for proposals within the STG team remained unfruitful.

- Topics formerly proposed by Nicole Crutcher:

1. A literature review on the role women are playing in radicalization/de-radicalization/terrorist incidents

2. A literature review on the role of support systems (e.g. community, family) to prevent terrorism/to be resilient
   → Karine did inquire with Brett Kubicek (Manager, Research and Academic Relations, Strategic Policy Branch, Public Safety Canada) whether Public Safety intends to conduct these two research projects in the near future.

   → Karine reported that such a determination is unlikely before the next fiscal year, given that the Kanishka initiative (led by Brett Kubicek's team) will not be going full speed before then. Even though these issues might be studied via Kanishka funds, it can't be certain at this point. Also, it was felt that the issue of radicalization has been studied by others with expertise and doing so at this time would be duplication.

s.21(1)(a)

s.21(1)(b)

Other potential research ideas:

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted] s.21(1)(a) s.21(1)(b)

B. BRAINSTORMING SESSION: The following 5 ideas were discussed at length:

1. **Focus Groups (FG) to assess the evolution in public perception of the ATA.**
   →Glenn proposed that the time may be ripe to undertake a Focus Group study, similar to the one conducted by the DOJ in 2003 to determine the following:

1. What is the public perception of the ATA a decade after 9/11?
   - The public would include members of minority communities (Muslims, other religious and ethnic groups) and the general Canadian population.

- Questions to explore in FGs would include the following:
  - Has there been a change in perception among minority groups, including Muslims, of the ATA?
  - Do these groups actually know about the ATA and the terrorism offences?
    - literacy of the ATA may be an obstacle
    - there may be differences in knowledge as between minority groups and the general population
  - In terms of terrorism offences in the *Criminal Code*, have the prosecutions in the Toronto 18 case, for example, changed their views of the ATA and notably of terrorism offences in the Code?
    - Have views changed to show the need for the AT offences in the Criminal Code or do the community groups still believe offences are not or no longer needed?

2. What is the best way to provide this information to the public especial minority communities?
   - DOJ internet and the ATA websites
   - Outreach in the different communities:

   →Karine pointed out that <u>outreach</u> is critical. [redacted]

- How can we inform and communicate better with Canadians on the ATA?
  - The objective would be to determine whether and how DOJ's efforts to communicate the ATA were used by members of the community.
    - In terms of the ATA website, what is their perception?
    - There is a perception that we have to do more to inform the public of the ATA, the offences etc.
    - Need to update the website - <u>Doug Breithaupt to task</u>

  - This FG could form part of DOJ's outreach strategy:
    - issues such as access to computers in rural areas may be of concern

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- To conclude, it was agreed that it may be useful to get a snapshot of the perception of various ethno-cultural communities about the ATA and the terrorism offences.

Considerations:

Costs:

- Conducting FGs can be relatively cost efficient:
  - FGs would cost less than $5000.00 each
  - Costs depend on the number and location of the FGs.
- Derek indicated that the 2011-2012 budget for PSAT national security/terrorism research is $47,000.
- Derek is to confirm whether this figure covers amounts from last fiscal year.
- $47,000 would easily cover FGs in different parts of the country

Alternative measures:

- The idea of using public opinion polls alone or in combination with FGs was also discussed. However, conducting public opinion polls is a cost intensive exact science, which could not be done by Research
- Public Opinion Poll Agencies can charge around $100,000.00 to create and conduct an opinion poll.
- Other obstacles to using opinion polls include:
  - identifying the polling sample i.e., representatives from the general population and minority communities
  - How would you formulate the questions to receive responses that are statistically reliable?

2. [redacted]

s.23

s.21(1)(b)

→There was consensus that this would be an excellent research topic for PSAT funding possibly through a sourcing contract.

3. [redacted]

s.21(1)(b)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(b)

[redacted]

s.21(1)(b)
s.23

Considerations for suggestions 2 & 3

s.21(1)(b)
s.21(1)(a)

- [redacted]

4. **Law School national security law essay writing competition:**
→Dorette brought forward the idea of devoting some of the PSAT funding to support and encourage legal research and writing through an essay competition on national security law and terrorism in Canadian law schools.
    - This would entail inviting Deans to encourage professors who teach national security law to have their students participate in the essay competition
    - The competition would have a monetary award: $1,000.00 to $3,000.00.
        - This competition would get the brightest minds in Canadian law schools to conduct research on national security law and terrorism
        - The topics may be preselected by the STG Research Committee, e.g.:
            - the armed conflict exception
            - [redacted]
        - The essays would be research essays prepared and graded in either second or third year of law school

    →Consensus was that this would be a great idea especially since it encourages legal scholarship and interest in national security law among future lawyers. The calibre of the research would be very high particularly since one of the criteria would be that the submission be a graded paper from a second or third year law school course.

Considerations

→Glenn raised the incident of a DOJ human rights law essay competition some years ago where the media got a hold of the winner, a student whose essay was critical of the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(a)

s.21(1)(b)

Government. [redacted] For example it should be noted that the views expressed in any selected essay represent those of the author and not the DOJ or the government. Otherwise this would be a worthy undertaking for PSAT funding.

5. Precedent Research

→Derek suggested that many of the precedent research on legal topics can be carried out by hiring a summer student i.e., a second year law school student or a co-op law student from a law school intensive legal programme. For example, Osgoode Hall Law School has a criminal law intensive programme, which includes a mandatory practicum component lasting 10 week during the school term, whereby second and third year students gain hands-on experience either in a defence firm, in a Crown law office or with a judge. The University of Ottawa also has similar programmes.

The idea here is to have DOJ-STG participate in such programs and have a co-op law student attached to the STG team to provide precedent research.

Considerations

- →Derek noted that this would be of great assistance not only to the students and STG. Research's expertise lies in the social science analysis and not the law. Such precedent research could well be conducted by hiring such summer law or legal co-op students.
- Costs would be nominal.

C. OTHER BUSINESS

These Research Proposals will be discussed at the next STG Team meeting on October 12, 2011.