DEFENDING CANADIAN PRIVATE SECTOR FROM SOPHISTICATED CYBER INTRUSIONS

s.15(1) - Defence s.16(2)(c)

Issue

There is a the defensive capabilities of the Canadian private sector. *Canada's Cyber Security Strategy* (CCSS)

Background

the Government is doing under the CCSS is helping to build the resilience of the Canadian cyber infrastructure and reduce the risks of losing valuable information, . These sophisticated cyber actors are often called Advanced Persistent Threats (APTs).

The current situation is that there are an increasing number of new software vulnerabilities that can be exploited to gain access to companies' networks.

because of resource limitations and software dependencies.

opening an infected file or following a bad link and downloading malware.

Discussion

The current approach of the CCSS will achieve a more resilient cyber infrastructure in Canada, by preventing or mitigating the harmful effects of much criminal activity.

The scale of the problem is significant. The cost of maintaining a highly secure network is high for each company, and they may not be willing to make that investment

With many thousands of companies in the same situation,

The sophisticated threat originates from purposeful actors. The nature of the internet allows sophisticated actors to operate anonymously and most of the time, avoid accountability for their actions.

Conclusion

The CCSS will increase the resiliency of Canadian cyber infrastructure The core problem to be solved is to make the negative consequences for bad cyber actors outweigh the benefits.

Date: July 11, 2012
By: Bud Cameron

s.15(1) - Def(2)(c)
s.16(2)(c)
s.21(1)(a)

Dvorkin, Corey

From: Coelho, Rose
Sent: December-02-10 9:33 PM
To: Bradley, Kees; Dvorkin, Corey; Hayward, Jane; Mohammed, Melanie; Vershinin, Sergey
Subject: FW: Symantec in Embassy Magazine re: CDN Government's Cyber Security Strategy

Rose Coelho
Director, Cyber Policy | Directrice, Politiques cyber
National Cyber Security | Cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
340 Laurier Ave W | 340, avenue Laurier O
Ottawa, ON K1A 0P8
Telephone | Téléphone: 613-993-9537
Rose.Coelho@ps-sp.gc.ca

s.19(1)

From: Gordon, Robert
Sent: December 2, 2010 4:53 PM
To: Durand, Stéphanie
Cc: Dick, Robert; Coelho, Rose; Maillé, Marie Anick; Eke, Darren
Subject: FW: Symantec in Embassy Magazine re: CDN Government's Cyber Security Strategy

Thought you would be interested in the comments from Symantec on the cyber security strategy.

Robert W. (Bob) Gordon
Special Advisor, Cyber Security /
Conseiller spécial, cybersécurité
Public Safety Canada / Sécurité publique Canada
340 Laurier Avenue West / 340 avenue Laurier Quest
Ottawa, Ontario K1A 0P9 / Ottawa (Ontario) K1A 0P8
613 949-7380 Fax/Téléc.: 613 990-3287
E-Mail / Courriel: Robert.Gordon@ps-sp.gc.ca

From: Tiffany Jones [mailto:
Sent: November 30, 2010 5:51 AM
To: Gordon, Robert
Subject: FW: Symantec in Embassy Magazine re: CDN Government's Cyber Security Strategy

FYI, we wanted to demonstrate our support of the effort and document when asked by the media. Please let us know if there is anything else we can do to support.
Best,
Tiffany

embassymag.ca "Industry sees only baby steps in cyber security"
This article discusses the Atlantic Council of Canada cyber-security conference held at the Department of Foreign Affairs headquarters. Academics, students, diplomats, politicians, members of the military and Symantec attended the conference.
The government brought in private security representatives to its news conference, such as Internet security firm Symantec, which is now singing the government's praises.
"Overall, the strategy is well conceived and we are excited about the Canadian Government's commitment to cyber security," wrote Michael Murphy, Symantec Canada's vice-president and general manager, in an emailed response.

Quotes by: Michael Murphy, vice-president and general manager, Symantec Canada; Paul Meyer, former cyber-security officer, Foreign Affairs department; Bill Graham; former minister, defence and foreign affairs; Bernard Courtois, president and CEO, Information Technology Association of Canada; Unnamed spokesperson, Public Safety Canada.

This article also appeared in:
Embassy Magazine (print) "Industry sees only baby steps in cyber security"

EMBASSY
http://www.embassymag.ca/page/view/cybersecurity-11-24-2010
November 24, 2010

Industry sees only baby steps in cyber security

By: Carl Meyer

Industry is praising Canada's new national cyber-security strategy as a needed step. But critics say the plan does not go far enough, and if one thing is clear, the country has a long way to go to catch up to its allies.

On Nov. 17, the Atlantic Council of Canada held a one-day cyber-security conference at the headquarters of the Department of Foreign Affairs that was attended by academics, students, diplomats, politicians and members of the military.

Cyber security refers to the protection of computers and information technology from unwanted tampering over the Internet and communications hardware. It is an umbrella term that covers two general ideas: cyber espionage, or electronic spying; and cyber crime, or electronic criminal activity.

The topic is hot on the agenda of Canada's allies. On Nov. 19, NATO released its new strategic planning document that referred to its desire to develop its member states' abilities to "prevent, detect, defend against and recover from cyber attacks." It also expressed a need to bring all NATO members "under centralized cyber protection."

As well, the Nov. 20 European Union bilateral summit with the United States addressed cyber-security issues. At the conclusion of that summit, the EU, US and NATO announced they had signed a three-way cyber-security pact. The EU will establish a cyber-crime centre in 2013 and a network of computer response teams in each EU country.

This follows the US government's establishment in May of US Cyber Command, a military unit that collaborates with Homeland Security to protect government and private-sector computer networks from the hundreds of attacks US officials say are being launched against that country daily.

All of this would seem to suggest that Public Safety Minister Vic Toews's announcement on Oct. 3 of a national cyber-security strategy places Canada firmly in the game. The government's plan discusses both electronic spying and criminal activity, as well as the need to reach out to the private sector and establish new public-private partnerships.

Indeed, preliminary reaction was predictably positive: the government brought in private security representatives to its news conference, such as Internet security firm Symantec, which is now singing the government's praises.

"Overall, the strategy is well conceived and we are excited about the Canadian Government's commitment to cyber security," wrote Michael Murphy, Symantec Canada's vice-president and general manager, in an emailed response.

But the plan is not as robust as some would like. Privately, industry representatives say there has not been enough progress from the federal government's side in recent years. The private sector has been forced to provide its own solutions by protecting its communications grids and monitoring its Internet and cell-phone traffic ever since the industry was born in the early 1990s.

And while the federal government has examined the issue at least as far back as 1987, with the establishment of the Interdepartmental Computer Security Panel, and several reports throughout the 1990s and 2000s have addressed the issue, so far there has been no significant shift to the government side on the big tasks like comprehensive monitoring.

"It's true that it's still at an early stage, in some ways it's a bit of a placeholder for perhaps a more ambitious document at a later stage," said Paul Meyer, a former Foreign Affairs department cyber-security officer.

Mr. Meyer also noted that because of Public Safety's funding constraints—the department is getting $90 million over five years for cyber security—it had to be "fairly modest" in terms of discussing particular program activities.

At the Atlantic Council conference, there were other problems mentioned. Former defence and foreign affairs minister Bill Graham pointed out that some view the strategy as being too "Canada-centric," focusing too much on national security and not enough on forging international collaborations like the US-EU-NATO pact. For their part, EU Commission officials say they have pressed their own member states to adopt "holistic" cyber-security strategies for years.

Publicly, the industry takes a softer line. Bernard Courtois, president and CEO of the Information Technology Association of Canada, the lobby group representing 1,300 information technology companies like Bell, Rogers, and Telus, acknowledged that there had not been a robust dissemination of the government's plan yet. But he said he expected, for security reasons, that the government would prefer not to divulge its specific efforts.

"The kinds of things that you're doing, the kinds of approaches that you're using, the attackers know all that but it's not the same thing as if you knew it officially and you had it described in a comprehensive fashion," he said.

And the government, for its part, says it is already being proactive and is collaborating internationally.

Public Safety Canada says that it participated in September in the US-led "Cyber Storm III" exercise with Australia, New Zealand and the United Kingdom, and that this exercise included private sector involvement.

A spokesperson for the department also said the government is "already engaging the private sector on cyber security issues" such as Mr. Toews's National Strategy and Action Plan for Critical Infrastructure, announced in May, that establishes "government and industry networks in all critical infrastructure sectors" including those that could be targeted in cyber attacks.

"This continuous dialogue with the critical infrastructure community has built a number of strong partnerships with private sector organizations, including the Canadian Electricity Association, Microsoft Canada, and other owners and operators of critical infrastructure," the spokesperson wrote.

That industry-wide approach dovetails with the government's efforts to wrap up its information technology efforts into a "digital economy strategy." A Nov. 22 presentation by Industry Minister Tony Clement included the cyber security plan under the notion of evolving regulatory frameworks with business.

Dvorkin, Corey

From: PETER.ARCHAMBAULT@forces.gc.ca
Sent: January-05-11 8:35 AM
To: DONALD.NEILL@forces.gc.ca; Dvorkin, Corey
Subject: RE: Cora report
Attachments: CR 2010-274.pdf

Viola

From: Neill DA@ADM(S&T) DOR(JOINT)@Ottawa-Hull
Sent: Wednesday, 5, January, 2011 08:34 AM
To: 'Dvorkin, Corey'; Archambault PM@Canada COM@Ottawa-Hull
Subject: RE: Cora report

It's not on the pubs database. Maybe PFJ has it.

From: Dvorkin, Corey [mailto:Corey.Dvorkin@ps-sp.gc.ca]
Sent: Wednesday, 5, January, 2011 08:28 AM
To: Archambault PM@Canada COM@Ottawa-Hull; Neill DA@ADM(S&T) DOR(JOINT)@Ottawa-Hull
Subject: Cora report

Don't suppose one of youse dee-ess-sci-guys could shoot me over a copy of this?

OTTAWA — Nearly a decade after the 9/11 attacks, Canada still hasn't developed a reliable strategy for protecting such critical energy infrastructure as refineries, power plants and offshore petroleum platforms, according to a new study commissioned by the Defence Department.

Inaction by the federal government has left key energy assets vulnerable to a range of threats, from terrorism and natural disasters to the emerging danger of a cyberattack, says the study quietly released last month but now reported for the first time by Postmedia News.

An attack that disrupts or damages energy infrastructure would not only have major social and economic impacts, but could also stoke "cross-border tensions" with the United States, which looks to Canada as a dependable supplier within increasingly integrated North American energy markets.

"The protection and resilience of critical infrastructure have often been described as major priorities for the government, yet the reality appears rather different from the rhetoric," writes Angela Gendron, a senior fellow at the Canadian Centre of Intelligence and Security Studies at Carleton University in Ottawa. Her study was commissioned by Defence R&D Canada, the research arm of the Department of National Defence.

Canada urgently needs to develop a national plan — and ideally appoint a central body to enforce it — to replace the patchwork of rules and safeguards currently being implemented by provinces and private industry, Gendron warns.

One of the diplomatic cables recently released by WikiLeaks contains a list compiled by the U.S. State Department of infrastructure around the world that Washington considers critical to American security, economic and public-health interests. Canadian sites include the James Bay hydroelectric power project in Quebec, the Seven-Mile dam in British Columbia, AECL's medical isotope-producing nuclear reactor in Chalk River, Ont., and the network of natural-gas pipelines operated by TransCanada Gas of Calgary.

However, Canada has yet to publicly identify the exact sites it considers critical to the nation's interests.

In the wake of the Sept. 11, 2001 attacks, the federal government created the department of Public Safety and Emergency Preparedness to oversee Canada's national-security efforts.

A Public Safety spokesman noted that the department released a national critical-infrastructure strategy in May that paves the way for the federal government and the provinces to develop and test plans for protecting key sectors. The department has made significant progress in implementing the strategy, such as through the publication of a "risk-management guide" for critical sectors, the spokesman said in an emailed statement.

But Gendron says the strategy is too "reactive" and relies too much on the voluntary participation of the private sector, which has been reluctant to share data with the government.

Energy assets in Canada tend to be concentrated in certain regions of the country and, increasingly, integrated with U.S. distribution networks. While that has worked to Canada's economic advantage, it has also made such assets "high-value" targets for an attack and heightened the potential impact of a natural disaster such as an earthquake.

The domino effect of a major network failure can be crippling, a reality that hit home in the summer of 2003, when problems at a power utility in Ohio left about 50 million people in Ontario and eight U.S. states in the dark. The blackout cost about $6 billion in economic losses.

Gendron notes that al-Qaida has called on its recruits to strike any petroleum interests that supply the U.S. as part of an "economic jihad" against the Americans.

"As both a target in its own right and as a means of striking at American oil dependency, which al-Qaida has identified as America's greatest strategic vulnerability, Canada is susceptible to a major attack," writes Gendron, who says such an attack should be considered a "low probability/high impact" risk.

If terrorists strike, it might not be a direct "physical" attack.

"Much of Canada's critical energy infrastructure and processes are today managed remotely from central control rooms which use computers and communications networks to control the flow of energy supplies (gas, oil, electricity) through pipelines or grids," says Gendron.

That makes modern energy networks vulnerable to cyberattacks that can be even more difficult to deter than conventional threats, according to Gendron.

"Sophisticated state-led cyber espionage or warfare is a serious issue but easier to deter when the adversary is a state with an easily identifiable government and location than when cyberattacks are carried out by surrogates, criminals, terrorists and hackers who cannot readily be traced."

Corey Michael Dvorkin
Senior Strategist / Conseiller principal
National Cyber Security Directorate / Direction générale de la cybersécurité nationale
Public Safety Canada / Sécurité Publique Canada
340 Laurier Avenue West / 340, avenue Laurier Ouest
Ottawa, Ontario, K1A OP8
Tel: (613) 990-9608
corey.dvorkin@ps-sp.gc.ca

Critical Energy Infrastructure Protection in Canada

Angela Gendron
Canadian Centre for Intelligence and Security Studies
Carleton University

DRDC CORA CR 2010-274
December 2010

Defence R&D Canada
Centre for Operational Research & Analysis

Strategic Analysis Section

National Defence / Défense nationale

Canada

Critical Energy Infrastructure Protection in Canada

Prepared By:
Angela Gendron
Canadian Centre of Intelligence and Security Studies
The Norman Paterson School of International Affairs
Carleton University
Senior Fellow
Contract Project Manager: Stéphane Lefebvre, 613-996-3918
PWGSC Contract Number: W7714-093788
CSA: Peter F. Johnston, Strategic Analyst, 613-996-3389

The contract report was produced in support of the Energy Security Project Thrust 10aa09.

Defence R&D Canada – CORA

Contract Report
DRDC CORA CR 2010-274
December 2010

Principal Author

Original signed by Angela Gendron

Angela Gendron

Senior Fellow - Norman Paterson School of International Affairs

Approved by

Original signed by Stéphane Lefebvre

Stéphane Lefebvre

DRDC CORA Section Head Strategic Analysis

Approved for release by

Original signed by Paul Comeau

Paul Comeau

DRDC CORA Chief Scientist

Energy Security Project Thrust 10aa09

Defence R&D Canada – Centre for Operational Research and Analysis (CORA)

Abstract

Various government Ministers have affirmed the importance government attaches to the protection of critical energy infrastructure. Nine years after the attacks on 11 September 2001 first focused attention on the potential vulnerability of infrastructure and the economic, social and political consequences of a failure of assurance, a strategy has still not been approved and the assets requiring protection not yet identified. While due respect must be given to the jurisdictional authorities which have been established by the Constitution, international terrorism and newly emerging global threats such as electronic attacks on IT and communication systems have only increased the urgency for Canada to have in place a proactive, seamless system for the protection of those energy assets and services which are so vital to Canada's well-being and prosperity, and North American security. The effectiveness of the draft Strategy and Action Plan proposed by Public Safety Canada will depend upon the voluntary participation of the various public and private sector stakeholders and the extent to which a culture of information sharing and collaboration can be inculcated. Arguably, this is a passive and reactive Plan which gives insufficient attention to deterring and preventing malicious attacks on infrastructure.

Résumé

Plusieurs ministres ont affirmé que le gouvernement attache beaucoup d'importance à la protection des infrastructures énergétiques essentielles. Neuf ans après les attaques du 11 septembre 2001 aient pour la première fois attiré l'attention sur la vulnérabilité potentielle des infrastructures et les conséquences économiques, sociales et politiques de notre incapacité à assurer leur sécurité, une stratégie n'a toujours pas été approuvée et les actifs ayant besoin d'être protégés n'a toujours pas été identifiée. Bien qu'il soit nécessaire de respecter les compétences de juridiction définies par la Constitution, le terrorisme international et les menaces qui ont commencé à émerger au niveau mondial—tels que les attaques électroniques contre les systèmes de TI et de communication—n'ont fait qu'accroître l'urgence pour le Canada de mettre en place un système proactif et transparent de protection de ces actifs producteurs d'énergie et des services énergétiques qui sont si essentiels à la prospérité et au bien-être du Canada ainsi qu'à la sécurité de l'Amérique du Nord. L'efficacité de l'ébauche de la Stratégie et plan d'action en matière d'énergie proposée par Sécurité publique Canada dépendra de la participation volontaire des différents intervenants des secteurs public et privé et de notre capacité à inculquer une culture de collaboration et de partage de l'information. Il est sans doute permis de penser qu'il s'agit d'un plan passif et réactionnel qui accorde une attention insuffisante à la dissuasion et à la prévention d'attaques malveillantes contre les infrastructures.

This page intentionally left blank.

Executive summary

Critical Energy Infrastructure Protection in Canada:

Angela Gendron; DRDC CORA CR 2010-274; Defence R&D Canada – CORA; December 2010.

Various governments have claimed that emergency management and critical infrastructure protection are major priorities. The reality appears rather different from the rhetoric. A 2008 draft strategy and action plan for Canada's critical infrastructure still awaits formal approval. Public Safety Canada has been criticized by the Auditor General for its lack of leadership in coordinating the efforts of the various actors who share responsibility for critical infrastructure protection.

Neither is there any consistency in the identification, regulation, or application of security standards from one sector to another. While complex and emerging threats respect no boundaries, different jurisdictions in Canada adopt a variety of countermeasures against the threats to national critical infrastructure.

Damage to or discontinuity of critical energy infrastructure is likely to have major social and economic repercussions. To the extent also that infrastructure forms part of the North American Energy Hemispheric network, political repercussions could prove more severe than the economic and social consequences of a disruption. As a major energy supplier to the United States (U.S.), the criticality of Canada's energy infrastructure derives in part from the vital contribution which energy exports make to the economic prosperity and growth of both Canada and the United States. This mutual dependence needs to be factored into any risk assessment.

Continental energy integration is supported and sustained by regional trading arrangements such as the North American Free Trade Agreement (NAFTA) and the Security and Prosperity Partnership (SPP), but more informal cross-border relationships between owners/operators and their industry associations do much to facilitate the exchange of information and alert warnings. There may be a need for more bilateral agreements between Canada and the United States.

Energy sector products are highly diverse but its supply infrastructure is regionally concentrated and closely integrated continentally with the United States. While the concentration of energy assets such as oil refineries and gas processing plants in certain geographic areas in North America reflect the economic advantages of location, that density also presents multiple high-value energy targets and increases the regional impact of natural disasters. Key installations are typically well-protected although off-shore production platforms may still be vulnerable to assault by sea or air. Over 80% of energy sector assets and installations are privately owned or operated.

Canada's highly de-centralized structure and distributed division of responsibilities with respect to critical infrastructure has resulted in disparate strategies for the protection of critical infrastructure and emergency management across provincial jurisdictions. The success of an integrated "all-hazards" risk management approach to security and emergency management as outlined in the draft strategy, will depend upon extensive public/private sector partnerships between the various actors who share responsibility for energy infrastructure.

Energy infrastructure is threatened by ongoing criminal acts of theft, vandalism, public order extremism and severe weather conditions but terrorism and cyber attacks pose significant risks. The main terrorist threat emanates from international Islamist extremism as epitomized by al-Qaeda, affiliated groups or homegrown terrorists inspired by jihadism. Electronic attacks may be perpetrated by widely different groups or individuals with various motives. Much of Canada's national critical infrastructure is now either built upon, or monitored and controlled by cyber information and communications technologies (ICT) which makes it vulnerable to electronic attacks and the cascading effects of disruptions in other critical infrastructure(s) (CI).

In the absence of an overarching coordinating authority, national infrastructure owners and operators have adopted different risk management methodologies. A lack of data impedes an accurate assessment of the risks from low probability/high impact events such as terrorism or the use by terrorists of weapons of mass destruction. Equally, the lack of an accurate measure for CI interdependencies means that assessments regarding the risks of cascading consequences are unreliable. In both cases, an undersupply of protection may result.

Departmental reorganizations in Canada which followed the attacks on 9/11, mirrored similar changes in the United States. Anti-terrorism measures were adopted in part to reassure U.S. sensitivities that its interests were protected in Canada. That initial focus on terrorism gave way when new and emerging global threats persuaded the Government of Canada (GOC) that a more integrated approach to security was required. A defensive focus on protective measures for specific physical assets of national interest became just one of a number of measures for reducing vulnerabilities and assuring critical infrastructure against all threats and across all sectors. National security risks are now treated as one part of an integrated 'all-hazards' risk management system.

Natural Resources Canada (NRCan), as lead line department for the Energy sector, has been pro-active and innovative in enhancing protection for national critical energy infrastructure (NCI). While Public Safety Canada now leads, by coordinating, the efforts of others to assure that infrastructure, NRCan continues to be a "subject expert" and supports and contributes to initiatives to assure critical energy infrastructure.

The draft Strategy Paper *Working Towards a Strategy and Action Plan for Critical Infrastructure* was issued in 2008 after prolonged discussions with stakeholders, circulation of two previous discussion papers and the formulation of a National Critical Infrastructure Assurance program in 2002. It has been succeeded by the National Strategy for Critical Infrastructure, Ottawa 2009 (issued in 2010). The strategy is essentially a reactive one, responding to threats rather than proactively seeking to prevent and deter attempts to destroy and disrupt NCI. It does not seek to change the status quo (dictated by custom and constitution) but relies on the voluntary participation of the private sector in the proposed integrated system and on measures to encourage more collaboration and information sharing to fill security gaps.

The inactivity on this file—or the apparent inability of government to fulfil its declared aims—is indicative of a governance problem. A failure of direction and control, or of relationships among the numerous actors involved, is likely to intensify the impact of a national security or public safety incident and therefore requires attention.

Clarity about roles and responsibilities, the fostering of trusted relationships and a more cohesive community, a common commitment to shared CIP principles—including the "duty to provide" (information), and a more proactive use of intelligence capabilities with respect to collection and analysis will all be relevant to creating a cost efficient and effective approach to protecting national critical infrastructure and assuring the assets and services vital to the well-being of Canadians.

Trans-boundary thinking is required from the outset given the global links and the interdependencies which exist within and across critical infrastructure sectors. A "containment" response to an incident will not be adequate. Prevention and planning must include the assumption that there will be cascading effects and these must be identified. Response strategies which engage the whole of government will necessitate thinking through all the inherent jurisdictional and legal ramifications and developing approaches which respect the rule of law but are anticipative and adaptive.

Sommaire

Critical Energy Infrastructure Protection in Canada:

Angela Gendron; DRDC CORA CR 2010-274; R & D pour la défense Canada – CARO; Décembre 2010.

Différents gouvernements ont prétendu que la gestion des urgences et la protection des infrastructures essentielles sont des priorités majeures. La réalité semble cependant différente de la théorie. Une ébauche de stratégie et de plan d'action pour les infrastructures essentielles du Canada datant de 2008 attend toujours d'être approuvée officiellement. Sécurité publique Canada a été critiquée par la vérificatrice générale pour son manque de leadership dans la coordination des efforts des différents acteurs se partageant la responsabilité de la protection des infrastructures essentielles.

De plus, il n'existe aucune forme d'uniformité dans l'identification des normes de sécurité, leur règlementation ou leur application d'un secteur à l'autre. Bien que les menaces émergeantes soient complexes et qu'elles ne respectent aucune frontière, les différentes juridictions existant au Canada ont adopté une vaste gamme de contremesures pour s'attaquer aux menaces envers les infrastructures nationales essentielles.

Il est probable que des dommages aux infrastructures énergétiques essentielles ou des ruptures de leurs services auront d'importantes répercussions économiques et sociales. Compte tenu du fait que ces infrastructures font également partie du réseau énergétique hémisphérique nord-américain, les répercussions politiques pourraient s'avérer plus graves que les conséquences économiques et sociales des ruptures de service. En tant qu'un des principaux fournisseurs d'énergie des États-Unis (É.-U.), la criticité des infrastructures énergétiques du Canada provient en partie de l'apport vital des exportations d'énergie à la croissance et à la prospérité économique du Canada et des États-Unis. Il faut tenir compte de cette interdépendance lors de toute évaluation des risques.

L'intégration continentale en matière d'énergie est appuyée et assurée par des ententes commerciales régionales telles que l'Accord de libre-échange nord-américain (ALENA) et le Partenariat nord-américain pour la sécurité et la prospérité (PSP), mais des relations transfrontalières plus informelles entre les propriétaires/opérateurs et leurs associations industrielles contribuent à grandement faciliter les échanges de renseignements et les informations concernant les alertes. Il pourrait être nécessaire de disposer de davantage d'ententes bilatérales entre le Canada et les États-Unis.

Les produits du secteur de l'énergie sont hautement diversifiés, mais les infrastructures de distribution sont concentrées régionalement et, au niveau continental, elles sont étroitement intégrées à celles des États-Unis. La concentration des actifs énergétiques — tels que les raffineries de pétrole et les usines de traitement de gaz naturel — dans certaines régions géographiques de l'Amérique du Nord témoigne des avantages économiques de leur lieu d'implantation, cette densité fait toutefois en sorte que ces régions offrent une multitude de cibles

de grande valeur et augmente les probabilités de répercussions régionales en cas de catastrophes naturelles. Les installations clés sont habituellement bien protégées, bien que les plateformes de production en mer puissent être encore vulnérables à une attaque par voie aérienne ou maritime. Plus de 80 % des actifs et installations du secteur énergétique sont détenus ou opérés par des intérêts privés.

La structure grandement décentralisée du Canada et la répartition des responsabilités en ce qui a trait aux infrastructures essentielles a eu pour résultat la création de stratégies asymétriques pour la protection des infrastructures essentielles et la gestion des urgences dans les différentes juridictions provinciales. Le succès d'une approche de gestion intégrée tous risques en matière de sécurité et de gestion des urgences, tel que décrite dans l'ébauche de stratégie, dépendra de l'étendu des partenariats des secteurs publics/privés entre les différents acteurs qui partagent la responsabilité des infrastructures énergétiques.

Les infrastructures énergétiques sont constamment menacées par la réalisation d'actes criminels tels que le vol, le vandalisme, l'extrémisme visant le désordre public ainsi que par les conditions météorologiques particulièrement mauvaises. Toutefois, le terrorisme et les cyberattaques constituent aussi des risques importants. La principale menace terroriste est issue de l'extrémisme islamiste international tel qu'incarné par Al-Qaeda, ses groupes affiliés ou les terroristes locaux inspirés par le jihad. Les attaques électroniques peuvent être perpétrées par des individus ou des groupes extrêmement différents ayant des motifs tout aussi variés. Les infrastructures nationales essentielles du Canada sont maintenant pour la plupart élaborées à partir de technologies de l'information et des communications (TIC) ou elles sont contrôlées ou surveillées par de telles TIC, ce qui les rend vulnérables aux attaques électroniques et aux effets domino de rupture de service dans les autres infrastructures essentielles (IE).

En l'absence d'une autorité de coordination globale, les propriétaires et opérateurs d'infrastructures nationales ont adopté différentes méthodologies de gestion du risque. Le manque de données ne permet pas de faire une évaluation précise des risques posés par des événements de faible probabilité et grandes répercussions, tels que le terrorisme ou l'utilisation par des terroristes d'armes de destruction massive. De même, l'absence de moyen de mesure précis permettant d'évaluer les interdépendances des IE signifie que les évaluations portant sur les possibilités d'effets domino que ces incidents pourraient entraîner ne sont pas fiables. Dans les deux cas, la situation pourrait entraîner une pénurie de protection.

Les réorganisations ministérielles qui ont eu lieu au Canada à la suite des événements du 11 septembre étaient le reflet des changements similaires qui se sont produits aux États-Unis. Des mesures antiterrorismes ont été adoptées en partie pour calmer les sensibilités américaines touchant la protection de ses intérêts au Canada. Cette approche initiale face au terrorisme a fait place à une autre lorsque de nouvelles menaces globales ont émergé et ainsi persuadé le gouvernement du Canada (GC) qu'une approche plus intégrée en matière de sécurité était nécessaire. Une approche défensive en matière de mesures de protection dans le cas de certains biens matériels d'intérêt national est devenue une des mesures permettant de réduire les vulnérabilités et d'assurer la protection des infrastructures essentielles contre toutes les menaces dans toutes les régions. Les risques pour la sécurité nationale sont maintenant traités comme un élément d'un système de gestion intégrée tous risques en matière de sécurité.

Ressources naturelles Canada (RNCan), en tant que ministère responsable jouant le rôle de chef de file dans le domaine de l'énergie, a agi de façon proactive et innovatrice en améliorant la protection des infrastructures énergétiques nationales essentielles (IENE). Bien que Sécurité publique Canada tienne maintenant ce rôle de chef de file en assurant la coordination des efforts de tous pour la protection de ces infrastructures, RNCan demeure un « spécialiste en la matière » et continue d'appuyer et de contribuer aux initiatives visant à assurer la protection des infrastructures énergétiques essentielles.

L'ébauche du document stratégique intitulé « Élaboration d'une Stratégie nationale de protection des infrastructures essentielles et d'un plan d'action connexe » a été publiée en 2008 après des discussions prolongées avec les intervenants, la circulation des deux documents de travail précédents et l'élaboration d'un Programme national de fiabilité des infrastructures essentielles en 2002. Le document « Stratégie nationale sur les infrastructures essentielles », Ottawa 2009 (publié en 2010) a été publié par la suite. Il s'agit essentiellement d'une stratégie réactive, répondant aux menaces plutôt que cherchant de façon proactive à les prévenir et à dissuader les tentatives de destruction et d'interruption de service des IENE. Elle ne cherche pas à changer le statu quo (dicté par les coutumes et la constitution); elle compte plutôt sur la participation volontaire du secteur privé dans le système intégré proposé et sur des mesures visant à encourager davantage de collaboration et de partage d'information afin de réduire les lacunes en matière de sécurité.

L'inactivité dans ce dossier—ou l'apparente incapacité du gouvernement à remplir ses objectifs déclarés—est révélateur d'un problème de gouvernance. Il est probable qu'un manque de direction et de contrôle, ou des problèmes à établir de relations entre les différents acteurs impliqués, aurait de plus grandes conséquences advenant un incident au niveau de la sécurité nationale ou publique. Il est donc nécessaire d'y prêter attention.

La clarification des rôles et responsabilités, l'encouragement à créer des relations de confiance, une communauté plus cohésive, un engagement commun envers les principes partagés en matière de protection des IE—y compris l'obligation de fournir des renseignements et une utilisation plus proactive des capacités de renseignement en ce qui a trait à la cueillette et l'analyse des données, tout cela sera permettra de mettre sur pied une approche économique et efficace en matière de protection des infrastructures nationales essentielles et à assurer les actifs et les services vitaux au bien-être des Canadiens.

Compte tenu des liens mondiaux et des interdépendances qui existent au sein et entre les différents secteurs des infrastructures essentielles, il faut faire usage dès le départ à une *réflexion transfrontalière*. Une réaction de « confinement » à un incident ne sera pas adéquate. La prévention et la planification doivent inclure l'hypothèse qu'il y aura des effets domino et ceux-ci doivent être identifiés. Des stratégies d'intervention pangouvernementale exigeront une réflexion tenant compte de toutes les ramifications juridictionnelles et légale inhérentes et la mise au point d'approches qui respectent la primauté du droit tout en étant capable d'anticiper et de s'adapter.

Table of contents

1 Introduction

When Canada's Minister of Natural Resources addressed the annual conference of the International Pipeline Security Forum in Ottawa in October, 2007 he noted that Canada had become an energy superpower and a major supplier of energy to the United States. As such, and given the vital importance of its exports to the economic growth, security, and prosperity of both countries, Canada must also, he said, be a *dependable* supplier. The protection and resilience of critical infrastructure have often been described as major priorities for the government, yet the reality appears rather different from the rhetoric.

Damage to or destruction of any critical infrastructure which seriously affects the safety, security, health and economic well-being of Canadians across the country becomes a matter of *national* security. The mutual reliance of both Canada and the U.S. on cross-border transfers of energy supplies (oil, gas and electricity) means that serious disruptions are likely to have *political* repercussions with respect to North American integration, as well as having economic and social consequences and undermining public confidence in the ability of government to protect core national interests.

Primary responsibility for protecting critical infrastructure rests with the owners and operators, but custom and constitutional law grant jurisdictional authority to the provinces and territories for legislating and regulating infrastructure within their boundaries. Together, they will select whatever protective measures they deem appropriate. However, it is a shared responsibility which involves a multiplicity of other actors including first line responders, municipalities, industry/business associations, regulators and federal line departments. While some emergencies can be handled locally by private sector owners/operators, municipalities or provinces, the federal government will assist when requested, when the emergency transcends jurisdictional boundaries, or when its assistance is in the national interest. The role of the federal government is therefore limited and must currently be negotiated against a backdrop of jurisdictional ambiguities, tensions and sovereignty sensitivities.

This highly de-centralized structure and distributed division of responsibilities means that protection of critical infrastructure and emergency management varies across jurisdictions: there are currently no consistent cross-Canada strategies or standards, nor have the assets and facilities which are critical to the government yet been determined.[1]

While the federal government is apparently committed to the development of a more collaborative emergency management framework and has drafted a strategy and action plan for Canada's critical infrastructure,[2] this has not yet been formally approved although officials are working towards its implementation.

---

[1] "Emergency Management-Public Safety Canada," Chapter 7 in Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons* (Ottawa: Autumn 2009), p. 22.
[2] Public Safety Canada, "Working Towards a National Strategy and Action Plan for Critical Infrastructure," 2008. http://www.publicsafety.gc.ca/prg/em/ci/strat-part2-eng.aspx, accessed on 29 March 2010.

Critical infrastructure protection (CIP) refers to measures which aim to ensure the availability, integrity and confidentiality of the physical and cyber assets, systems and services which support the nation's critical infrastructure (CI).

This study will look at the characteristics of the energy sector with respect to threats, vulnerabilities and risks, before examining how the government of Canada (GOC) has responded to emerging threats; current and proposed government policy with respect to Canada's critical infrastructure; and the governance framework which is in place to implement that policy. The study concludes with a brief comment on concerns raised in connection with an 'all-hazards' risk management approach to critical energy infrastructure protection, including the need for a more pro-active strategy.

2 Critical National Infrastructure Defined

While the term "energy security" is sometimes used to refer to the *reliability* of energy supply, the International Energy Authority (IEA) noted in a study of natural gas, that energy security is threatened not only by political and economic factors but "technical" factors i.e. those "which involve accidents, terrorism or natural catastrophes."[3] Energy installations and assets are therefore of *national* interest because technical and infrastructural reasons can both cause and aggravate the impact of large fluctuations in supply.

The term "critical infrastructure" is used to describe various categories of vital assets and services, the destruction or discontinuance of which would have serious repercussions for the owners and operators. The nature of the assets in the various sub-categories will have a bearing on the strategies adopted to protect them and how and to whom that responsibility is allocated. If destruction or disruption of certain infrastructure is expected to seriously impact upon the economic and social welfare of a nation, the effective functioning of governments, or the health, safety and security of its citizens, the criticality is such as to be of national interest and such infrastructure is described by many countries as comprising the critical national infrastructure (CNI).[4]

That term—critical national infrastructure—is not currently used by Canadian federal authorities who define critical infrastructure as consisting of the "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Disruptions of this critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence."[5]

The draft national strategy and action plan for critical infrastructure[6] does not appear to differentiate between the critical infrastructure which *collectively* exists across Canada, and infrastructure which is critical to *national* interests.[7] Whether this is a matter of sovereignty or semantics, Public Safety Canada, the lead federal department, describes its own role in terms of being one among many working to protect critical infrastructure and collaborating with others to enhance the effectiveness of that effort.

---

[3] International Energy Agency, *The IEA Natural Gas Security Study* (Paris: IEA/OECD, 1995), p. 23.

[4] UK CPNI Glossary: "CNI—Critical National Infrastructure… the loss or compromise of which would have a major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life. These critical elements of infrastructure comprise the nation's critical national infrastructure."

[5] Public Safety Canada, *Emergency Management Planning Guide 2010-2011*, accessed on 6 December 2010 at http://www.publicsafety.gc.ca/prg/em/emp/emp-2010-11-eng.aspx. Note: This definition accords closely with that contained in EU, Critical Infrastructure Protection in the fight against terrorism, COM(2004) 702 final, Communication from the Commission to the Council and the European Parliament, Brussels, Belgium, 2004, a document which does use the term CNI.

[6] "Working Towards a National Strategy and Action Plan for Critical Infrastructure."

[7] The terms "Canada's national critical infrastructure" and (protecting) "Canada's critical infrastructure," are used.

Critical infrastructure in Canada is categorized into ten sectors: (1) Energy and Utilities; (2) Communications and Information Technology; (3) Finance; (4) Health Care; (5) Food; (6) Water; (7) Transportation; (8) Safety; (9) Government; and, (10)Manufacturing. These sectors are further divided into sub-sections. Energy and Utilities, for example, is divided into electric power, natural gas and oil production, and transmission systems. "Electric power" includes power generation plants, transmission stations, power line corridors (or transmission lines), distribution stations, control stations and nuclear. These categories remain unchanged from those in an earlier "Position" paper which was published in 2005[8] to stimulate debate among public and private sector stakeholders about a strategy for critical infrastructure. (See Annex A).

[8] Public Safety and Emergency Preparedness Canada, "Government of Canada Position Paper on a National Strategy for Infrastructure Protection" (Ottawa: November 2004, released in 2005).

3 Characteristics of Canada's Energy Infrastructure Sector

Canada is richly endowed with natural energy resources. In 2009, the value of total energy exports was $327.9 billion. Canada is the largest foreign supplier to the United States of oil, natural gas, electricity and uranium, exporting more than $125 billion annually.[9] The products and services delivered by critical energy infrastructure contribute significantly to Canada's National Income, employment, economic activity and growth.

3.1 Continental, Concentrated and Diverse

Most of Canada's critical energy infrastructure is owned or operated by the private sector or provincial/territorial levels of government.[10] It is geographically dispersed and regionally concentrated. A major proportion of oil and natural gas production is in Alberta; Saskatchewan is rich in uranium; while Ontario, New Brunswick and Quebec are nuclear power producers. Over time, component parts have become deeply embedded in the distinctive history and culture of the regions in which they are situated. Much of it is connected to international networks since the energy sector is particularly likely to be operating in a global environment which is neither defined nor limited by jurisdictional or geographic boundaries.

The infrastructure required to produce, process, deliver and consume energy in Canada is diverse and complex. It includes oil pipelines and interconnected electricity grids as well as ships which deliver coal for electrical generators. Extensive networks of pipelines and power grids transmit oil, natural gas and electricity from points of production to consumers and user industries across Canada, the United States and Mexico. They cross remote territory as well as densely populated regions and, as a consequence, are vulnerable to accident and malicious acts.

Energy is a leading sector in the regional economies of Alberta, Newfoundland and Labrador, and Saskatchewan. Arctic oil and gas reserves may become important in the future as a means to boost supply.[11] The activities of the sector encompass the production, refining and delivery of petroleum and natural gas, and the generation of electric power from hydro, oil, gas, coal and nuclear power plants. These energy resources are vital for interdependent industries, commercial facilities, public and social services, and household requirements.

Canada is a part of a North American energy economy which is closely integrated continentally with the United States, connectivity being maintained by pipeline networks, electricity grids and

---

[9] D.H. Burney, "Pipeline Security, Energy Security and Economic Resilience," paper given at the International Pipeline Security Forum, Ottawa, October 2009 subsequently published online as "Pipelines, Energy, Economy," *Global Brief*, 17 November 2009, accessed at http://globalbrief.ca/?s=Derek+Burney.

[10] The Hon. Gary Lunn, P.C., M.P. Minister of Natural Resources in a speech to the 2007 International Pipeline Security Forum, Ottawa, Ontario said that 85 percent of Canadian energy infrastructure was privately owned.

[11] Peter F. Johnston, "Arctic Energy Resources and Global Energy Security," *Journal of Military and Strategic Studies*, Vol. 12, No. 2, 2010.

extensive commercial interactions among operators in the industry.[12] Canada's system of transmission pipelines for oil and gas extends for 80,000 kilometers and is connected to 345,000 kilometers of local distribution pipelines. An electricity grid operates in an integrated fashion to satisfy peak demands on either side of the border. Growing US demand for Canadian oil and natural gas over recent decades, led to the expansion of this North American pipeline network and the interconnectedness of gas grids as Canadian supplies formed an increasing share of total U.S. demand. In 2008, Canada exported 2 million barrels (bbls) per day of crude oil to the U.S. With the expected 2 million bbls/day rise in Canadian crude production by 2020, most of which will be available for export, U.S. net imports from Canada could well rise to over 4 million bbls/day of crude oil.[13]

By 2006 Canada had become the single largest international supplier of oil and natural gas to the United States. In 2008, its crude oil exports to the U.S. were valued at US$64 billion. A large proportion of Western Canada's crude oil production is heavy oil or bitumen which most Canadian refineries cannot process. The ability to export heavy crude oils to suitable U.S refineries is advantageous both to the Canadian producer and the American consumer.

These energy exports are vital to the security and economic prosperity of both countries and are likely to grow further with increased oil-sands production, the addition of more crude oil, northern gas pipelines and liquefied natural gas (LNG) facilities.[14] Continental energy integration is supported and sustained by regional trading arrangements such as the North American Free Trade Agreement (NAFTA) and the Security and Prosperity Partnership (SPP). In March 2001, the energy ministers of Canada, Mexico and the United States met to discuss a common energy strategy which included integration of their power grids. Considerable reciprocity already existed between the electric power sectors of Canada and the U.S. although the connectivity between Mexico and the United States is more limited comprising Mexican exports of oil to the U.S.A. in return for gas.

3.2 Private Ownership/Multiple Actors

Private ownership of Canada's energy infrastructure can be beneficial in that market forces tend to create the redundancies and duplications necessary for coping with disruptions, but competition also encourages businesses to invest in diverse security and business resilience solutions. This creates a fragmented security and resilience landscape which may have weak links because of a lack of consistency within and across sectors. Owners and operators and their provincial regulators are responsible for day to day protective measures and ongoing risk assessments but CIP is a shared responsibility among a multiplicity of stakeholders, including various tiers of government, industry/business associations, standardization bodies, regulators, and other jurisdictional authorities. An effective strategy requires all of them to participate fully since no one body alone can provide the necessary level of protection. While the scope for federal intervention is limited, some overarching body is needed to coordinate the efforts of all.

---

[12] In April, 2001, Canada, Mexico and the United States established a North American Energy Working Group to enhance energy trade within the common economic space, and to foster cooperation in hemispheric energy issues, infrastructure and technologies: North American Energy Working Group, *North America—The Energy Picture*, June 2002.

[13] Burney, "Pipeline Security, Energy Security and Economic Resilience."

[14] Ibid.

3.3 Dependencies and Interdependencies

The term *Dependency,* describes how one product or service affects another; an *interdependency* refers to the mutual (though usually unequal) dependency of products or services. With respect to critical infrastructure, these are the physical and electronic (cyber) linkages within and among the ten critical infrastructure sectors defined by the federal government as *national.* In order to identify the direct and indirect infrastructure linkages which support critical facilities, owners and operators need "situational awareness," i.e., a detailed understanding of organizational functions, internal infrastructures and how these link to external infrastructures.

Producers *within* the energy sector are dependent upon one another to varying degrees. As an example, oil supply is highly dependent upon electrical supply because refineries, oil pipelines and service station pumps need electric power for operation. Dependencies also exist *between* sectors: road and rail transport, for example, is critical in moving energy products to consumers and the Atlantic offshore industry relies on coastal shipping for access to drilling platforms and tankers to access and remove production to market. These dependencies can lead to disruptions which have serious commercial consequences for the owners and operators. However, the energy sector is also characterized by interdependencies which arise in large part because of a heavy reliance on information systems and communications technologies. Much of Canada's critical energy infrastructure and processes are today managed remotely from central control rooms which use computers and communications networks to control the flow of energy supplies (gas, oil, electricity) through pipelines or grids. The use of computer-based supervisory control and data acquisition (SCADA) information managements systems and the complex web of cyber connections which link energy infrastructure, means that a disruption in one system can quickly spread to others.

The vulnerabilities inherent in these dependencies became apparent in August 2003 when an estimated 50 million people across eight States and the Canadian province of Ontario were left without electrical power after a utility in Ohio experienced problems that began a chain reaction of events leading to power outages lasting, in some places, several days. This incident, known as the "Northeast Blackout of 2003," cost roughly $6 billion and caused at least 265 power plants temporarily to shut down.[15]

3.4 The Vulnerabilities

Given its diversity and complexity, Canada's energy infrastructure is vulnerable to disruption from many sources. The vulnerabilities are as varied as the systems: for example, thermal electricity generators rely on a constant and secure supply of feedstock to function efficiently, while hydro-electric production can be threatened by prolonged drought.

Energy infrastructures operate on a national and global scale and require comprehensive actions to keep them viable. Dislocation can come about as a result of failures, natural disasters or hostile action. The information needed to counter common threats and reduce vulnerabilities will vary

---

[15] U.S-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," April 2004.

between infrastructures because of the nature of their different assets. Nevertheless, common principles of security and emergency management apply to all. The likelihood of disruption can be reduced and the consequences mitigated, through measures that focus at least some resources on key vulnerabilities. The core problem is to find those nodes and connectors that drive critical infrastructures of national significance.

Critical energy infrastructure systems comprise many different companies and organizations which are linked to each other electronically within the sector and to other CI sectors through information systems. Reliance on SCADA technologies further increases vulnerability to network failures and electronic attacks making the energy sector as a whole very vulnerable. Cyber attacks may be launched to obtain or corrupt information, disrupt services or plan further attacks on infrastructure. The availability and integrity of those systems and the information transmitted is highly dependent on good physical, personal and technical protective security procedures.

Such interdependencies increase the likelihood that security incidents will have a more intense and wider impact as the consequences cascade across one or more infrastructure systems and sectors. Critical infrastructure is particularly vulnerable when it crosses boundaries and borders because it is precisely in such circumstances that jurisdictional regulations and security standards diverge, and issues relating to direction, control and accountability are most obscure.

Oil and natural gas wells are vulnerable to malicious attacks but have some protection by virtue of being dispersed and located in remote areas. Pipelines and transmission systems are inherently difficult to protect and especially vulnerable to sabotage, but they are considered minor strategic targets compared to critical energy installations and physical protective measures and system redundancy[16] can mitigate the risks to pipelines so that damage does not result in a major interruption of supply.

High-value energy assets which are geographically concentrated such as oil refineries, gas processing plants and offshore platforms,[17] are more vulnerable to large-scale disruption. These installations are typically well-protected although off-shore production platforms may still be vulnerable to assault by sea or air. The concentration of energy assets in certain geographic areas in North America reflect the economic advantages of location but density also presents multiple high-value targets for terrorist attacks and is likely to increase the regional impact of natural disasters. The destruction of much of the oil and gas infrastructure in and adjacent to the Gulf of Mexico during Hurricanes Katrina and Rita in 2005 illustrates the point.

Energy infrastructure tends to have a long life span. The location of particular physical components in a community are often considered undesirable, ("the nimby" syndrome) therefore new installations are often erected in the same location as previous structures even though sites selected years ago may not be best suited to the prevailing economic and natural environmental conditions.

---

[16] Gal Luft, "Pipeline Sabotage is Terrorists' Weapon of Choice," *Energy Security,* 28 March 2005. http://www.iags.org/n0328051.htm, accessed on 29 March 2010.

[17] Paul Parfomak, "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options," *CRS Report for Congress* RL 33206 (Washington D.C: Library of Congress, Congressional Research Service, 21 December, 2005), p. 4.

There are many different methodologies for assessing vulnerabilities but owners and operators are likely to be using either a qualitative methodology such as a risk matrix which identifies vulnerabilities and categorizes assets, sites or systems into discrete levels of risk, or a quantitative methodology which computes risk as a function of the threat, probability and consequences of an event or attack.

The likelihood of dislocations can be reduced and the consequences mitigated through measures that reduce vulnerabilities by strengthening the robustness and resilience of buildings, installations and equipment against attacks or natural events. For example, site hardening measures (increasing the robustness of the electric power grid); planning some redundancy in order to reduce the number of single points of failure (additional generator or alternative pipelines); improved modeling capability so as to better understand the downstream and cascading effects of systemic failures; correcting technical problems when they occur. The core problem is to find those nodes and connectors that drive critical infrastructures of national significance and provide additional protection.

3.5 Impact of Loss of Assurance

International travel, the interconnectedness of communications and state-of-the-art electronic and digital information systems are shrinking the world to such an extent that emerging human-induced threats are likely to spread more rapidly and have a more intense impact than was once the case with respect to threats to energy infrastructure.

The Canadian energy industry possesses a high degree of criticality for the national, provincial and local economies, for consumers and user industries, and for public well-being generally. Oil, natural gas, and electricity production are operating with little if any spare capacity or redundancy. A sudden loss of production capacity caused by a terrorist attack on a "choke" point, a technical failure, or any other cause, would bring about immediate shortages of supply. Aside from price spikes, an interruption in natural gas supply or electricity for several days would impact on systems as varied as food, education and government services as well as the health and safety of citizens—for example, those affected by inadequate heating in winter or air-conditioning in summer.

Interdependencies and infrastructure shared in common with the U.S. mean that disruptions can affect the economic prosperity and inflict severe hardships not only upon Canadian citizens but their American counterparts. The estimated costs of the 2003 electric blackout were between US$4–10 billion.[18] In Canada, gross domestic product (GDP) was down 0.7 percent in August; there was a net loss of 18.9 million work hours; and manufacturing shipments in Ontario were reduced by $2.3 billion.[19] The political repercussions of such an event could well prove to be of greater importance than the economic consequences if such events shift from being extraordinary to an increased frequency. A major loss of public confidence is likely to ensue if citizens feel that

---

[18] U.S-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout." Section 4.

[19] Statistics Canada, *Gross Domestic Product by Industry,* August 2003, Catalogue No. 15-001; *September 2003 Labour Force Survey; Monthly Survey of Manufacturing, August 2003,* Catalogue No. 31-001.

such occurrences are attributable to the inability or unwillingness of government to protect assets critical to their interests.

Canada's dependence upon the free-flow of goods, services and people across the border means that such a loss of assurance can quickly ignite cross-border tensions and precipitate U.S. actions which may be detrimental to Canadian interests. While the 2003 blackout was not attributable to any Canadian failure, it did highlight the degree of mutual dependency in terms of power generation and the need for both countries to commit to joint measures to enhance the security of energy transmission facilities. The blackout might have been averted, according to the Task Force Report[20] if the North American Energy Research Corporation (NERC) had been invested with more independent authority (from the industry it represents) to develop strong reliability standards and enforce compliance.

[20] "Final Report on the August 14, 2003 Blackout."

4 The Threats—"All Hazards"

The national infrastructure faces a wide range of physical threats: attacks by terrorists and other extremists, technical faults or failure of infrastructure, accidents involving hazardous materials, criminality (theft of equipment, materials, extortion, vandalism), industrial espionage and extreme weather, i.e., flooding or hurricanes. Certain threats are short term events such as natural disasters, but others such as the depletion of oil and gas resources are long-term trends. In addition, there are growing cyber threats from criminals, foreign agents, disgruntled employees and hackers.

Historically, planning and protective measures to secure national critical infrastructure in Canada have been premised on key infrastructure sites being targets for malicious attacks—terrorism, theft, vandalism, and commercial espionage—against which physical measures to secure sites and equipment were the deterrents. Otherwise, vulnerabilities were assessed from the perspective of incident response and consequence management under the incident category "all hazards" traditionally associated with safety and emergency management responses to flooding and other natural disasters rather than national security threats.

Little emphasis was given in Canada to the threat from terrorism until the 9/11 attacks in the U.S. which shifted attention from responding to emergency incidents towards preventing terrorism and protecting critical infrastructure against terrorist attacks. As time progressed, however, the term "all hazards" was expanded to give more weight to the potential consequences of other complex threats (e.g., pandemics). As the line between national security and emergency management (safety) became blurred, conceptually and functionally, it made sense to tackle security and safety together. Terrorism became one of many threats. For example, hostile states, terrorists, criminals and hackers all operate in cyberspace in ways which imperil not only national interests but also those of businesses and individuals. Criminals especially, but terrorists too, are exploiting the opportunities provided by the internet to increase the scope and impact of their (hitherto physical) activities. Thus "all hazards" now includes both the security and safety aspects of human-induced threats (intentional and accidental) as well as 'natural' and environmental threats and is a key element of the more comprehensive and integrated risk management approach to national security and emergency management which is set out in *Securing an Open Society: Canada's National Security Policy* April, 2004.[21]

The likelihood that preventing an attack might not be possible in the face of growing and emerging threats indicated the need for a more flexible and adaptable strategy for limiting the impact of disruptions to essential services as well as deterring potential attackers. An integrated response was perceived as a way of achieving an 'acceptable' level of protection against all threats more efficiently and effectively.[22]

---

[21] Privy Council Office, "Securing an Open Society: Canada's National Security Policy," April 2004. http://www.pco-bcp.gc.ca/docs/information/publications/natsec-secnat/natsec-secnat-eng.pdf.

[22] See Department of Homeland Security 2010 Budget Report which paraphrases a speech by President Obama's who takes the same position.

5 Energy Specific Threats

The criticality, high value and inherent vulnerabilities of energy infrastructure make it a potentially attractive target for terrorists, criminals, anarchists and single issue extremists groups. Not all groups present the same level of threat; in some cases *disruption* rather than *destruction* may be the objective; a demonstration of capabilities might suffice for some groups, whereas other groups may perpetrate violence with the intention of altering public policy. For example, a Canadian pleaded guilty in a U.S. court in March 2008, for plotting an attack on the Trans-Alaska Pipeline in order to profit from the expected rise in oil and gas futures.[23] A series of mysterious explosions in late 2008 to early 2009, targeted natural gas pipelines around Dawson Creek, in northern British Columbia. However, these ongoing, low level threats to Canada's energy infrastructure are essentially a law enforcement and public order problem.

The human-induced threats which are currently deemed potentially the most injurious to critical energy infrastructure in terms of potential impact are terrorism, cyber crime and cyber attacks. The energy sector is also susceptible to infrastructure failures and accidents—a category which includes industrial hazards such as the chemical spills that regularly occur and have the potential for significantly impacting public health and the natural environmental.

In its latest Public Report, the Canadian Security and Intelligence Service (CSIS) placed particular emphasis on the threat posed by Al-Qaeda and its affiliates to Canada's energy interests and infrastructure: "*Al-Qaeda...has warned that our country can expect attacks similar to those experienced in New York, Madrid, London...*" ... "*Additionally, Al Qaeda has identified Canada's oil industry as a target...*"[24] This is not a perception shared by most Canadians who, according to a recently commissioned survey, considered climate change to be a bigger threat to Canada's vital interests over the next ten years than terrorism.[25]

5.1 Terrorism

International terrorism, specifically violent Islamist terrorism, is a low probability/high impact threat to Canada's energy infrastructure. The risk from Al-Qaeda, its affiliates or the home-grown terrorists it inspires, derives from Canada's combat role in Afghanistan,[26] and its relationship to the U.S. in terms of geographic proximity and as a major energy supplier. Al-Qaeda has called for "economic jihad" against energy installations in the West in order to weaken their ability "to resist the Islamist onslaught."[27] As both a target in its own right and as a means of striking at American oil dependency, which Al-Qaeda has identified as America's greatest strategic

---

[23] Deborah Baker, "Canadian pleas guilty in pipeline plot," *Associated Press*, 13 March 2008.

[24] Canadian Security and Intelligence Service, *Public Report 2007-2008* (Ottawa: Public Works and Government Services, Canada, PS71-2008, 2009).

[25] Survey commissioned by the Canadian Defence and Foreign Affairs Institute: Canadian perceptions about threats critical to Canada's interests over next ten years. January 1010. http://www.cdfai.org/PDF/Poll%20on%20Threat%20Perceptions%20in%20Canada.pdf.

[26] Canadian Security and Intelligence Service, *Public Report 2007-2008*.

[27] Chris Zambelis, "Attacks in Yemen Reflect al-Qaeda's Global Oil Strategy," *Terrorism Monitor,* Vol. 6, No. 17, 4 September 2008.

vulnerability, Canada is susceptible to a major attack. Supply disruptions which raise oil prices serve Al-Qaeda's expressed aim of "bleeding America to the point of bankruptcy."[28]

Canada first appeared on a list of target countries in 2002.[29] In June 2004, Al-Qaeda in the Arabian Peninsula (AQAP) issued "The (Islamic) Laws of Targeting Petroleum-Related Interests and a Review of the Laws Pertaining to the Economic Jihad."[30] Its oil and natural gas facilities were later explicitly identified as potential targets when in February 2006, Al-Qaeda called for terror attacks on North American oil fields, pipelines, loading platforms and carriers as a means of disrupting services to the United States.

Primary targets in non-Muslim jurisdictions were identified as being oil and natural gas wells, pipelines, refineries and oil plants, and industry personnel. In February 2007, a further call encouraging the mujahideen to strike oil targets "in all areas which supply the United States" in order to choke the U.S. economy was made by AQAP in its publication, *Sawt-al-Jihad*.[31] The group was responsible for armed attacks on oil facilities in Yanbu and Khobar in Saudi Arabia in 2004 and for the assault on the Abqaiq oil processing complex in February 2006. The article was addressed not only to militants in the Arabian Peninsular but to jihadist cells in other energy producing and exporting countries.

Islamic extremist websites have identified specific energy installations as potential targets for attack, including the Trans-Alaska oil pipeline. Many miles of oil pipelines cross North America above ground and are impossible to protect day and night but the risk is mitigated to a large extent by the demonstrated ability of companies to carry out rapid repairs.

While the risk of direct physical attacks on infrastructure in Canada is acknowledged, the threat to personnel receives less attention. Furthermore evidence exists of a growing "insider" threat to sensitive government and business infrastructure by persons whose loyalty is ambiguous and who infiltrate, or who are suborned after recruitment, to serve Al-Qaeda's interests. The many examples which have been uncovered are consistent with the action plan proposed by al-Qaeda strategist Abu Bakr Naji and articulated as follows:

> (We) should infiltrate the police forces, the armies, the different political parties, the newspapers, the Islamic groups, the petroleum companies (as an employee or

---

[28] "Full Transcript of bin Laden's Speech," *Al Jazeera.net*, 30 October 2004.

[29] "Securing an Open Society: Canada's National Security Policy," April 2004, p. 6.

[30] Al-Qaida in Saudi Arabia: Excerpts from "The Laws of Targeting Petroleum-Related Interests," written by Shaykh Abdullah bin Nasser al-Rashid (aka Abdelaziz bin Rashid al-Anzi), Global Terror Alert, March 2006. See also: Jack Williams, "Al-Qaida Threats and Strategies: The Religious Justification for Targeting the International Energy Economy," CEIPPR Research Series No.3 – 2008.

[31] Adeeb al-Bassam, "Bin Laden and the Oil Weapon," *Sawt al-Jihad* (Voice of Jihad) *Muharram 1428 AH* February 2007, translated by the SITE Institute, Washington, D.C. See also, Stewart Bell, "Al-Qaeda affiliated website calls for attacks on Canadian Oil Industry," *National Post*, 9 February 2007; and Ian MacLeod, "Al-Qaeda Calls for Attacks on Canadian Oil Facilities," *National Post*, 14 February 2007.

> as an engineer), private security companies, sensitive civil institutions. (Abu Bakr Naji) [32]

Examples are legion: former US Navy sailor Hassan Abu-Jihaad was convicted of giving intelligence about naval movements—including of a Canadian warship—to potential jihadist enemies; the UK domestic intelligence service, MI5 unmasked Al-Qaeda sympathisers who attempted to join its ranks following a recruitment drive aimed at young British Muslims; and in Canada, recently-convicted Canadian-born terrorist Momin Khawaja worked as a software consultant at the Department of Foreign Affairs, Ottawa.[33]

Given that Al-Qaeda persists in its efforts to acquire weapons and materials of mass destruction—chemical, biological, radiological, or nuclear (CBRN)—the insider threat is of particular concern because of the possibility that these materials might fall into the hands of rogue states or terrorist groups.[34] While a physical attack on nuclear facilities is a risk despite protective measures, the theft of fissile and toxic materials from a nuclear site, chemical or biological facility is a greater one.[35] A UK Government report has noted that expertise acquired by insurgents in Afghanistan has increased the threat from a radiological "dirty bomb."[36]

These risks are mitigated to some extent by the stringent regulatory controls applied to nuclear facilities. Unlike other energy sub-sectors, nuclear power and uranium production exceptionally comes within federal jurisdiction because of its special characteristics and international treaty obligations even where provincial governments own the reactors.[37] The Canadian Nuclear Safety Commission (CNSC) derives authority to regulate security matters under the Nuclear Safety and Control Act (2000).

However, infiltration could result in a facility shut down if an "insider" has sufficient skills to sabotage control systems or if restricted access codes are compromised. Last year a former Arizona Palo Verde nuclear generating station engineer, Mohammad Reza Alavi, was convicted of taking restricted access codes to Iran, his country of origin.[38] The recent arrest in Yemen of Sharif Mobley, formerly a labourer at nuclear plants in New Jersey, caused alarm because of his

---

[32] Abu Bakr Naji, "The Management of Savagery," Trans. William McCants (Cambridge, Mass.: John M. Olin Institute for Strategic Studies, Harvard University, 23 May 2006). http://ctc.usma.edu/publications/pdf/Management_of_Savagery.pdf.

[33] For other examples see Marc Lebuis, "Islamism and the Infiltration Challenge," Civitas Annual Conference, 20 August, 2009, accessed at www.pointdebasculecanada.ca/article/1178-islamism-and-the-infiltration-challenge-by-marc-lebuisnbsp-2009-civitas-annual-conference.php.

[34] CSIS Public Report 2007-2008, p4.

[35] The International Atomic Energy Authority recorded 1,562 incidents where nuclear material was lost or stolen between 1993 and 2008, mostly in the former Soviet Union, and 65 percent of the losses were never recovered.

[36] Annual Update Report, 2010 to Contest II, the UK's Counterterrorism Strategy. http://www.statewatch.org/news/2010/apr/uk-nss-contest-annual-report-2010.pdf.

[37] John B. Hay, "Who Does What? Critical Energy Infrastructure Protection in the Canadian Government," *Critical Energy Infrastructure Protection Policy Research Series* (Ottawa: Carleton University, Canadian Centre for Intelligence and Security Studies, 2006).

[38] "American Spy for Iran Receives 15-month Sentence," *Associated Press*, 17 December 2008.

links to the radical extremist preacher, Anwar al-Awlaki[39] whose influence has contributed to acts of militant *jihadism* in the United States.

Lethal technologies, often dual-use, circulate easily in our globalized economy, as do the personnel with scientific expertise who design and use them. To reduce the associated risks, the government of the UK introduced the "Academic Technology Approval Scheme" (ATAS) in November 2007 which requires postgraduate students from non-European Union countries to be vetted by government officials. The scheme seeks to prevent the acquisition of knowledge or skills from British universities being used to build weapons of mass destruction (WMDs).

5.2 Environmental

Extreme weather events put a strain on power delivery systems. Generally speaking, the consequences of environmental threats are a matter of incident response, emergency management and adapting to environmental circumstances. Many regions of Canada have been subject to severe "natural disasters" which have taken lives and caused extensive property damage. Natural disasters encompass a variety of meteorological and geological hazards of which floods are the most frequent and the leading cause of property damage and death. Hurricanes, earthquakes and wildfires are also part of the natural hazard landscape and can result in the discontinuity of power supplies which in turn are likely to affect recovery efforts.

The issue is whether events such as the ice-storm which affected South-Eastern Canada in 1998 and cut off power supplies to millions are extremely low probability events, or whether there is sufficient actuarial evidence to indicate that investment in more robust infrastructure is needed to avoid the risk of a re-occurrence. Those who are convinced that climate change (perceived as being human-induced or exacerbated) is a significant contributor to the frequency or severity of traditional environmental threats, argue for more proactive measures to ensure the future resilience of society and its infrastructure.[40] They attribute inaction and the lack of concern about associated security risks to Canadian complacency, scepticism or confusion.[41]

Be that as it may, the immediate priority for policy makers is to rectify inadequacies in *current* provisions for protecting critical energy infrastructure and services against *known* risks—a calculus which must now also take into account the likelihood of attacks on the resource-based energy sector by radical activists who believe that environmental degradation will ultimately be detrimental to economic prosperity and human survival in the long-term.

---

[39] Peter Finn, "The Post-9/11 Life of an American Charged with Murder," *Washington Post*, 5 September 2010. Mr. Mobley had been in contact with Anwar al-Awlaki, the Yemeni-American cleric whose radical sermons have been found on the computers of more than a dozen terror suspects in the West and had recently been linked to the Nigerian man accused of attempting to bomb a jetliner bound for Detroit on Christmas Day, and Major Nidal Hasan, the army psychiatrist accused of killing 13 people at Fort Hood Texas in November, 2009.

[40] Cleo Pascall, "The Vulnerability of Energy Infrastructure to Environmental Change," Chatham House Energy, Environment and Resource Governance, April 2009, EERG BP 2009/01. The study calls for the design, location and retrofitting of infrastructure for changing environment conditions.

[41] Margaret Purdy and Leane Smythe, "From Obscurity to Action," *International Journal*, Vol. 65, Issue 2, Spring 2010 p.414.

Opposition to environmentally destructive and water-polluting Canadian oil-sands production could threaten the reliability of Canada's future energy exports to the United States. To date, U.S. policy has supported oil-sands production but this may not continue to be the case indefinitely if at some point that policy comes into conflict with a U.S. water and food security policy which prioritizes access to uncontaminated water supplies.

5.3 Cyber Attacks

Cyber security is at the forefront of the trans-border challenge to Canada's critical infrastructure. Since cyberspace knows no borders, defensive efforts must be similarly seamless. Protecting the cyber links and IT services which connect and control critical infrastructure is much more complex than protecting physical assets because of the fragmented nature of the ownership and regulatory control of the global cyber domain.

Sophisticated state-led cyber espionage or warfare is a serious issue but easier to deter when the adversary is a state with an easily identifiable government and location than when cyber attacks are carried out by surrogates, criminals, terrorists and hackers who cannot readily be traced. These attackers also exploit cyber space for their own ends and their activities pose a real threat not just to state interests but to ordinary individuals and businesses across Canada. Confidence in government can be undermined if cyber attacks target and shut down government websites causing a denial of service.

While the assessment of some analysts is that terrorists operating under the umbrella of Al-Qaeda are more likely to opt for a high profile physical attack which inflicts mass casualties or the destruction of infrastructure, cyber attacks which cause prolonged disruptions rather than physical casualties can wreak massive economic damage of the sort which Al-Qaeda has called for in terms of its "economic jihad." Nevertheless, choke points in the data and communications part of the NCI could be a tempting target for a physical attack.[42]

FBI Director Robert Mueller has referred to "numerous denial-of-service attacks" by Al-Qaeda terrorists and other extremists and suggests they have an "eye toward combining physical attacks with cyber attacks."[43] According to The Centre for the Protection of National Infrastructure, (CPNI), a UK Government Agency, "large scale" electronic attacks by foreign intelligence services have successfully compromised the security of many large British companies in operations aimed at stealing government, defence and technology information.[44] Islamist terrorists were also said to be behind internet attacks which, although limited in scope, were on the increase.

Power supply chains can be subverted by the implantation of malicious programs into software. Recent attempts to hack into the shared U.S.-Canada electrical grid comprising high-voltage transmission lines which span 340,000 kilometres and serve 334 million people, did not damage

---

[42] A view supported by MI5, the UK's Security Service. The data underpinning London's role as an international financial centre is stored in the Dockland area and would provide such a target.

[43] The Federal Bureau of Investigation, "The Cyber Threat' Headline Archives," 4 March 2010. http://www.fbi.gov/page2/mar10/cyberintel030410.html

[44] "Foreign Intelligence Services Hack into British Companies," *Daily Telegraph* (London), 12 March 2010.

the power grid or other key infrastructures but intruders left behind software which, according to U.S. officials, could be used to disrupt the system at some future date—for warfare purposes or commercial advantage.[45] Similar intrusions have been detected, not by the companies in charge of the infrastructure, but by U.S. intelligence agencies concerned about cyber attackers taking control of electrical facilities, a nuclear power plant or financial networks via the Internet.[46]

There are no known similar "embedded" threats to the Canadian portion of the international power network, but growing reliance on Internet-based communications has increased the vulnerability of control systems to the activities of criminals, spies and hackers. Almost all critical industrial infrastructures and processes are today managed remotely from central control rooms using computers and communications networks. Understanding and mitigating the risks of electronic attack to SCADA systems is a key issue for infrastructure protection.

The worst-case scenario is that a cyber attack could override controls at a chemical or nuclear plant and cause a chemical release or nuclear meltdown. However, where there is such a risk, control systems are generally disconnected from networks that connect to the Internet. While an "insider"[47] who understood the control software for an electric grid could pose a threat, such skills are not widely available and the vulnerability can be reduced by adherence to good personnel practices and access control procedures.

Protecting the electrical grid and other infrastructure is a key part of the Obama administration's cyber security strategy and it was mentioned in Canada's *National Security Policy* (2004).[48] Despite a statement by (then) Public Safety Minister Peter Van Loan regarding the need for the Canadian government to create "an overall cyber-security strategy" which encompasses both the public and private sectors, it has not yet been published. Former Canadian ambassador to Washington, Derek Burney, believes that the Canada-U.S. power grid is probably a primary cyber target and urges a more robust defence for computer systems.[49]

Reducing the vulnerabilities of cyber networks is complicated by the fact that while more than 90 percent of the physical infrastructure of the Web is owned by private industry, key elements of cyber security expertise lie within federal government. On its own, neither side can ensure the continuity and integrity of the infrastructure.

---

[45] Siobhan Gorman, "Electricity Grid in the US Penetrated by Spies," *Wall Street Journal*, April 2009. The attacks are believed to have been perpetrated by China or Russia but attribution has not been confirmed.
[46] Ibid.
[47] For example, a disgruntled employee or someone who becomes disaffected for religious or ideological reasons.
[48] "Securing an Open Society: Canada's National Security Policy," p. 26.
[49] "CEIP: Canada and US legislation to protect its power grid against cyber-attack," *Ottawa Citizen*, 22 November 2009.

6 Managing the Risks to Canada's National Critical Infrastructure

Identifying specific physical assets of national importance and developing plans to protect them is the traditional, defensive response to site specific threats. Protective security measures aim to reduce physical, personal, technical and communications vulnerabilities by providing mutually reinforcing security layers for national infrastructure. They include security by design and other site hardening measures which seek to strengthen the robustness and resilience of buildings, installations and equipment against attacks or natural events, e.g., building redundancy capacity is a way of accommodating equipment failure or destruction, and ensuring business continuity. Physical and cyber access controls, security clearances and personnel practices aim to prevent unauthorized visitors, system users and identify disaffected staff.

This "guards and gates" approach to national security is still the first line of defence for key installations but it is now considered to be just one of the strategies available for reducing vulnerabilities and contributing to the assurance of critical infrastructure within a comprehensive risk management effort to assure national critical infrastructure against all threats and *across all sectors*. The focus of Canada's integrated approach to *national* security now with respect to securing critical infrastructure is on improving resilience (preparedness and recovery), supply assurance (continuity of essential services), and mitigation measures (minimizing the impact). National security risks are treated as just one part of an integrated 'all-hazards' risk management system.

Reducing vulnerabilities to natural disasters traditionally focuses on incident response and consequence management. The primary responsibility for the protection of critical infrastructure at the local level rests with the owners and operators who are responsible for day-to-day protective measures and ongoing risk assessments. Identifying and managing the risks to their critical infrastructure assets, services and systems allows scarce resources to be allocated where they are most needed to prevent, mitigate and recover from security and emergency management events.

The expertise, local knowledge and motivation to protect their own assets, investments and reputation makes owner/operators better suited to the task than any government authority and they may also have access to resources and expertise not always available to the public sector. Developing the necessary "situational awareness," or understanding of the risks, will be foremost a site or service specific exercise, but a comprehensive approach includes examining risks to the sector as a whole and the critical infrastructure community more broadly. This is done in consultation with and assistance from federal, provincial and territorial authorities (FPT).

The aim of evaluating and assessing the risks from a comprehensive "all-hazards" approach is to ensure adequate levels of protective security for all critical infrastructure, (depending upon the impact caused by the failure of particular assets and services), minimal points of failure and rapid, tested recovery arrangements. The assumption that the synergies derived from a common approach to all threats will provide the necessary level of protection for each is questionable, but attractive given the reality of finite security budgets and an acceptance that preventing attacks may not always be possible when confronted with numerous and sometimes unknown threats.

Reliance on an integrated approach for delivering protection against all-hazards, including terrorism, is premised on the assumption that vulnerabilities across the spectrum of risks can be reduced to an "acceptable" level by enhancing resilience to improve recovery capabilities and mitigation measures to reduce impacts. As the 2008 Emergency Management Framework for Canada states, "assessing the risks associated with all hazards in an integrated way, may be broadly effective in reducing the vulnerability of people, property, the environment and the economy."[50]

In an integrated "all-hazards" risk management system, emergency management decisions, particularly those concerning resource allocation, are invariably risk-based, or risk informed by the construct that risk is the product of threat, vulnerability and consequence (R = T x V x C). While logically intuitive and consistent with conceptualizations of risk in other domains, this approach is less applicable to low probability/high impact national security threats where invariably no actuarial data is available for calculating the risks, i.e., terrorism. Owners and operators are unlikely to invest in specific prevention and protection measures against such risks and therefore an "undersupply of security" is likely without some regulatory provincial or federal intervention. Some risks are so catastrophic that "disproportional" countermeasures might be warranted, i.e., to prevent terrorists using CBRN materials.

Risk-based decisions which assess the likelihood and potential impact of a range of different risks to specific assets are helpful to owners of specific assets because they are familiar with their normal operating conditions (their baseline) and can apply their risk assessment to it. But given the range of viable, credible threats against any of the currently defined CI sectors, assessing risks in the context of an "all-hazards" approach is less meaningful because understanding the interdependencies within and between sectors and managing cascading risks requires a common measurement for mapping CI interdependency. Lacking this, the allocation of resources for CI protection will be determined by data which is incomplete and inadequate for assessing the impact of current vulnerabilities and emerging threats.

The specific data necessary for managing the risks by assessing the impact of current vulnerabilities or emerging threats is not always available.

[50] Public Safety and Emergency Preparedness Canada, 'An Emergency Management Framework for Canada' 2008. http://www.publicsafety.gc.ca/prg/em/emfrmwrk-eng.aspx, accessed on 30 March 2010.

7 Government Response to Emerging Threats

In March, 2001, ministers responsible for energy matters from Canada, Mexico, and the United States met to discuss a common hemispheric energy strategy for the three North American Free Trade Agreement (NAFTA) countries. The outcome of these trilateral discussions was the drafting of an energy annex to the North American Security and Prosperity Partnership (SPP) agreement which committed signatories to the protection of the critical energy infrastructure deemed vital for North American economic well-being.

7.1 Post 9/11 Perceptions, Reorganization, Legislation

Terrorist attacks against the U.S. on September 11th 2001 increased the focus on the threats from international terrorism and brought about a shift from a culture of emergency management and safety to one of security. The attacks were the catalyst for change and reorganization within Canadian federal government departments and agencies but anti-terrorism legislation, (aimed primarily at facilitating the detection, detention and prosecution of terrorists), was introduced as much to reassure U.S. authorities that its interests were being satisfactorily protected in Canada than because there was any real conviction that Canada itself was a target. Nevertheless, any perceptions that Canada was a potential launching pad for attacks against the U.S. had to be dispelled[51] if the free flow of goods and people across the shared border, vital to Canada's economic prosperity, was to be preserved.

A National Security Advisor to the Prime Minister was appointed and new cabinet committees created, including one for security, public health and emergencies, to oversee among other files infrastructure protection. A Government Operations Centre was established in 2004 to serve decision-makers as a central collection and communications repository of information from federal departments, agencies, provinces, territories and other countries, including the United States.

Reorganization brought together security and law enforcement organizations under the newly created department of Public Safety and Emergency Preparedness Canada (PSEPC)—the Canadian analogue to the Department of Homeland Security in the U.S. Critical energy infrastructure assurance was to be achieved through protective measures focused on key facilities and enhanced emergency preparedness and mitigation management.

[51] Ahmed Ressam's attempt to blow up Los Angeles Airport was foiled by a border guard when he crossed into the U.S. from Canada on 14 December 1999.

7.2 Smart Border for the 21st Century Declaration, December 2001

To improve security on their shared border, Canada and the U.S. signed the *Smart Border for the 21st Century* Declaration on December 12, 2001[52] which aimed to find a workable balance between security and the free flows of trade and people across the border. Included in its Action Plan was an undertaking to "conduct bi-national assessments on trans-border infrastructure and identify additional protection measures…" that might be necessary. Comprehensive threat and vulnerability assessments on shared cross-border critical infrastructure (especially energy) were to be based on "a spectrum of potential threats."

7.3 Public Safety Act, 2002

The Public Safety Act (2002) and a number of legislative amendments[53] were enacted to provide Regulators with a clear statutory basis for regulating the *security* as well as the safety aspects of interprovincial and international energy assets[54] a change necessitated by a growing realisation that oil, gas and nuclear/electrical power facilities were attractive, high value/high impact targets for terrorists.

7.4 The Integrated Threat Assessment Centre (ITAC)

The Integrated Threat Assessment Centre (ITAC) was created in 2004 as an interdepartmental agency for assessing predominantly terrorist threats. It was established after difficult and protracted negotiations between participant departments protective of their own analytic authority. ITAC prepares and distributes its assessments to other parts of government and law enforcement. In effect, these are the same organizations which supply ITAC with the raw intelligence upon which its assessments are based.

7.5 Natural Resources Canada

Natural Resources Canada (NRCan) was assigned federal responsibility for policies relating to critical energy infrastructure protection (CEIP), including terrorism, in 2002. Constitutionally natural resources fall mostly under *provincial* jurisdiction, however, that authority is limited to "in Province" activities only. Federal authority therefore covers energy infrastructure and related

---

[52] The Smart Border for the 21st Century Declaration which the US and Canada signed on 12 December 2001 was to be implemented through a 30-point action plan which aimed to secure infrastructure, secure the flow of goods and people across the border, and enhance information sharing and cooperation.

[53] The new law amended the Criminal Code, the Official Secrets Act and other legislation in order that terrorist threats could more effectively be identified, investigated and prosecuted. It also provided for the ratification of the Suppression of the Terrorist Financing Convention and the Suppression of Terrorist Bombings Convention (which contains specific provisions against attacks on infrastructure.) The *Public Safety Act, 2002* amended the National Energy Board Act by extending the powers and duties of the National Energy Board to include matters relating to the security of pipelines and international power lines.

[54] For example, oil and gas pipelines, offshore oil and gas facilities, international power lines and nuclear facilities.

matters of national security which cross inter-provincial boundaries and international borders. From a policy perspective, a systems approach is adopted by the federal authority which tracks the point of production/generation (of oil, natural gas and electricity) to the point of distribution/consumption. The Minister's powers, and those of the Regulatory "Portfolio Agencies" derive from a number of sources, as detailed in section 11 below.

Soon after the events of 11 September 2001, NRCan established the Energy Infrastructure Protection Division (EIPD) to implement its mandate. EIPD provided a central point of contact for energy sector owners and operators across Canada and established a reputation nationally for being pro-active in developing initiatives in pursuit of it six main tasks which included collecting, analyzing and sharing information among energy sector stakeholders.

As the lead interlocutor with the U.S. Department of Energy, EIPD was involved with bi-national assessments of shared critical energy infrastructure and represented NRCan on North American Working Groups. It was required to liaise with federal and provincial governments, regulatory agencies, the energy industry and its associations and to promote initiatives to strengthen Canada's critical energy infrastructure.

As John Hay commented, "taken together, these initiatives marked a dramatic redirection of government energies towards security and intelligence priorities—and towards a more coherent management of Canada-US relations."[55] Although some progress was made and PSEPC established a cross-Canada program for providing appropriate assurance for national critical infrastructure assurance in 2002, initiatives regarding the protection of critical infrastructure stalled thereafter.

7.6 National Critical Infrastructure Assurance Program—Discussion Paper 2002

The National Critical Infrastructure Assurance Program (NCIAP) made it clear that the traditional site specific, physical approach to protecting the national infrastructure was to be superseded by a more integrated approach which recognized "a need to focus instead on the overall systems and networks that make up the National Critical Infrastructure and, more importantly, on the associated interdependencies."[56] The purpose of the NCIAP was "to provide a national framework for cooperative action and to build a resilient national critical infrastructure."[57] This was to be done through collaborative public/private sector partnerships. Work was begun on developing a strategy in which would include "voluntary participation from industry stakeholders as well as federal, provincial and territorial governments."

The assurance program introduced the concept of "all-hazards" and it provided a formal definition of "national critical infrastructure" (NCI); furthermore, it identified six NCI sectors (these were later increased to ten). Defining them presented a challenge due to the increasing

---

[55] John B. Hay, "Who Does What? Critical Energy Infrastructure Protection in the Canadian Government," p. 12.
[56] Public Safety and Emergency Preparedness Canada, "The Creation of the NCIAP," 2002.
[57] Public Safety and Emergency Preparedness Canada, (PSEPC) National Critical Infrastructure Assurance Program, (Ottawa: PSEPC, 2002).

dependence on information systems and networks of all CI, the possibility of cascading effects resulting from interdependencies, Government ownership and operation of only a small share of the NCI and the challenges of 'borderless' cyberspace.

Previous consultations with owners and operators regarding the production of a *master list* of National Critical Infrastructure (NCI) had raised concerns regarding the ownership and protection of the list and associated information. As a consequence the focus henceforth was to be on coordinating the efforts of all stakeholders to provide assurance that their *combined* efforts would result in a resilient and viable NCI. Two general elections and a change of Liberal leadership were to take place before a "Position Paper" on critical infrastructure would be released in 2005.

8 An Integrated Approach to Emerging Threats

As the trauma of 9/11 receded, security authorities gained more experience and developed a better understanding of the global dimensions of newly emerging threats and vulnerabilities. In 2004, the most extensive formal statement on national security ever made by a Canadian government was published which stated that while Canada had a system in place with respect to *terrorism,* whereby government shared threat information with first responders, law enforcement officials, critical infrastructure providers and provincial and territorial governments, it intended to "expand its capacity to ensure full connectivity on a wider range of threats to create a truly national system of protection and prevention."[58]

Terrorism was henceforth to be treated as one of many threats, and national security incidents were to be viewed as one part of a modern integrated strategy for emergency management of all-hazards in which the federal government would play an enhanced role. Federal entities would be required to work together in a more coordinated way and to develop closer links with emergency operations at the provincial, territorial and local levels. The statutory framework for the Government's emergency management activities, in particular, the Emergency Preparedness Act (1985), was to be reviewed and updated (The Act was later repealed upon assent of the Emergency Management Act (2007)). The Government acknowledged that existing national emergency coordination suffered from the absence of both an effective federal-provincial-territorial governance regime, and from the absence of commonly agreed standards and priorities. Federal entities were henceforth required to work together in a more coordinated way and to develop closer links with emergency operations at the provincial, territorial and local levels.

Critical infrastructure protection was identified in the document as one of the main challenges. Reference was made to work that had begun "to drive forward a national process that prioritizes substantial improvement of our national capabilities in critical infrastructure protection."[59] A "Position" paper was eventually released in 2005[60] which contained proposals for a National Strategy for Critical Infrastructure which would establish a basis for federal, provincial and territorial governments and the private sector to meet that challenge (see Summary at Annex B). Protection of assets was just one of the strategies available to better secure critical infrastructure.

Public Safety Canada (the successor to PSEPC) was described as the lead department in protecting the government's own infrastructure, but more than that, it was to be "the focal point for the integration of CIP activities, strategic coordination, and national level policy development and integration… (as well as) for coordinating, analyzing and sharing threat and vulnerability information, (cyber and physical)." Ten key critical infrastructure sectors were identified (see Annex A) and federal departments were designated to head each sector. Natural Resources Canada, supported by the Canadian Nuclear Safety Commission (CNSC), International Joint Commission (IJC) and the National Energy Board (NEB), were to be responsible for "Energy and Utilities."

---

[58] "Securing an Open Society: Canada's National Security Policy," 2004.
[59] Ibid.
[60] "Government of Canada Position Paper on a National Strategy for Infrastructure Protection."

Key elements of the strategy were set out in the paper which described a continuum of activities but the paper failed to clarify how these activities would be integrated and guided by a national-level capacity. Hay remarked that "its treatment of practical governance issues—who should do what—remained cursory and vague."[61] By early 2006, no strategy had been approved. Under the newly elected Conservative government, priorities had changed and an alteration in the cabinet committee structure meant that infrastructure protection was now handled by a cabinet committee on foreign affairs and national security. Nevertheless, in January 2007, federal, provincial and territorial ministers agreed to adopt a comprehensive all-hazards approach to emergency management which would incorporate its four functions: prevention and mitigation, preparedness, response and recovery.

[61] Hay, "Who Does What? Critical Energy Infrastructure Protection in the Canadian Government."

9 "Working Towards a National Strategy and Action Plan for Critical Infrastructure," 2008

The latest iteration of a critical infrastructure strategy for Canada was issued in 2008 by Public Safety Canada in a draft paper entitled, *Working Towards a National Strategy and Action Plan for Critical Infrastructure.*[62] If approved, the strategy will focus primarily on improving emergency preparedness, supply assurance, and mitigation management. While optimists are hopeful that a comprehensive and clear strategy aimed at securing critical infrastructure and enhancing business resilience is finally about to emerge, sceptics question whether this latest strategy and action plan will achieve any more than its predecessors given the amount of time which has elapsed since it was first mooted.

The draft strategy builds upon the principle of subsidiarity, where primary responsibility for critical infrastructure remains with private and public sector owners and operators; it is an "all-hazards" approach to emergency management and focuses on critical infrastructure which is of *Canada wide* importance. The integrated action plan is structured on federal coordination of the efforts of other stakeholders in a collaborative approach which would aim to improve information sharing among all participants and thereby enhance protection. Greater consistency and coherence would be achieved through the development of cooperative partnerships at home and abroad. Collaboration and information sharing are key elements.

Public Safety Canada describes its own role as leading and coordinating the activities of other actors across all CI sectors[63] to develop a more comprehensive, coherent, cross-Canada approach for securing critical infrastructure. Officials have indicated that they are working on the implementation of the Strategy pending formal approval. (The main points are summarized at Annex C).

As the line between security and safety incidents has become blurred, so there is recognition that a more integrated approach which bridges jurisdictional divisions is needed to enhance the efficiency and effectiveness of measures to protect and strengthen the resilience of Canada's critical infrastructure. Present priorities place emphasis on Cyber-security and Critical Energy Infrastructure Protection (pending approval of the proposed National Strategy and Action Plan).

[62] "Working Towards a National Strategy and Action Plan for Critical Infrastructure," 2008.
[63] Ibid., p. 4.

10 The Governance Framework

When the Conference Board of Canada asked public and private sector leaders to identify the greatest threat to national security and public safety in Canada, the responses focused not on natural disasters, terrorism, cyber-attacks or pandemics but instead identified the lack of clarity around governance as the greatest threat.[64] In a 2006 study for the Canadian Centre of Intelligence and Security Studies at Carleton University, John Hay observed that, despite the post 9/11 reorganization "it is still not altogether clear who in the federal government does what" in terms of responsibility for the protection of infrastructure. How authority is exercised with respect to policy approval and resource acquisition is a critical factor in terms of a government's ability to fulfill its declared strategy aims. In developing an appropriate governance framework for the protection of critical infrastructure, the federal government must confront the fact that since threats respect neither national, sectoral, nor jurisdictional boundaries, an effective response will need to be equally seamless. Given Canada's constitutional arrangements, achieving a collaborative, participative and integrated approach involving *all* stakeholders is likely to be a long and difficult process, fraught with jurisdictional tensions. But any failure in direction and control or in the relationships among the numerous actors involved could intensify the impact of a national security or public safety incident.

Where there are multiple stakeholders, regulatory authorities and different levels of government, each required to engage collaboratively in the security and emergency management aspects of critical infrastructure and related mitigation and resilience issues, a clear and undisputed lead department with the necessary powers of direction and control will be crucial. Good governance further requires that there be shared principles and agreed mandates, clear terms of reference, coordination mechanisms and accountability protocols in place as part of the policy approval and resource acquisition road map. If these are lacking, there will be confusion about roles and responsibilities; how expressed "concerns" can be prioritized at all levels of government; and which individuals and organizations are to be held accountable for policy implementation. Arguably, it has been the inability to address these issues which have caused the extensive delays in formalizing a national strategy for critical infrastructure protection in Canada.

---

[64] Trevor Munn-Venn and Andrew Archibald, *A Resilient Canada: Governance for National Security and Public Safety*, (Ottawa: Conference Board of Canada, November 2007).

11 National Leadership—CEIP

The Emergency Management Act (2007) affirmed federal authority over critical infrastructure protection. It stipulates that the role of the Minister of Public Safety is to 'exercise leadership relating to emergency management by coordinating federal emergency management activities among federal departments and agencies, and in cooperation with the provinces and territories' and "to provide advice and to analyze and evaluate federal departmental emergency management plans, which include critical infrastructure protection." Although constrained by the constitution, the federal government has a duty to ensure the continuity of essential services and systems, make them more resistant to disruption and better able to recover. Federal involvement is focused on those events and circumstances that generally require a *national* response.

The same Act designated Public Safety Canada the lead federal department, answerable to the Minister, with respect to the protection of national critical infrastructure. Through legislation and policy, it is responsible for leading, by coordinating, the management of emergencies among federal departments and agencies, and coordinating the protection of critical infrastructure. Canadian federal authorities are empowered to respond to all hazards including acts of terrorism but only have statutory powers to intervene in incidents, other than terrorism, which have a *national* security interest if they cross provincial, territorial or international boundaries although provinces can elicit federal assistance on a case-by-case basis. Exceptionally, nuclear power and uranium production comes under federal jurisdiction.

In late 2009 the Auditor General questioned whether Public Safety Canada was able to identify emergencies that are beyond the capacity of other players and coordinate emergency management activities given that no *formal* framework at the national level linking the federal government with the owners and operators of critical infrastructure existed.[65] Furthermore the Interim Federal Emergency Response Plan did not include "updated or completed definitions of the roles, responsibilities, and capabilities needed for an integrated, coordinated approach to emergency response." In 2010, Public Safety Canada issued a National Strategy for Critical Infrastructure (dated 2009) which did little more than outline future aspirations.

11.1 Federal Departments Responsibility for National Critical Infrastructure

All federal Departments have mandates and roles which govern their response to particular emergencies. The Royal Canadian Mounted Police (RCMP) would be the primary federal response agency for an incident involving terrorist or criminal acts; Natural Resources Canada is the primary subject matter expert for a natural event causing a power outage. However, lead departments with subject expertise are responsible for each of the critical infrastructure sectors. Statutory or regulatory powers vested in these key federal line departments can be exercised only in respect of infrastructure which crosses inter-provincial boundaries or international borders.

---

[65] "Emergency Management—Public Safety Canada," Chapter 7 in *Report of the Auditor General of Canada to the House of Commons* (Ottawa , Fall 2009), esp. pp. 9-18.

11.2 Natural Resources Canada

The Minister of Natural Resources derives authority from a number of pieces of legislation i.e. the Department of Natural Resources Act (1994), National Energy Board Act (1985), Canada-Nova Scotia Offshore Petroleum Resources Accord Implementation Act (1988), and Energy Supplies Emergency Act (1985). As the lead federal department for the Energy and Utilities sector NRCan is supported in the exercise of its responsibilities by the portfolio agencies—Canadian Nuclear Safety Commission (CNSC), The International Joint Commission, (IJC), the National Energy Board (NEB), The Canada-Newfoundland and Labrador Offshore Petroleum Board and the Canada-Nova Scotia Offshore Petroleum Board. NEB, CNSC, CNLOPB, and CNSOPB are required to report to Parliament through the Minister. They derive their authority through separate specific Acts and Regulations.

Those functions formerly carried out by the Energy Infrastructure Protection Division, (EIPD), were allocated to various parts of NRCan's energy sector branch in 2009 when the EIPD ceased to exist, for reasons not made explicit. NRCan supported PSEPC in the formulation of the first discussion document which underpins the current strategy for critical infrastructure. Although the Emergency Management Act (2007) designated Public Safety Canada the lead agency at the federal level, the absence of any previous effective overarching central coordination meant that pro-active departments had already developed their own initiatives for the protection of critical infrastructure and were using different critical risk assessment methodologies. While Public Safety Canada has started to develop guidance to promote a consistent approach, this has yet to be finalized or distributed to those departments designated to lead the ten critical infrastructure sectors.[66]

A number of other federal departments may become involved in an emergency incident if it escalates or spreads. In such cases, Public Safety Canada has a coordinating role in helping to communicate and receive information about the current situation to other departments and agencies and to senior officials in the federal government and other jurisdictions. Although reference has already been made to the Government Operations Centre, the Canadian government does not yet have in place a centralized clearing house for information pertaining to critical energy infrastructure protection for its own departments and agencies, or for sharing with other jurisdictions.[67]

11.3 Regulatory Bodies

Regulatory agencies are key players in matters relating to critical energy infrastructure protection within their jurisdiction. Their role in support of the Minister's responsibility for safety and security is exercised in accordance with Canada's security policy and goals. The National Energy Board Act (1985) was amended in 2005 to provide the regulator (i.e., NEB) with a clear legislative mandate for addressing issues related to the security of critical energy infrastructure such as international power lines and international and inter-provincial oil and gas pipelines.

---

[66] Auditor General's Report, 2009.
[67] Ibid.

The North American Energy Reliability Corporation (NERC) is a non-governmental entity whose mission is to ensure that the bulk electric system in North America is reliable, adequate and secure. It was established in 1968 as a result of the Northeast blackout in 1966. NERC has operated as a voluntary organization, relying on reciprocity, peer pressure and the mutual self-interest of all those involved to ensure compliance with reliability requirements. However, some NERC standards and processes were deemed inadequate in connection with the 2003 failure and the Task Force Report[68] noted that if NERC had had the authority to enforce mandatory compliance with the standards the blackout might have been averted.

[68] US-Canada Power System Outage Task Force, p. 17.

12 Information Sharing and Collaboration

Information sharing and collaboration between the public and private sector and the various tiers of government are key strategic objectives of the proposed national strategy for critical infrastructure. Besides fostering closer relationships and a better mutual understanding between the various stakeholders, the federal government needs help in identifying the criticality of different infrastructure and its vulnerabilities, while owners and operators need information in order to provide appropriate protection for the nation's infrastructure. Effective two-way exchanges of sensitive information will only be possible once trusted partnerships are established and a "responsibility to provide" culture has become engrained across the private and public sectors. Various initiatives have been launched to foster confidence and to remove legal and bureaucratic impediments.

Energy sector owners and operators have been reluctant to share with federal authorities information about critical infrastructure that might identify vulnerabilities or aspects of their business which could give competitors an advantage. The Access to Information Act (1985) has therefore been amended to encourage them to share network information—on a controlled basis—without fear of disclosure to third parties. This has not yet been tested in the courts. Under the Emergency Management Act, Section 8, Deputy Ministers are authorized to withhold information received from third parties, e.g., owner/operators. Conversely, owners and operators need information from central authorities, especially about particular security threats. NRCan sponsored security clearances for approximately 200 industry representatives so that they could attend bi-annual classified briefings on the threats delivered by members of the Canadian Security and Intelligence Community and other experts.[69] This was to assist them in adopting appropriate security enhancement measures. Information which enhances local understanding about the threats is one thing; actionable intelligence which is sufficiently specific and timely to prevent or pre-empt them is another. Managing expectations about what the central agencies have to offer will be the challenge.

Regular meetings between industry and government officials have been convened and horizontal collaboration encouraged across the sectors with federal, provincial and territorial authorities. NRCan has facilitated information sharing between government departments, intelligence and security agencies, with international allies, and with regulators and energy sector stakeholders. It has co-hosted regular fora on pipeline security with its American counterparts and joined with industry associations in mounting professional conferences and meetings on issues of shared concern. Private and public sector owners/operators in the energy sector have established their own organizational mechanisms for information sharing and cooperation in the management and mitigation of threats. For example, the electric power industry has set up ten regional "reliability councils" across the U.S. and Canada, headed by (NERC) for the setting and enforcing of reliability and performance standards. Similar mechanisms exist for other energy sectors, including oil and natural gas producers and pipeline operators.

---

[69] The Hon. Gary Lunn, former Minister of Natural Resources, addressing the 2007 International Pipeline Security Forum, 24 October 2007, Ottawa—"We have sponsored over 200 industry representatives in obtaining Secret Level II security clearance. This enables us to share information with industry and their associations so that the appropriate security enhancement measures can be adopted."

12.1 International Partnerships

Since Canada's energy economy is part of a North American energy hemisphere Canada's energy policy must not only be "rational and national" but international. North American energy policy is formalized to some degree by Canada/U.S. bi-lateral and Canada/U.S./Mexico tri-lateral and NAFTA agreements, but cooperative informal relationships are responsible in large part for advancing mutual objectives. Informal arrangements such as information and alert exchanges between owners and operators and their industry associations on both sides of the border have been invaluable. However, the vital importance of protecting energy security from emerging threats suggests that there may be a need to bring more bilateral structure and organization to the task.[70]

In the event of an imminent cyber threat, no single U.S. government entity currently has sufficient authority to issue emergency orders to the private-sector bulk power industry. Two current congressional bills in the U.S. propose assigning much of that power to the Federal Electricity Regulatory Commission (FERC), as well as giving it authority to order the power industry to upgrade operational security standards. Although the Canadian power-utilities association and the broader NERC support the proposal that FERC become the lead authority during an emergency, they oppose granting FERC the power to impose new and presumably tougher security standards since this would mean that FERC would be determining operating standards in Canada—a jurisdictional sovereignty issue. A bi-lateral agreement is preferred.

NRCan's *Energy Sector Reporting* service, which was once available through the Internet to selected stakeholders, comprised current updates on incidents, government reports and other important open-source documentation pertaining to energy security. It is no longer available although Public Safety Canada produces a *Daily Infrastructure Report* comprising summaries of emergency management information concerning critical infrastructure.[71] NRCan has sponsored a series of published research studies on various energy related topics: an information-sharing initiative which has served to build capacity. The importance of academic outreach has been emphasized by the US Department of Homeland Security which looks to academic research to develop knowledge about vulnerabilities and emerging threats[72] and create the skill sets needed for future homeland security professionals.

The draft strategy seeks to encourage the establishment of sector networks for each of the critical infrastructure sectors based on existing coordination and consultation mechanisms. At a minimum these would provide a forum for sector discussions and information exchange between key members of the private and public sectors analogous to those which exist in the U.S. which bring together various industrial groups into a consultative arrangement with government through dedicated Information Sharing and Analysis Centers (ISACs). The Energy and Utilities sector is currently the only one in operation. To promote information-sharing across the sector networks

---

[70] "U.S. grid-security measures may hurt Canadian companies," Homeland Security Newswire, 25 November 2009.

[71] The *Public Safety Canada Daily Infrastructure Report* is accessible at: http://www.publicsafety.gc.ca/dir/dir09-040-eng.aspx?rss=false.

[72] Remarks made by speakers at the 4th Annual Homeland Defense and Security Education Conference, Washington, 24-26 February 2010.

and address cross-jurisdictional issues, Public Safety Canada proposes to establish a Cross-Sector Forum.[73]

[73] "Working Towards a National Strategy for Critical Infrastructure," p. 5.

13 Conclusion

> …the Government of Canada focuses its efforts both on improving ways to provide protection where it is reasonable, and also on ways to assure the continued provision of essential services to Canadians. Protection and assurance can be achieved through better information collection, assessment and sharing, and through risk management. Both protection and assurance are ongoing objectives that the Government of Canada seeks.[74]

How is Canada doing with respect to the protection and assurance of critical energy infrastructure? Space precludes a comprehensive review, but the long delays in the emergence of a formal strategy for both critical national infrastructure and cyber are clear indications that there are problems. The challenge to existing mandates and responsibilities, the absence of good governance and leadership and a period of political turmoil, may explain why, so long after the first attempts to build a national framework for cooperative action, "the strategy to do this is still in draft form and the critical infrastructure that needs to be protected has not yet been determined."[75] There is a long way to go yet before Canada's integrated strategy is in place and the collaborative relationships on which it depends are established. The Auditor General has observed that "Public Safety has not exercised the leadership necessary to coordinate emergency management activities, including critical infrastructure protection in Canada."[76] Part of the difficulty in meeting its goals, it was suggested, was the high turnover in the senior ranks of Public Safety.

No *national* critical infrastructure assets or services have yet been identified or agreed with the various owners/operators and federal, provincial and territorial authorities nor is there any legislation which requires them to do so. Yet as Jacques Shore points out there is a legal imperative on the part of both government and private enterprise to protect critical infrastructure.[77] Canada's integrated approach to preventing or mitigating potential threats builds on existing relationships rather than challenging the status quo: it aims to encourage and facilitate a more cohesive, coordinated effort by all stakeholders and in that sense is essentially passive and reactive.

Developing protective security measures and incident response plans for national critical infrastructures necessarily involves "*trans-boundary thinking*" from the outset. A "containment" response to an incident will not be adequate. Prevention and planning must include the assumption that there will be cascading effects and these must be identified. Response strategies which engage the whole of government from the inception will entail thinking through the jurisdictional and legal ramifications and conflicts, and developing approaches that are anticipative, flexible, adaptive, and respect the rule of law.

---

[74] "National Strategy for Critical Infrastructure Protection," 2004.
[75] "Report of the Auditor General of Canada to the House of Commons," p. 2.
[76] Ibid.
[77] Jacques J. M. Shore, "The Legal Imperative to Protect Critical Energy Infrastructure," *Critical Energy Infrastructure Protection Policy Research Series* (Ottawa: Carleton University, Canadian Centre for Intelligence and Security Studies, 2008).

Martin Rudner has suggested a more pro-active approach which would involve adopting a counterintelligence mentality and an intelligence-led strategy to prevent destructive adversaries from attacking and penetrating national CI assets and services.[78] The aim would be to identify, deter and prevent threats, but since there will always be protective gaps, measures to enhance resilience are also necessary.

[78] Martin Rudner, "Protecting Critical Energy Infrastructure Through Intelligence," *International Journal of Intelligence and Counter Intelligence,* Vol. 21, No. 4, Winter 2008-2009.

This page intentionally left blank.

Annex A National Critical Infrastructure Sectors

The 10 sectors that form the basis of the NCIAP and sample sub-sectors for each sector[79] are the following:

1. Energy and Utilities
Electrical power (generation, transmission, nuclear)
Natural gas
Oil production and transmission systems

2. Communications and Information Technology
Telecommunications (phone, fax, cable, satellites)
Broadcasting systems
Software
Hardware
Networks (internet)

3. Finance
Banking
Securities
Payments System

4. Health Care
Hospitals
Health-care facilities
Blood-supply facilities
Laboratories
Pharmaceuticals

5. Food
Food safety
Agriculture and food industry
Food distribution

6. Water
Drinking water
Wastewater management

7. Transportation
Air
Rail
Marine

---

[79] 'Working Towards a National Strategy and Action Plan for Critical Infrastructure' (2008).

Surface

8. Safety
Chemical, biological, radiological, and nuclear safety
Hazardous materials
Search and rescue
Emergency services (police, fire, ambulance and others)
Dams

9. Government
Government facilities
Government services (for example meteorological services)
Government information networks
Government assets
Key national symbols (cultural institutions and national sites and monuments)

10. Manufacturing
Chemical industry
Defence industrial base

Annex B Summary: Government of Canada Position Paper 2004

1. **Guiding Principles**: five guiding principles (awareness, integration, participation, accountability and all-hazards) will influence the development of the national CIP strategy.

2. **Risk Management**: use the integrated risk management (IRM) framework as a starting point when developing the national CIP strategy.

3. **Information Sharing**: promote and support timely and accurate information sharing across jurisdictions and CI sectors. This will require establishing working groups with participants at all levels and conducting stakeholder consultations, including with international partners, to determine: the nature of the information required; the most appropriate vehicles to exchange the information; and to increase interoperability.

4. **Inventory of CI Assets**: identify and assess its own CI. In addition, the Government of Canada will work with other levels of government and the private sector to ensure that processes are in place to identify their critical infrastructures (or components thereof) as a measure to strengthen public safety and as part of good business practices, and that all associated information be protected to the fullest extent of the law.

5. **Threats and Warnings**: continue to improve mechanisms to quickly and effectively communicate relevant information and intelligence on threats to CI to stakeholders.

6. **CI Interdependencies**: interdependency analysis must be integrated into risk management decisions, mitigation and preparation strategies, and response and recovery activities. In addition, the Government of Canada will coordinate national efforts in interdependency research and development, which is essential to understanding this issue.

7. **Governance Mechanisms**: establish a governance architecture that will result in national direction and coordination of CIP activities. To this end, the Government of Canada will establish a CIP national body, and where appropriate mechanisms within sectors and to address horizontal and regional issues.

8. **Research and Development**: conduct targeted research projects and leverage Canadian and international science and technology capabilities in order to address gaps in knowledge, build national capacity, and to create innovative solutions for CIP.

9. **International Cooperation**: participate in international CIP initiatives and to strengthen information-sharing mechanisms and operational linkages with other countries and international organizations.

Source: Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection (2004) p.12.

Annex C "Working Towards a National Strategy and Action Plan for Critical Infrastructure" (2008)

Purpose: Strengthen the resilience of critical infrastructure in Canada by "setting the direction" against current and emerging hazards. [see definition of critical infrastructure on page 1 of this study]

Objectives: To enhance resilience

- Build trusted and sustainable partnerships
- Implement an all-hazards risk management approach; and
- Advance the timely sharing and protection of information among partners.

Primary responsibility for critical infrastructure remains with private and public sector owners and operators but to co-ordinate their efforts, the integrated action plan proposes a *collaborative* approach the aim of which would be to improve information sharing among participants and thereby enhance protection.

Classification of Critical Infrastructure: The National Strategy proposes that "critical infrastructure efforts" be aligned across ten sectors and also across the various jurisdictions. The ten sectors as follows:

> Communications, Emergency Services, Energy, Finance, Food, Government, Health, Transportation, Water, and Manufacturing.

Guidance: The Plan provides guidance on the identification of risk, the implementation of protective measures and effective responses to disruptions of critical infrastructure.

Public Safety Canada has been designated to lead and co-ordinate these collaborative efforts across all CI sectors. Its role is described in the paper as being to develop a more comprehensive, coherent, cross-Canada approach for protecting all critical infrastructure by leading and coordinating the activities of other actors within a collaborative framework.

Distribution list

Document No.: DRDC CORA CR 2010-274

Internal

Internal

1 DDG [PDF via email]
1 Section Head Strategic Analysis [PDF via email]
1 Library [print and CD]
1 Johnston PF [PDF via email]
---
1 print TOTAL PART 1
1 CD TOTAL PART 1

External

1 ADM(IE) [PDF via email]
1 Canada Command/D Comd [PDF via email]
1 DRDC CSS/DG [PDF via email]
1 SJS/DG Plans [PDF via email]
1 DRDC DSTIC [PDF via email]
1 CFD/DFSA [PDF via email]
1 ADM(Mat)//DF&L [PDF via email]
1 SJS/DSOA [PDF via email]
1 ADM(Pol)/D Strat A [PDF via email]
1 CDI/Director Regional Intel [PDF via email]
1 Author [PDF via email]
1 DRDKIM [CD]

---

1 CD TOTAL PART 2

1 print TOTAL REQUIRED
2 CD

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Angela Gendron
Canadian Centre for Intelligence and Security Studies
The Norman Paterson School of International Affairs
Carleton University

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Critical Energy Infrastructure Protection in Canada:

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Angela Gendron

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
December 2010	57	79

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – CORA
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
10aa09	W7714-093788

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
Contractor's Document Number:	DRDC CORA CR 2010-274

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Various government Ministers have affirmed the importance government attaches to the protection of critical energy infrastructure. Nine years after the attacks on September 11, 2001 first focused attention on the potential vulnerability of infrastructure and the economic, social and political consequences of a failure of assurance, a strategy has still not been approved and the assets requiring protection not yet identified. While due respect must be given to the jurisdictional authorities which have been established by the Constitution, international terrorism and newly emerging global threats such as electronic attacks on IT and communication systems have only increased the urgency for Canada to have in place a proactive, seamless system for the protection of those energy assets and services which are so vital to Canada's well-being and prosperity, and North American security. The effectiveness of the draft Strategy and Action Plan proposed by Public Safety Canada will depend upon the voluntary participation of the various public and private sector stakeholders and the extent to which a culture of information sharing and collaboration can be inculcated. Arguably, this is a passive and reactive Plan which gives insufficient attention to deterring and preventing malicious attacks on infrastructure.

Plusieurs ministres ont affirmé que le gouvernement attache beaucoup d'importance à la protection des infrastructures énergétiques essentielles. Neuf ans après les attaques du 11 septembre 2001 aient pour la première fois attiré l'attention sur la vulnérabilité potentielle des infrastructures et les conséquences économiques, sociales et politiques de notre incapacité à assurer leur sécurité, une stratégie n'a toujours pas été approuvée et les actifs ayant besoin d'être protégés n'a toujours pas été identifiée. Bien qu'il soit nécessaire de respecter les compétences de juridiction définies par la Constitution, le terrorisme international et les menaces qui ont commencé à émerger au niveau mondial—tels que les attaques électroniques contre les systèmes de TI et de communication—n'ont fait qu'accroître l'urgence pour le Canada de mettre en place un système proactif et transparent de protection de ces actifs producteurs d'énergie et des services énergétiques qui sont si essentiels à la prospérité et au bien-être du Canada ainsi qu'à la sécurité de l'Amérique du Nord. L'efficacité de l'ébauche de la Stratégie et plan d'action en matière d'énergie proposée par Sécurité publique Canada dépendra de la participation volontaire des différents intervenants des secteurs public et privé et de notre capacité à inculquer une culture de collaboration et de partage de l'information. Il est sans doute permis de penser qu'il s'agit d'un plan passif et réactionnel qui accorde une attention insuffisante à la dissuasion et à la prévention d'attaques malveillantes contre les infrastructures.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

All-hazards Risk; Anti-terrorism; Critical Energy Infrastructure Protection (CEIP); Critical Infrastructure; Critical Infrastructure Protection; Critical National Infrastructure; Cyber-attack; Cyber-security; North American Free Trade Agreement; SCADA; Terrorism.

Defence R&D Canada

Canada's Leader in Defence and National Security Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière de science et de technologie pour la défense et la sécurité nationale

DEFENCE R&D DÉFENSE

www.drdc-rddc.gc.ca

s.19(1)

Dvorkin, Corey

From: Dick, Robert
Sent: June-30-11 1:44 PM
To: Champoux, Martin
Cc: Maillé, Marie Anick; Dvorkin, Corey; Hatfield, Adam; Filipps, Lisa; Fergusson, Janis; Eke, Darren; Stanfield, Charles; DeJong, Michael
Subject: RE: For DG approval: Media Lines-Network World Canada

fine

From: Champoux, Martin
Sent: June 30, 2011 11:32 AM
To: Dick, Robert
Cc: Maillé, Marie Anick; Dvorkin, Corey; Hatfield, Adam; Filipps, Lisa; Fergusson, Janis; Eke, Darren; Stanfield, Charles; DeJong, Michael
Subject: For DG approval: Media Lines-Network World Canada
Importance: High

Robert

Industry Canada (IC) and Public Safety have received a media call from [redacted] of Network World Canada. He was asking about an IC advisory group for the telecom sector, the Canadian Security Telecommunications Advisory Committee. IC provided him with the information found below. Based on this information, the journalist would now like to know the following:

In a cyber security context, what is PS's role in this Advisory Committee? Is somebody in PS attending these meetings as an observer or with some other status? If nobody from PS is attending is there a mechanism by which PS is informed of the Advisory Committee's work (briefing notes, records of decision, etc)?

After discussion with Marie Anick, I have prepared the following media lines for your approval:

- **Public Safety Canada's Assistant Deputy Minister for Emergency Management and National Security is a permanent member of the Canadian Security Telecommunications Advisory Committee (CSTAC).**

- **Our work with CSTAC is in keeping with Public Safety's leadership role in cyber security and critical infrastructure protection.**

- **Canada's Cyber Security Strategy (www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx) and the National Strategy and Action Plan for Critical Infrastructure (http://www.publicsafety.gc.ca/prg/em/ci/index-eng.aspx) provide more information about the Government of Canada work in cyber security and critical infrastructure protection.**

Industry Canada

Canadians are increasingly relying on the privately-owned and operated telecommunications networks as a foundation for a digital economy and society. Industry Canada is currently developing a digital economy strategy and recognizes that the security and availability of the telecommunication infrastructure is essential to economic growth and national security. Circuit-switched infrastructure has provided decades of robust and secure telecommunications. However, the next generation packet-based technologies and networks have inherent vulnerabilities, and networks have become both an attractive target and vehicle of attack.

As such, Industry Canada, the telecommunications industry and other government departments on November 23rd, 2010 established the Canadian Security Telecommunications Advisory Committee (CSTAC). The purpose of the CSTAC is for senior executives in the public and private sectors to exchange information, to collaborate strategically on current and evolving issues that may affect the confidentiality, integrity or availability of the telecommunications infrastructure and to provide advice on measures to address these issues. It will focus on issues related to the security and resiliency of the Canadian Public Telecommunication Networks (PTN), such as:

- Risks to the critical telecommunication infrastructure;
- Proactive and mitigating measures to address threats and vulnerabilities;
- Network monitoring;
- Emergency management;
- Interdependencies;
- Disaster recovery; and
- Other pertinent topics.

Members of the CSTAC will bring forward its advice for consideration within their respective organizations. CSTAC collaboration may also result in the development of white papers, technical reports and best practices.

The CSTAC will also support the Government's efforts under the Canadian Cyber Security and the National Critical Infrastructure Protection Strategies. Both Strategies recognize the importance of partnering with industry to ensure systems vital to Canadian security, economic prosperity and quality of life are protected. The CSTAC is similar to advisory committees established in other countries, such as the US National Security Telecommunications Advisory Committee (NSTAC).

Martin Champoux
Senior Communications Advisor | Conseiller principal en communications
Communications Directorate | Direction générale des communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-5967
Fax | Télécopieur : 613-993-7062
Email | Courriel : Martin.Champoux@ps-sp.gc.ca

Journal of Military and Strategic Studies

VOLUME 14, ISSUE 2, 2012

The Government of Canada and Cyber Security: Security Begins at Home

John Adams

Computers and information systems have become a fundamental part of Canadian life. Life, commerce and statecraft have gone digital. The associated information technology underpins nearly all aspects of today's society. They enable much of our commercial and industrial activity, support our military and national security operations and are essential to everyday social activities.

Data collection, processing, storage, and transmission capabilities are increasing exponentially. The interconnected networks, to include all levels of government, where billions of people are linked together to exchange ideas and services are known as cyberspace. Cyberspace is now conventionally used to describe anything associated with the Internet.

In today's global community, national security is not assured by having control over an area within recognized borders, it is dependent upon having the ability to navigate through the global commons. These commons – sea, air, space and cyberspace – facilitate the functioning of the global economy[1]. Technologically advanced societies are becoming increasingly dependent upon the rapid and reliable transmission of ideas, information and data. A vast amount of data is constantly in motion and an

[1] Murphy, Tara. "Security Challenges in the 21st Century Global Commons", Volume 5, Issue 2, 2010, Yale Journal of International Affairs, available at http://yalejournal.org/2010/07/page/2/.

ISSN : 1488-559X

astronomical quantity is being stored. Furthermore, owing to market incentives, innovation in functionality is outpacing innovation in security and neither the public sector nor the private sector has been successful at fully implementing existing best practices. Consequently, data is vulnerable be it at rest or in motion. The potential for malicious activity is endless. National, commercial and industrial security are therefore threatened.

Canada is in Love With the Internet

Table 1: Proportion of Canadians using the Internet[2]

Online Landscape Worldwide in 2010

Canada maintained its position as the most engaged online audience ranking highest among the top markets in average hours and visits per visitor in Q4 2010.

			#1		#2		#1	
	Total Unique Visitors (000)		Average Hours/Visitor		Average Pages/Visitor		Average Visits/Visitor	
Location	Q4 2010	Q4 2009	Q4 2010	Q4 2009	Q4 2010	Q4 2009	Q4 2010	Q4 2009
Worldwide	1,314,031	1,206,146	23.1	23.7	2,133	2,252	53.0	54.6
China	287,451	232,037	13.5	15.6	1,238	1,599	38.6	57.7
U.S.	181,239	172,194	35.3	33.3	2,953	2,822	80.9	70.8
Japan	72,913	69,826	18.4	20.0	1,928	2,108	43.8	47.3
Germany	49,257	45,216	24.1	22.0	2,858	2,654	60.0	58.7
Russia	45,692	36,589	21.8	16.5	2,704	2,399	52.9	44.5
France	41,827	39,137	26.6	28.1	2,752	2,934	68.7	70.3
India	41,170	36,535	11.9	12.1	1,089	1,183	30.6	27.1
Brazil	39,335	32,849	25.8	27.0	2,089	2,672	56.5	58.8
UK	38,581	37,674	32.3	31.3	2,883	2,735	69.4	60.3
South Korea	30,155	29,424	27.7	35.6	4,093	4,986	50.1	72.5
Canada	22,945	23,138	43.5	42.2	3,349	3,793	95.2	88.8

[2] http://blog.suitcaseinteractive.com/2011/03/comscore-report-sows-that-canucks-are-internet-usage-stars/

Canadians spend more time on the Internet than anyone in any other country, and the amount of time they spend online is nearly double the worldwide average, 43.5hrs/month versus 23.1[3].

And the potential for continued growth is high. People aged 55 and older are now the fastest growing demographic of Internet users and now accounts for 1 in 5 Internet users[4].

And there is virtually no aspect of Canadians' lives that is not touched by the Internet[5].

[3] Thomas, Knowlton. "Trends and Stats: Canadians use the Internet more than anyone else in the world", Mar 9, 2010, available at http://www.techvibes.com/blog/trends-and-stats-canadians-use-the-internet-more-than-anyone-else-in-the-world-2011-03-09

[4] Ibid.

[5] Statistics Canada," Online activities from any location (% of internet users), Wednesday, October 12, 2011, available at http://www.statcan.gc.ca/daily-quotidien/111012/t111012a3-eng.htm

Table 2: Online activities from any location (% of Internet users)

	2010
	%
E-mail	93
Window shopping or browsing for information on goods or services	74
Electronic banking (e.g., paying bills, viewing statements, transferring funds between accounts)	68
Reading or watching the news	68
Travel information or making travel arrangements	65
Visiting or interacting with government websites	65
Searching for medical or health-related information	64
Using social networking sites	58
Researching community events	54
Using an instant messenger	47
Downloading or watching movies or video clips online	47
Obtaining or saving music (free or paid downloads)	46
Searching for employment	37
Formal education, training or school work	37
Listening to the radio online	37
Obtaining or saving software (free or paid downloads)	35
Playing online games	33
Downloading or watching TV online	33
Researching investments	27
Making telephone calls online	24
Selling goods or services (e.g., through auction sites)	19
Contributing content or participating in discussion groups (e.g., blogging, message boards, posting images)	19

In 2010, 51% of Internet users ordered goods or services for personal or household use. In total, Canadians placed in the order of 114M orders, valued at approximately $15.3B[6].

[6] Ibid.

The average Canadian visits nearly 100 different websites over a three-month period, more than double the worldwide average of 42. 25M Canadians used the Internet in the last quarter of 2010.[7]

And the beat goes on. Worldwide tablet shipments rose more than 56% quarter over quarter at the end of 2011 to over 20M units, according to the International Data Corporation (IDC). That marks a 155% boost year over year, IDC says. 2011 saw just under 70M units shipped in total. In 2012 IDC expects more than 100M units to be shipped.[8]

An obvious impact of the digital world's evolution is evident in the near-total sea change with respect to how we communicate. In the order of 90% of Canadians use email at least weekly.[9] Furthermore, the "digital native" generation is going to change how the world does business, according to Symantec CEO and President, Enrique Salem.[10]

Salem describes "digital natives" as people typically born in the 1990s who have never known a time before the Internet or smart mobile devices. Where the previous generation welcomed email into its business practices, these "natives" are entirely comfortable with a constant staccato of texting and messaging as a key means of communication. As a group, their social fabric is interwoven with media such as Facebook, LinkedIn and Twitter, and individuals' cyber security practices may be affected by shifting attitudes towards online privacy.

To "digital natives", there's no distinction between the Internet at work and the Internet at home. Thus, the trend we see emerging – primarily thanks to "digital natives" – is "BYOD" or Bring Your Own Device to work, blurring the lines between personal life and work.

---

[7] techvibes Op. cit.

[8] Poeter, Damon. "IDC: Strong Q4 IPads, Android Tablet Sales Push 2012 Forecast Upwards", March 13, 2012, available at http://www.pcmag.com/article2/0,2817,2401531,00.asp

[9] Internet World Stats: Usage and Population Statistics (Canada), available at http://www.internetworldstats.com/am/ca.htm#links

[10] King, Rachel. "Symantec CEO: 'Digital Natives' will change the way we do business", February 23, 2012, available at http://www.zdnet.com/blog/btl/symantec-ceo-digital-natives-will-change-how-we-do-busiess/70395?tag=content;siu-container

This will introduce more vulnerabilities that will clearly impact on the way we do business Salem suggests. It will add to the cyber challenge.

The Threat

Let me at the outset of this section spend a few minutes on terminology. I will start with "cyber- attack". It is an umbrella term for several types of cyber related activities, each of which has different motivating factors:

- "Hacktivism" is a cyber- attack motivated by political activism that often involves defacing a website for the explicit purpose of publically shaming the target;
- "Cyber- crime" may involve using cyber attack as a means, but its sole motivation is to gain financially from the attack;
- "Cyber- espionage" is using cyber attack methods to covertly access information of national interest belonging to others;
- "Cyber- terrorism" is the systematic threat or use of violence, often across national borders, to attain a political goal or communicate a political message through fear or intimidation of non-combatant persons or the general public.[11]

Threats from cyber-espionage, computer crime and attacks on critical infrastructure will surpass terrorism as the number one threat facing the United States, FBI Director, Robert Mueller testified before the Senate Select Committee on Intelligence on 31 Jan 2012.[12]

"I do not think today it is necessarily [the] number one threat, but it will be tomorrow." Mueller said. "Counter-terrorism – stopping terrorist attacks – with the FBI

---

[11] Czinkota, M. R., Knight, G. A., Liesch, P. W., and Steen, S. (2005) Positioning Terrorism in Management and Marketing: Research Propositions. Journal of International Management, 11(4), pp. 581-604.

[12] Associated Press, "FBI Director Robert Mueller Talks Cyber Security: We must Find a Way to Stop the Bleeding", January 3, 2012, available at http://www.huffingtonpost.com/2012/03/01/fbi-director-robert-mueller-cybersecurity_n_1315112.html

is the present number one priority. But down the road, the cyber threat, which cuts across all [FBI] programs, will be the number one threat to the country."

United States' officials estimate that there are 60,000 new malicious computer programs identified each day.[13] This past June, the computer security firm Symantec released a report on a Trojan Horse[14] program dubbed "Sykipot".[15] "The Sykipot attackers have a long running history of attacks against multiple industries. Based on these insights, the attackers are familiar with the Chinese language and are using computer resources in China. They are clearly a group of attackers who are constantly modifying their creation to utilize new vulnerabilities and to evade security products and we expect that they will continue their attacks in the future." Symantec noted.

In the past several years, there has been a growing list of complex computer breaches that highlight the wide array of threats:

- The high-profile intrusions of Google's Gmail in 2009 also targeted as many as 30 other high-tech companies including Yahoo, Adobe, Rackspace and Northrop Grumman. US officials believe China was attempting to gain access to these firms' networks to obtain intellectual property and source code information.

- China is also believed to have hacked into computer systems run by `NASDAQ-OMX, the parent company of the NASDAQ stock exchange, and to have executed an intrusion last year into computers at the International Monetary Fund.

- Last year RSA, the security division of the EMC Corp., suffered a breach of the firm's intellectual property, SecureID, which provides encrypted authentication services to defence contractors and the US government, including the FBI. Officials say Chinese entities compromised the RSA

---

[13] Ryan, Jason. "FBI Director Says Cyber Crime will Surpass Threat from Terrorists", January 31, 2012, available at http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/

[14] Trojan Horse: A standalone malicious program designed to give full control of an infected personal computer to another computer.

[15] http://www.net-security.org/malware_news.pld?id=1975

Secure ID system to try to break into computers used by defence contractor Lockheed Martin.

- In 2007, Russia waged cyber-attacks against computer systems in Estonia and United States (US) officials have also cited Russia using cyber-capabilities in the conflict between Russia and Georgia in 2008.

- Non-state entities, such as Anonymous, a loose coalition of web-based "hacktivists", have wreaked havoc recently with distributed denial of service attacks against the websites of the US Justice department, Universal Music, the Motion Picture Association of America, the Recording Industry Association of America and the FBI. Anonymous also has conducted sophisticated intrusions, breaching the computer systems of government contractor HB Gary, a cyber security firm, in early 2011. In that incident, they downloaded more than 50,000 emails from the firm and posted private information about the CEO on his own Twitter account.

- Canada's Public Safety Minister, Vic Toews, was the latest in a string of public-policy targets to feel the wrath of Anonymous, who went after the minister for his approach in promoting the Government's online surveillance bill.[16]

Impact on Canada

Nearly two thirds (63%) of Canadian users reported having experienced a computer virus at one point in the past. Of those who had experienced a virus, almost one half (49%) said that the virus (or viruses) resulted in the loss of information or damage to software.[17]

---

[16] National Post Staff, "Anonymous revives Vikileaks, targets Vic Toews over online surveillance bill" http://news.nationalpost.com/2012/02/20/vic-toews-anonymous-hackers/

[17] Statistics Canada, "Individual Internet use and E-commerce", Wednesday, October 12, 2011, available at http://www.statcan.gc.ca/daily-quotidien/111012/dq111012a-eng.htm

Over one third (37%) said they had received emails requesting personal information (such as bank account numbers or passwords) from a fraudulent source.[18]

These numbers are not surprising in that hacking isn't rocket science and needn't cost a fortune. An off the shelf desktop computer can test anywhere between one and fifteen million passwords per second. It would crack a password from a dictionary in less than1 minute. A strong random password could be cracked in less than 15 minutes. The same computer, in combination with an off the shelf graphics processor can speed up the cracking process by a factor of 50 to 100.[19]

The threat issue is compounded by the fact that Canadians, despite being enthusiastic users of the technology, typically know very little about the Internet. The Canadian Internet Registration Authority released a report this past November entitled "The Internet and Canada's Future Opportunities and challenges". Some of the published results are revealing:

- 32% of Canadians could not identify a challenge faced by individual users of the internet;
- 18% claimed there are no challenges;
- among the clever half, 9% cited a lack of digital literacy and 7% cited slow Internet connection speed.[20]

Compared to counterparts in the US and the United Kingdom (UK), Canadians demonstrate a greater willingness to publish and share their personal details and stories online. As an example, the National Director of Facebook Canada this year produced statistics on uptake in our country: nearly half of all Canadians actively participate on Facebook.[21] It is no wonder, then, that Canada's Privacy Commissioner has been keenly

---

[18] Ibid.

[19] Password Cracking Wikipedia, available at http://en.wikipedia.org/wiki/Password_cracking

[20] Thomas, Knowlton. "Half of Canadians Don't Have a Clue About the Internet" November 10 2011, available at http://www.techvibes.com/blog/half-of-canadians-dont-have-a-clue-about-the-internet-2011-11-10

[21] Breikss, Chris. "Mind Blowing Canadian Facebook Usage Statistics", May 3, 2011,available at http://www.6smarketing.com/canadian-facebook-statistics

interested in Facebook's privacy practices and has effectively challenged the popular giant on its compliance with Canadian law.[22]

Yet basic security is not uppermost in the minds of most Canadian Internet users. Speaking of IT security more generally, most Canadians only change their passwords every 2-5 years. Up to 30% report that they never change their passwords.[23]

Furthermore, in general, only 25% of smartphone owners use the auto-lock feature to protect their mobile devices. Less than 10% of people currently using their own tablets for work have "auto-locking" enabled. Barely 30% of lap top owners use the "auto-locking" feature.[24]

Security firm Sophos has warned that malware writers and cyber criminals will switch their focus to the now more popular smartphones. While such attacks will target all smartphone operating systems, Android – which is becoming increasingly popular – is particularly vulnerable because of the way patches are distributed.

"Google will issue patches for vulnerabilities to network providers, who will decide when to make it available to users," said Mark Harris, global director of Sophos Labs.

"Many of those users won't be accustomed to patching their systems, which could mean an awful lot of users running versions that contain vulnerabilities," he added.[25]

So we have a rich target with robust attackers using readily available commercial off-the-shelf products and having considerable success in taking advantage of the target. Consider the following, between 2010 and 2011:

---

[22] Office of the Privacy Commissioner, News Release, "Facebook shows improvement in some areas, but should be more proactive on privacy when introducing new features", April 4, 2012, available at http://www.priv.gc.ca

[23] http://www.symantec.com/region/can/eng/press/200

[24] King, Rachel. "Most smartphone, tablet owners not concerned with locking devices: report", zdnet, March 26, 2012, available at http://www.zdnet.com/blog/btl/most-smartphone-tablet-owners-not-concerned-with-locking-devices:report

[25] Morgan, Gareth. "SOPHOS warns of rising Android malware threats in 2012", vs.co.uk, January 26, 2-12, available at http://www.v3.co.uk/v3-uk/news/2141640/sophos-warns-rising-android-malware-threats-2012

- There were 286 million unique variants of malware that exposed and potentially exfiltrated our personal, confidential, and proprietary data;
- Each data breach exposed, on average, 260,000 identities;
- There was a 93% increase in web-based attacks (compromised/hijacked websites where the visitor would become infected);
- The underground economy paid anywhere from $.07 to $100 for each of our stolen credit card numbers;
- Realizing that mobile payments and mobile platforms (e.g., smart phones and iPads) would be the newest vector of technology adoption, there was a 42% increase in mobile-operating-system vulnerabilities and subsequent exploitation.[26]

An issue that warrants a few words is the idea of the Internet as a "force multiplier".[27] It is, in fact, an excellent force multiplier. There is virtually no personal, physical risk incurred by an Internet attacker. There are no geo-spatial boundaries on the Internet, nor are there behavioural rules. There are no threats to the attacker who can use unpredictable techniques and is very difficult to find as he/she hides in plain sight among billions of users. The attacker is also able to recognize when their practices and techniques have been compromised and regularly change these to avoid detection.(Recall the "Sykjpot" Trojan Horse referred to earlier.) An individual could simply run a program from his/her home computer that could cause extensive interruption or damage to the computer systems that our governments increasingly rely on.

It is important to understand that cyber- attack's ability to do harm is not limited to damaging electronic information. For example, there are some power distribution control rooms that run supervisory control and data acquisition (SCADA) systems. Rather than have an engineer on site, operating engineers can log in via the Internet to do their work remotely. The danger here is that a "hacker" may break into a SCADA

---

[26] Symantec Internet Security Threat Report: Trends for 2010, Volume 16, April 2011.

[27] Force Multiplier; Refers to an attribute or a combination of attributes which makes a given force more effective than that same force would be without it.

system and use it to damage, destroy or cripple the power distribution of a potentially large area. This represents a very real risk to critical infrastructure.

The Government of Canada (GOC) has not been spared. What has been seen more and more in recent years, particularly through the lens of our national cryptographic agency, the Communications Security Establishment Canada (CSEC), are attempts at cyber espionage and the presence of malicious emails on GOC networks.

Acts of espionage to clandestinely access the secrets of others is nothing new. The use of spies or various forms of intelligence to access a state's political, military and economic secrets or a company's industrial and business secrets have been practiced since time immemorial. Cyber-espionage is ultimately the same as traditional espionage: the covert access of information of national interest belonging to others, only accessed electronically.

The threat to Canada's security, and to the security of our allies, is much greater than it might appear to be at first glance. More than 100 countries are capable of conducting cyber operations against technologically advanced countries such as Canada. The attempts are constant and relentless. Many countries are prolific, unconstrained by resource, legal, or policy limitations. With our advanced economy, connected government services, important international role and our proximity to the United States, Canada is an extremely attractive target. And as we experienced in January/February 2011 in the case of Treasury Board and the Department of Finance, undetected compromises can be both expensive and time consuming to address, to say nothing of lost productivity in the meantime.

The potential for harm to our way of life through the exploitation of the Internet is boundless. States, organized crime, terrorists, and individuals use the Internet for a range of illegal activities. They attempt to steal our industrial and national security secrets and our personal identities and they work relentlessly to penetrate our critical infrastructure networks, potentially disrupting our daily lives and forcing us into costly clean up.

And the implications do not stop there. They could lead to our closest allies questioning whether we are the weakest link to their own information infrastructures.

The compounded impact of these activities is a very real threat to the sovereignty of our nation on the cyber front.

Government of Canada Approach

The GOC has a critical and unique role. It is responsible for the defence of Canada's physical and economic security, in addition to being the guardian of sensitive national security, economic and personal information. It must therefore lay the foundation upon which Canada's defence of its cyber livelihood will be built.

But the GOC cannot do this alone. They do not control all things critical to national security. For example, other levels of government and industry control approximately 85% of Canada's critical infrastructure[28], providing energy, and water and essential services such as police, medical care, financial services and air traffic control. They also store sensitive personal and economic information.

National security and critical infrastructure are not the only concerns. As has been made clear above, large commercial organizations are prime targets for cyber attacks. And our adversaries, be they state actors, criminals or non-state actors, have aggressively targeted them, thereby threatening our economic prosperity.

The GOC has devised a cyber strategy[29] that will provide the leadership and guidance that will ensure a coordinated approach, both domestically and internationally, to all aspects of cyber security.

The three pillars of the strategy are founded on:

- securing government systems;
- partnering to secure vital systems outside the GoC; and
- helping Canadians to be safe online (public awareness).

---

[28] Canada's Critical Infrastructure: When is safe enough safe enough? Andrew Graham. The MacDonald Laurier Institute, National Security Strategy for Canada Series, Volume 2

[29] Public Safety Canada, Canada's Cyber Security Strategy, available at http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx

Security

Clarity of roles and responsibilities is the first intent of the Strategy. It is a whole of Government approach and it is a complex web. Public Safety Canada will provide central coordination for assessing emerging complex threats and developing and promoting comprehensive and coordinated approaches to address risks within the GOC and across Canada.

An indication of the evolving breadth and complexity of GoC roles and responsibilities can be drawn from both the Cyber Security Strategy and the IMP, with the latter reflected in Annex A.

Any discussion of securing government systems must start with the Communications Security Establishment Canada (CSEC). Their mandate, inter alia, states that the CSEC is:

> to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructure of importance to the Government of Canada.[30]

CSEC's technical knowledge and capacity to fulfill this mandate is assisted by the fact that they are also mandated:

> "to acquire and use information from the global information infrastructure (GII) for the purposes of providing foreign intelligence, in accordance with Government of Canada intelligence priorities."[31]

While an aside, it is important to note that CSEC's multi-faceted mandate is bound by a robust authorities framework, designed to maintain focus on GOC priorities while taking measures to protect the privacy of Canadians. Further, these unique activities are subject to review for lawfulness by the CSE Commissioner[32].

I highlight these particular responsibilities because the second compliments the first, and this combination gives CSEC a distinct advantage in its challenge to help

---

[30] Canada's National Defence Act (NDA) Part V.1 273.64(1)(b), available at http://laws.justice.gc.ca/eng/acts/N-5/page-100.html#docCont

[31] Ibid. Part V.1 273.64(1)(a).

[32] Ibid. Part V.1 273.63(2)(a).

secure GOC networks. This is an advantage also enjoyed by Canada's Five Eyes partners (US, UK, Australia and New Zealand). I will speak of this partnership later.

Working in the GII to acquire the signals intelligence in support of GOC policy priorities[33] enables CSEC to anticipate and understand the capabilities of foreign state sponsored threat actors, enabling the crafting of a defence well before they reach the GOC networks. This technical know-how is mirrored in and leveraged by the Information Technology Security staff [34], who applies similar skillsets closer to home, on the perimeter of the GOC networks. These combined capabilities enable CSEC to see the threat coming and to prevent it from reaching its potential victims on the GOC's systems. By leveraging classified signals intelligence data, CSEC can recognize foreign intrusions that are undetected by commercial technologies.

Leveraging the knowledge and capabilities of the Five Eyes partners, who are doing the same things for their systems, enlarges the database of exploiters and their tradecraft such that the partnership can collaborate on defences and mitigation methodologies.

But this challenge is a complex one, as even one of the best-resourced cryptographic agencies in the world would attest. General Keith Alexander, Commander, United States Cyber Command/Director, National Security Agency/Chief, Central Security Service, in speaking at the International Conference on Cyber Security sponsored by the Federal Bureau of Investigation this past January, told the conference that the Pentagon's complete infrastructure is too chaotic and archaic to be successfully defended from cyber-espionage, cyber-terrorism or cyber-warfare assault. He went on to say that the National Security Agency (NSA) "can't see them all (interconnected networks) [let alone] defend them all."[35]

The GOC has a patchwork of networks of unique architecture and configurations such that the same threat in each network requires a unique mitigation approach. If this

[33] Ibid. PartV.1 273.64(1)(a).

[34] Ibid. PartV.1 273.64(1)(b).

[35] Fitsanakis, Joseph. "US Pentagon computers cannot be protected, says NSA head", January 13, 2012, available at http://intelnews.org/?s=Internation Joseph Fital+Cyber+Security+Conference+

isn't indefensible, it is very close to it. Shared Services Canada, the Treasury Board and Public Works Government Services Canada, among others, are working to consolidate and streamline the delivery of GOC information and technological services thereby improving its defensibility.

The new system will be designed such that security will be enhanced by built in redundancies and resiliencies. This effort will be further leveraged by a profound reduction, hopefully from thousands down to hundreds, in the number of GOC network connections to the Internet.

It must, however, be stressed that the threat, as has been highlighted earlier, is growing unhindered by resource concerns or legal and policy constraints. The same cannot be said for the defenders, who are constrained by resources, and legal and policy issues. None of these limitations are impossible, however, the current fiscal reality will limit how much can be done quickly. This combined with the challenge of finding properly qualified Canadians motivated to work in the field of cyber security will be a limitation.

Nevertheless, CSEC's legislation does give Canada an advantage over our neighbours to the south. I return to the B Mandate as written in the legislation: "… to help ensure the protection of electronic information infrastructures of importance to the Government of Canada;"[36]

It is noteworthy that the scope of CSEC's mandate is not limited to military networks or even government networks. It has the legislative authority to protect/defend any information or information infrastructures of importance to the Government of Canada. Its focus, at this point in time, is Government of Canada systems but critical infrastructure could be included were the Government of Canada to so decree and should resources permit.

In the US the responsibility for government systems is shared. The NSA is responsible for Department of Defense systems (.mil) and the Department of Homeland Security (DHS) for the rest of government (.gov). The matter of responsibility for critical infrastructure is before Congress and has not yet been resolved. The NSA is currently

[36] (36) NDA, Op. cit., PartV.1 273.64(1)(b).

the only US organization with the capabilities and monitoring infrastructure to protect US information infrastructure. Partnering with the DHS is an option but is it the optimal solution?[37]

Partnering

Critical infrastructure, much of which is controlled by Internet-connected systems and susceptible to cyber-attack, is high on the Canadian list of national security concerns. Accordingly, the GOC must do more with the provinces, the private sector and non-governmental agencies, who own and operate 85% of the critical infrastructure, if they are to address this matter. Canada's National Plan for Critical Infrastructure[38], in conjunction with the Action Plan for Critical Infrastructure[39], is intended to meet this need.

The intent is to substantially expand the GOC's engagement activities with the ten critical infrastructure sectors. The relatively newly created Canadian Security Telecommunications Advisory Council was the first of the National Cross-Sector Fora intended to promote collaboration across the sector networks, address interdependencies and promote information sharing across sectors.

Comparable fora have been, or soon will be, created for the other nine sectors listed below. Opposite each is the GOC lead.[40]

Sector	Federal Lead
Energy and Utilities	NRC
Finance	Finance Canada

[37] Gorman, Siobhan. "NSA Chief Seeks Bigger Cyber Security Role"-WSJ.com, available at http://jamadots.olhblogspace.com/?tag=keith-alexander

[38] Public Safety Canada, Canada's National Strategy for Critical Infrastructure, 2011, available at http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx

[39] Public Safety Canada, Canada's Action Plan for Critical infrastructure, 2011, available at http://www.publicsafety.gc.ca/prg/ns/ci/ct-pln-eng.aspx

[40] Ibid.

Health	Public Health
Water	Environment Canada
Transportation	Transport Canada
Safety	Public Safety Canada
Manufacturing	Industry Canada
Government	Public Safety
Food	Agriculture and Agri-Food Canada

Further partnering initiatives include Public Safety Canada (PS) initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors. PS has also reoriented the mandate of their Canadian Cyber Incident Response Centre[41] to focus on national issues and on supporting the provinces, territories and industry. At the same time, PS has transferred the GOC incident response coordination to CSEC.

Public Awareness

PS has taken the lead for the third pillar with a national awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online.

More needs to be done in this regard. The GOC must reach out to the business community and work with them based on a layered approach to security. Vince Plaza,

[41] CCIRC's Former Role: responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber attacks.

Vice President Information Technology at Team Logic IT, offers the following advice that could certainly be the basis of an approach.

- Protecting the internal network, at the external level: Having hosted anti-`spam and/or hosted email services will protect against most, if not all, email borne threats.

- Protecting the gateway layer: One of the most vulnerable spots in a network is the point at which the company connects to the Internet. An up-to-date security appliance with gateway anti-virus and web content filtering is absolutely necessary to curbing threats to the Internet.

- Protecting the end-point, the computer: Downloading and keeping spyware and anti-virus software up-to-date on all in-network computers will minimize risk. In addition, proper risk management is critical. Finally, password management must be enforced.

- Vulnerability and penetration testing: You only know how secure you are if you test.

- Vendor diversity: Diversify security tasks. If one vendor doesn't have the necessary tools, in all likelihood someone else will.

- Training, training, training: Regular employee training is absolutely essential for the security health of any network. Annual or bi-annual practices will pay for themselves many times over.[42]

The Canadian Forces and Cyber Security

Consistent with the current policy within the GOC for all departments, the Department of National Defence (DND) and the Canadian Forces (CF) are responsible for all aspects of securing their own systems. Furthermore, they are responsible for the provision of defence intelligence to inform the GOC threat and risk assessment process.

[42] Savitz, Eric. "6 Ways to Protect Any Size Business fro Cyber Threats, Forbes, 26 Jan, 2012 , available at http://www.forbes.com/sites/ciocentral/2012/01/26/6-ways-to-protect-any-size-business-from-cyber-threats

They provide cyber security information from military allied sources, in-theatre monitoring and reporting on technical information technology threats and providing options analysis for potential military responses.[43]

In the wake of Canada's Cyber Strategy, DND and the CF are currently analyzing the cyber challenge from their own perspective and with the functions of other community stakeholders in view. This thinking will assist the Department in effectively organizing its approach, prioritizing its needed partnerships and external dependencies, and articulating their contribution to cyber security.

A partnered approach between the cryptographic and defence organizations appears to be a logical approach and potential model for Canada. For example, the US Department of Defense (DOD) partnered similarly with the NSA to take advantage of the NSA's unique Signals Intelligence/Information Assurance platform.

Within Canada, the CSEC is the only organization capable of the full spectrum of cyber network operations (CNO).[44] It would be prohibitively expensive, if even logistically possible, for another government department to duplicate the full spectrum of CSEC capabilities in CNO. Aside from the complexity of the cryptographic infrastructure required, subject matter experts would not likely be available in sufficient numbers in our country to consider staffing a second agency.

A promising option from the perspective of efficiencies and appropriate authorities would be to enable the CF to leverage CSEC's capabilities and platform.

While certainly not the only possible approach, this option does efficiently leverage the GOC's current capabilities and it can learn from and build upon the US's experience in a manner tailored to the unique Canadian reality.

---

[43] Cyber Security Strategy, Op. sit.

[44] Computer Network Operations (Government of Canada terminology): CNO comprises three categories of activity;

- Exploitation or Signals intelligence within CSEC, for intelligence gathering purposes;
- Defence or Information Technology Security within CSEC, defending the GOC or critical infrastructure;
- Attack or Cyber Warfare, as part of modern military operations.

The International Scene

Dr. Paul Cornish, Professor of International Security at the University of Bath, suggests that, "Technological strength and superiority has, unfairly though it might seem to its originators and beneficiaries, prompted what military analysts would describe as 'asymmetric vulnerability', where a fleet-footed and sharp-witted adversary can manoeuvre so fast and decisively that the strongest and most elaborate defences are turned into a cumbersome liability and a disadvantage."[45]

Is the situation we find ourselves in beyond the capacity of the 'nation state' to deal with? Is it a strategic liability that demands a co-operative approach among nation states?

The initial attempt to such an approach was the two-day conference of early November 2011, hosted by UK Foreign Secretary William Hague. Although the goal of the conference was initially billed as a major advance in an urgent quest for a 'treaty' to govern international conduct on the Internet, it finally settled on the goal of non-binding norms, which would set out the broad "rules of the road" for interactions in cyberspace. The hope is that such an approach would promote safe, predictable and consistent interactions while ensuring the Internet's accessibility and openness. The idea would be to seek support for the concept that existing principles of international law (e.g. human rights law, the law of armed conflict) apply equally in cyberspace.

Mr. Hague, supported by the US and Canada among others, pushed the concept forward but China and Russia would not be moved from their preference for a cyber-arms control regime set up by the UN.

One could surmise, that it is the difference between information security and cyber security that may underpin the conceptual impasse between Russia, China and the Western nations in cyberspace. Cyber security, the preferred focus of Western countries, centers on the technical security of hardware, software, data and its transmission. Information security includes all aspects of cyber security but also delves

---

[45] Cornish, Paul. "The Vulnerabilities of Developed States to Economic Cyber Warfare", Working Paper, June 2011, available at http://www.chathamhouse.org.uk

into the content of cyber data – usually for the purposes of censorship. The Chair addressed this issue head on in his concluding remarks.

> "The fourth message is that, while working together to defeat threats in cyberspace, you should not imagine for an instant that you can resist the growing force of the tide now flowing for transparency, open information, and the free exchange of ideas. Those Governments that try to do so are in my view certain to fail."[46]

Even if "non-binding rules of the road" could be agreed to, one wonders if signatories would eventually be tempted to design a corresponding range of punitive actions. Were that to be entertained, it is unclear how such action would be instigated or endorsed, and what court of higher appeal would exist to ensure just and proportionate action.

Much work remains to be done in these matters, and discussion will continue to pursue a way forward. Hungary and Korea accepted to host the next iterations of the conference in 2012 and 2013 respectively.

In the meantime, Melissa Hathaway, President of Hathaway Global strategies LLC and special advisor of Harvard Kennedy School's Belfer Center, and John Savage, the An Wang Professor of Computer Sciences at Brown University, suggest that nations pursue the thought that ISPs must accept additional responsibilities such that they ensure the reliable delivery of an essential service, such as the Internet.

They argue that the gap between written and implied responsibilities for ISPs needs to be closed such that they become explicit duties. They define eight ISP duties:

- Duty to provide a reliable and accessible conduit for traffic and services;
- Duty to provide authentic and authoritative routing information;
- Duty to provide authentic and authoritative naming information;
- Duty to report anonymized security incident statistics to the public;
- Duty to educate customers about threats;

[46] London Conference on Cyberspace, Closing Press Conference, Foreign Secretary William Hague, November 2, 2011, available at http://www.fco.gov.uk/en/news/latest-news/?view=PressS&id=685663282

- Duty to inform customers of apparent infections in their infrastructure;
- Duty to warn other ISPs of imminent danger and help in emergencies;
- Duty to avoid aiding and abetting criminal activity.[47]

Is Canada Doing Enough?

A new benchmarking of 19 of the world's leading economies (G20 – EU) which ranked countries in their ability to withstand cyber attacks and to deploy the digital infrastructure necessary for a productive and secure economy, the Cyber Power Index, is one measure. Each country's ranking is a weighted mean of scores from four categories: legal and regulatory environment, economic and social context, technology infrastructure and industry application.

The study concluded that the top five countries exhibiting cyber power, as measured by the index – the UK; the US; Australia; Germany and Canada – illustrate that developed Western countries are leading the way into the digital era. The top five performers rated highly across the board, ranking in the top seven in all four categories[48].

Conclusion

Computers and information systems are an integrated component of Canadians daily lives. They are an essential service to our social lives, our commercial and industrial activity and they are our interface with our governments. And Canadians are among the world's leaders in embracing cyber technology and the advantages it offers. At the same time, we have not been as enthusiastic in understanding its vulnerabilities and embracing secure operating procedures. This combination of factors leaves us ripe for exploitation.

---

[47] Hathaway, Melissa E. and John E. Savage, Stewardship of Cyberspace Duties for Internet Service Providers, March, 2012, available at http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012-hathaway-savage.pdf

[48] (48) Booz/Allen/Hamilton, "The Cyber Hub", available at http://www.cyberhub.com

And exploitation comes from a multitude of sources; states, organized crime, criminals, pedophiles, hacktivists, terrorists and adventurers/joy seekers. And they attack indiscriminately. We are vulnerable as individuals, as organizations/associations, as businesses and as governments. All of have a part to play in addressing this challenge to what is a fundamental part of a modern society.

We have a responsibility to understand the technology and its vulnerabilities, we have a responsibility to understand the threat and its impact on our way of life, we have a responsibility to do our part as individuals, as businessmen and business women and as citizens to address this challenge to what is precious to us.

As citizens we must press our governments; municipal, provincial and federal to ensure that they lay the foundation upon which a 'whole of country' cyber security effort can be built.

That foundation has its beginnings at the federal level. Canada's Cyber Security Strategy is the Federal Government's action plan to secure cyberspace for Canadians. The start point has to be the security of Government systems. At all levels, there is evidence that governments' ability to deliver services could be threatened by attacks on the supporting IT infrastructure.

The strategy calls for a 'whole of government' approach to achieve the level of security required to assure Canadians that the Government can effectively serve Canadians and safeguard their personal data while so doing. The effort is broad based but has its beginnings in further enabling the CSEC's unique cryptographic capabilities and global partnerships to address the sophisticated (state sponsored) cyber threat.

This effort will need to be implemented through the efforts of numerous other departments and agencies, including but certainly not limited to, those departments and agencies who are key to designing and assembling a federal government network that is more easily defensible.

At the same time the GOC has the lead in partnering with other levels of government and the private sector to strengthen Canada's cyber resiliency, including that of its critical infrastructure.

Finally the GOC is responsible for negotiations at the international level. An international resolution in the form of a treaty or a 'rules of the road' approach may well be needed, regardless of what we are able to accomplish domestically.

Industry, for its part, must accept that security is essential for the long term health of its relationship with its clients. In this regard, the ISPs could set a positive example by closing the gap between regulated responsibilities and the unwritten, yet expected ones. Should this not happen, nations may need to impose this approach through legislation and regulation.

All businesses can improve security through four actions on a consistent basis: a layered approach to security; that is, protecting at the external to network level, protecting at the level of the gateway and at the end point, the computer and wherever information is held/stored. This in combination with regular testing of defences, vendor diversity and training will vastly improve on the current reality.

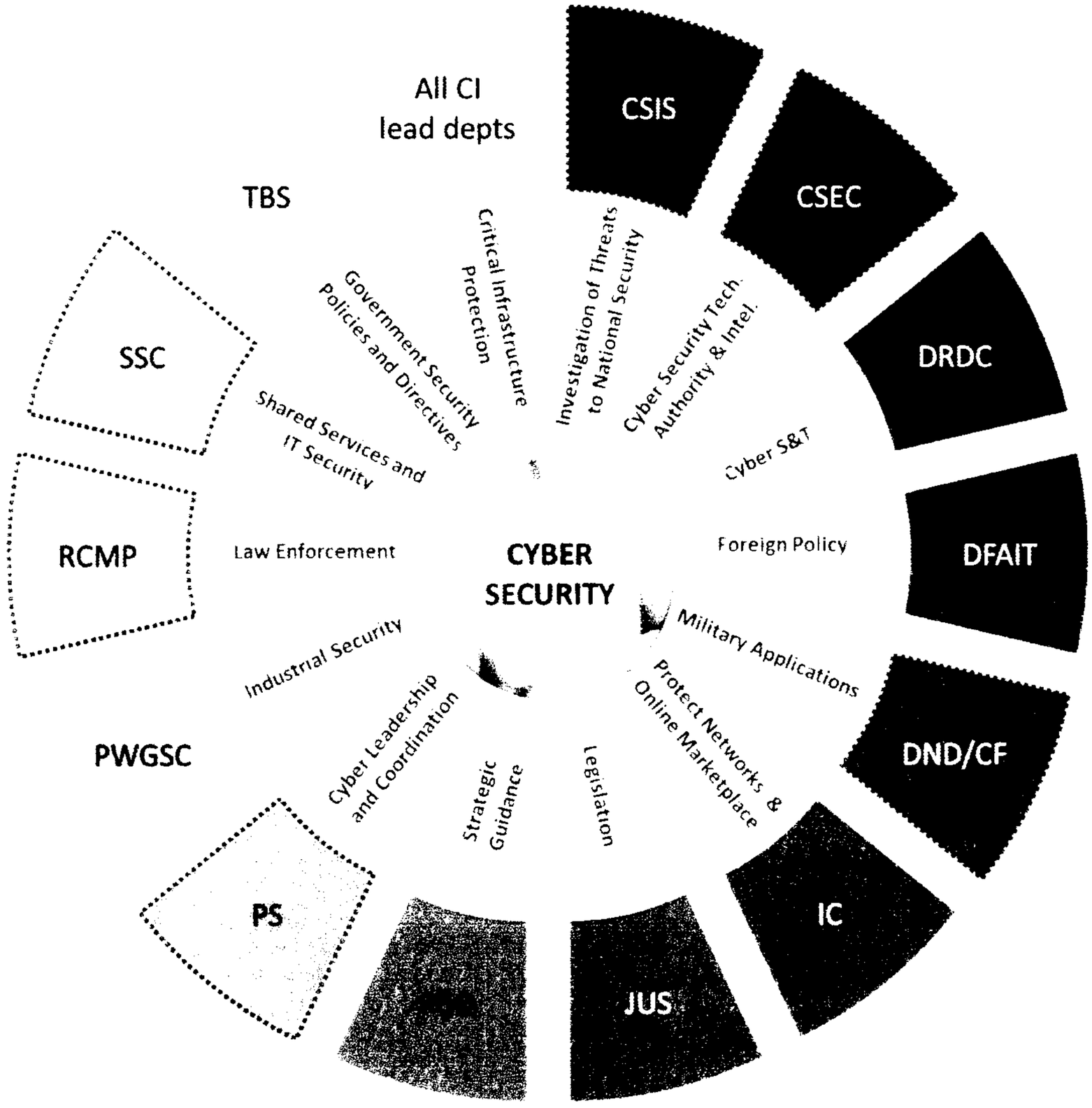
As individual users, two simple improvements will address up to 80% of the compromises; strong passwords changed regularly and prompt patching/updating of software. As well, citizens must reconcile the ease and comfort with which they live online with the need to defend against cyber threat. A populace that arms itself against even small-scale attacks helps its government to project a secure cyber front thereby encouraging the average attacker to seek out softer targets elsewhere.

The cyber world in which Canadians live, work and play lacks the regimes of law and order that govern our physical world. The long-term objective for cyberspace must be to foster an environment where online threats are known and managed to the greatest extent possible. Achieving this will require sustained and coordinated collective action and investment by the federal Government, its international allies, industry, academe and individual Canadians. It must be a team effort.

The Government of Canada and Cyber Security:

Security Begins at Home – Annex A

Roles and responsibilities with respect to cyber security



Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

All critical infrastructure lead departments
Includes Finance Canada, Environment Canada, Health Canada, Transport Canada, Natural Resources Canada, Agriculture and Agri-Food Canada, and Public Safety Canada.

Treasury Board of Canada Secretariat
Establishes and oversees a whole-of-government approach to cyber security, including: setting government-wide direction and establishing priorities for securing government IT systems and networks; providing direction and advice to lead security agencies on the approach and implementation of measures for managing IT security incidents; and providing oversight of IT incident management, including post-mortem reviews and lessons learned.

Shared Services Canada
Streamlines and consolidates ICTs in the areas of email, data centres and networks, and for ensuring the confidentiality, integrity and availability of common IT services provided to departments.
Provides common information technology (IT) security services and other solutions to enable departments to exchange information with citizens, businesses and employees.
Gathers, analyzes, consolidates and facilitates the sharing of operational threat and vulnerability information related to common IT services and Government IT critical infrastructure managed by Shared Services Canada, and communicates the information to the Canadian Cyber Incident Response Centre and, as authorized, to departments and cyber security partners.

Royal Canadian Mounted Police
Leads the criminal investigative response to suspected criminal cyber incidents involving critical information infrastructure (i.e., unauthorized use of computer and mischief in relation to data). Leads the investigative response to suspected criminal national security cyber incidents.
Assists domestic and international partners with advice and guidance on cyber crime threats.

Public Works and Government Services Canada
Provider of shared and common services. As part of its Industrial Security Program activity, ensures security in contracts awarded by the Department or when requested by other Government departments.
Ensures the protection of foreign and NATO classified information within the private sector in Canada.
The Industrial Security Sector maintains relationships with allies and negotiates Memoranda of Understanding on industrial security matters, including cyber security, in contracting.

Public Safety Canada
Leads and coordinates the implementation of *Canada's Cyber Security Strategy*, including the design of a whole-of-Government approach to performance measurement and reporting; engagement with provinces and territories, critical infrastructure, and international allies on strategic cyber security policy issues and national cyber incident management; and public awareness activities to inform Canadians of the risks they face and the actions they can take to protect themselves and their families in cyberspace.
The Canadian Cyber Incident Response Centre acts as Canada's national CERT (Computer Emergency Response Team) in providing assistance and mitigation advice to domestic partners and coordinating the national response to any cyber security incident.

Privy Council Office
Houses and provides support to the National Security Advisor to the Prime Minister.
Coordinates activities among members of the Canadian security and intelligence community, and promotes a coordinated and integrated approach to national security issues.

Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

Communications Security Establishment Canada
Monitors and defends Government of Canada networks by detecting, discovering and responding to sophisticated cyber threats to the Government, and provides mitigation and/or recovery advice and/or guidance to Government departments to help them recover from cyber incidents.
Government of Canada's cryptologic agency responsible for the collection of cyber foreign intelligence and Canada's interface with the Five Eyes cryptologic community. Undertakes classified research and development for cyber security.

Canadian Security Intelligence Service
Conducts national security investigations. Reports to and advises the Government of Canada of activities constituting a threat to the security of Canada as defined in the *Canadian Security Intelligence Service Act*.
Provides analysis to assist the Government of Canada in understanding cyber threats, and the intentions and capabilities of cyber actors operating in Canada and abroad who pose a threat to the security of Canada. This intelligence enables the Government of Canada to improve its overall situational awareness, better identify cyber vulnerabilities, prevent cyber espionage or other cyber threat activity, and take action to secure critical infrastructure.

Defence Research and Development Canada
Leads the development of military cyber security S&T in support of the Canadian Forces.
Leads domestic Public Safety Canada cyber security S&T efforts not specifically assigned to another department or agency through the Centre for Security Science and with domestic security partners in the Public Security Technical Program. This is delivered in partnership between Government, industry, academia and allies.

Department of Foreign Affairs and International Trade
Supports international bodies in mitigating cyber threats and assisting foreign governments in improving their cyber security profile and capabilities.
Contributes to diplomatic engagement in order to help shape the multilateral regulatory space that is emerging with respect to cyber security. Enables the Government to better position Canada on the international stage to defend and promote its foreign policy and cyber security-related interests.

Department of National Defence / Canadian Forces
Responsible for the provision of defence intelligence to inform the Government of Canada threat and risk assessment process.
Contributes to Government situational awareness during the monitoring and analysis, mitigation, and response phases of the *GC IT IMP* by providing cyber security information from military allied sources, monitoring and reporting on technological IT threats, and providing options analysis for potential military response.

Industry Canada
Responsible for spectrum management in Canada and for fostering a robust and reliable telecommunications system. Develops policies to ensure a safe and secure online marketplace. Helps to ensure the continuity of telecommunications during an emergency.

Department of Justice Canada
Supports initiatives of client departments and agencies through the provision of legal advice on matters relating to cyber policy and law.
In respect of certain matters, especially those relating to criminal law policy and information sharing, Justice plays a leading role. Departmental Legal Services within the Communications Security Establishment Canada had been designated as the centre of excellence on cyber-related legislation.