Pilon, Claude

From: Pilon, Claude
Sent: Thursday, March 08, 2012 4:19 PM
To: Hunter, Linda
Cc: Ste-Marie, Lili
Subject: FW: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous
Attachments: CCIRC CYBER FLASH CF12-001: Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property

Linda,

Here is an overview of Anonymous done by CCIRC on March 1st.

Thanks

Claude

Claude Pilon, B.Sc., LL.L, LL.B
Counsel / Avocat
Public Safety Canada Legal Services / Services juridiques de Sécurité publique Canada
(613) 991-4364 / claude.pilon@ps-sp.gc.ca
PROTECTED: SOLICITOR-CLIENT PRIVILEGE/PROTÉGÉ: PRIVILÉGE DU SECRET PROFESSIONNEL DE L'AVOCAT

Please feel free to reply in the official language of your choice/ N'hésitez pas à me répondre dans la langue officielle de votre choix

-----Original Message-----
From: GOC-COG
Sent: March-01-12 1:25 PM
To: _GOC Distribution List / Liste de distribution du COG
Subject: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous

(La version française suit)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
INFORMATION NOTE
****

Number: IN12-501
Date: 1 March 2012

****
Overview of the Hacktivist Group "Anonymous"

****

PURPOSE
=======

The purpose of this report is to provide an overview of the hacktivist group "Anonymous." It contains information on its organizational structure, tradecraft and targets; the threat to Canadian Critical Infrastructure systems; and recommended mitigation.

ASSESSMENT
==========

EXECUTIVE SUMMARY

Anonymous targets governments, private firms and individuals whose activities or purposes appear to be in conflict with principles espoused by the group. These principles mainly focus on: civil rights (e.g. oppressive regimes); information accessibility (e.g. Internet censorship); and other causes associated with perceived social injustice.

Based on a view of previous targeting by Anonymous, Canadian critical infrastructure systems could be targeted due to government legislative and regulatory initiatives (e.g. the Copyright Modernization Act) and initiatives that may result in activist opposition (e.g. environmental or social issues).

Anonymous uses a number of capabilities against its targets. These include, but are not limited to, distributed denial-of-service attacks (DDoS)(2), password cracking, SQL injections(3) and malware (virus) deployments. Canadian organizations have been both direct and indirect targets of Anonymous activity. For example, the Toronto Police Service website was hacked in 2011, likely in response to the "Occupy Toronto" camp evictions; Canadian corporations involved with the Alberta Tar Sands have been targeted, in particular to protest against the Keystone XL pipeline; and subsequent to a late-2011 breach of STRATFOR, a US corporation with links to intelligence and law enforcement organizations, credentials used by Canadian organizations to access STRATFOR databases were published. Although Anonymous leverages a variety of tradecraft to achieve its aims, strong IT security practices will help to defend against Anonymous exploits. The majority of these exploits are not leveraging zero-day(4).

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their agendas. Most notably, "Anonymous" is a term that refers to a group of activist hackers, or hacktivists, that poses a wide range of cyber threats to government and commercial organizations around the world. Anonymous' agenda has included initiating cyber threat activities in protest of perceived government-mandated Internet censorship and in support of worldwide activist movements.

STRUCTURE

Anonymous is loosely composed of sub-groups (e.g. Anon-ops5, LulzSec6) and often conducts joint campaigns with other hacktivist groups in support of the same agenda. For example, TeaMp0isoN and People's Liberation Front are separate hacktivist groups with the freedom to opt-in or opt-out of projects conducted jointly with Anonymous. The Anonymous movement has also inspired copycat actions from other hacktivist groups, such as LulzRaft7.

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several unofficial spokespeople(8), Anonymous does not officially have a specific spokesperson. The only requirement for members of Anonymous (known as "Anons") is that they must always remain anonymous while participating in cyber campaigns supporting Anonymous' efforts. In many cases, Anons voluntarily join a botnet by downloading and installing the Low Orbit Ion Cannon (LOIC)(9) onto their computers. (Comment: The absence of a defined leadership structure is possibly why some threats associated with Anonymous are carried out, whereas others become empty threats if general consensus of a target was not agreed upon by the group at large.)

CHOOSING TARGETS

Since Anonymous is decentralized, new targets are determined in a variety of ways. Some of the most commonly used and documented methods of selecting targets are listed below.

- Through consensus among Anons using online polls. Following a discussion on an IRC, an online poll will be conducted to determine the target(s) of DoS/DDoS attacks. Although it appears to be a democratic process, elite Anons who are IRC channel operators are the ones who make the final decision about where to direct the LOIC attacks.
- As a response to perceptions of direct or indirect provocation by governments, by other hacking groups or companies (e.g. HBGary(10)), against the group as a whole, or against the principles to which Anonymous adheres.
- By exposing poor security practices. For instance, Anonymous members may use "Google Hacking" to identify vulnerable targets of opportunity. Results of such reconnaissance activities are often posted ans shared using sites such as pastebin.com .

These targeting practices are generally implemented in support of a specific Anonymous objective or campaign. For instance, one key Anonymous raison-d'être is to promote the ongoing "Operation Anti-Security" (also known as "AntiSec"), which is a declaration of cyber warfare on governments and corporations in response to perceived corruption and Internet censorship. As part of this campaign, Anonymous members are encouraged to locate and leak classified government information and to target banks or other high-profile establishments.

PAST TARGETS/BEHAVIOUR

Anonymous has initiated cyber threat activities in protest of government decisions and in support of their own principles. Recently, its hacktivism efforts have been concentrated on the various Occupy(11) movements, protesting Internet censorship and Internet filtering, protesting against oppressive regimes, and supporting WikiLeaks. These campaigns include:

2008:
Project Chanology (worldwide)
Action: DDoS attacks were launched against the Church of Scientology websites and non-violent protests worldwide.
Reason: The Church of Scientology was attempting to restrict access to information that it found embarrassing and was readily available on the Internet.

2009:
Anonymous Iran (Iran)

Action: An Iranian Green Party Support site, Anonymous Iran, was created to provide covert resources and event updates for Iranian protestors during government-imposed Internet information censorship.
Reason: To provide support to Iranian protestors against a regime perceived to be corrupt.

Operation Didgeridie (Australia)
Action: A DDoS attack was launched against the Australian prime minister's website.
Reason: To protest against proposed government policy and legislation related to the implementation of ISP-level blacklists.

2010:
Operation Titstorm (Australia)
Action: A DDoS attack was launched against the Australian parliament's website and the prime minister's website was defaced.
Reason: To protest against the implementation of an Internet filter that would block websites containing child abuse material and certain types of pornography.

Operation Payback / Operation Sony (worldwide)
Action: DDoS attacks were launched against Sony PlayStation websites.
Reason: To support online file-sharing and to retaliate against Sony for seeking legal action against two individuals who successfully hacked the PlayStation3 system to allow users to run generic applications(12).

Operation Avenge Assange (US)
Action: DDoS attacks were launched against Amazon, PayPal, MasterCard and Visa websites.
Reason: To show support for WikiLeaks and to protest against its founder's arrest.

Operation Zimbabwe (Zimbabwe)
Action: DDoS attacks were launched against the Government of the Republic of Zimbabwe's websites.
Reason: To protest against censorship of WikiLeaks documents.

2011:
Operation Tunisia (Tunisia)
Action: DDoS attacks were launched on the Government of Tunisia's websites.
Reason: To protest against Internet censorship and to support the Arab Spring(13).

Operation Syria (Syria)
Action: Website of the Syrian Defence Ministry website was defaced.
Reason: To support the Arab Spring (Syrian uprising).

Operation Egypt (Egypt)
Action: A DDoS attack was launched against the Government of Egypt's website and the National Democratic Party's website. Also, the names and passwords of email addresses of government officials were released.
Reason: To support the Arab Spring (Egyptian revolution).

HBGary Federal (US)
Action: HBGary's website was defaced, company files were deleted and 68,000 employee emails were published.
Reason: An HBGary official provoked Anonymous by threatening to expose information about the group.

Bank Of America (US)
Action: Sensitive Bank of America documents were released online, which allegedly proved cases of corruption and fraud at the bank.
Reason: To protest in support of allegations of corruption and fraud within the US banking system.

Operation Malaysia (Malaysia)
Action: DDoS attacks were launched on 91 Government of Malaysia's websites.
Reason: In response to the Malaysian government's censorship of sites such as Pirate Bay(14) and WikiLeaks.

Occupy Wall Street (US)
Action: DDoS attacks were launched on the Oakland Police Department website and the St. Louis mayor's website.
Reason: To protest evictions of protestors from Occupy sites, in support of the worldwide Occupy movement.

Operation Mayhem (US)
Action: Guy Fawkes virus was released on Facebook.
Reason: To protest the Stop Online Piracy Act(15), perceptions of police violence towards protestors in Occupy movements and any opposition to Anonymous activities.

Cox Communications (US)
Action: Domain Name System (DNS) servers were taken offline, removing Internet access for clientele in most of southwest America.
Reason: To protest Cox Communications' attempted regulation of customers' data usage quota.

Operation Blackout (US)
Action: In November, Anonymous threatened action against the US government.
Reason: To protest against the Stop Online Piracy Act.

STRATFOR (worldwide)
Action: STRATFOR is a US company that provides services to intelligence and law enforcement agencies, among others. Two hundred gigabytes of data was stolen from STRATFOR's web servers and subsequently published. The stolen information included active credit cards, e-mail addresses, phone numbers, encrypted passwords and sensitive information from clients (including government and military departments). Anonymous planned to donate to charities using the stolen credit card information.
Reason: Following the HBGary incident, Anonymous began to investigate what it refers to as a "state-corporate alliance against the free information movement." Due to STRATFOR's ties with the intelligence and military contracting sectors and government agencies, Anonymous believed that targeting STRATFOR would "improve [their] ability to continue this investigation and thereby bring to light other instances of [perceived] corruption, crime and deception on the part of certain powerful actors based in the US and elsewhere(16)."

Ongoing:
Operation Antisec (NATO, Tunisia, Brazil, Australia, US, Turkey, UK, and other countries)
Action: In the US, DDoS attacks were launched against the Central Intelligence Agency's (CIA) website, the US Senate website was hacked and information about its internal server structure was released. In the UK, DDoS attacks were launched against the Serious Organised Crime Agency's (SOCA) website.
Reason: The declaration of cyber warfare on governments and corporations worldwide in response to perceived corruption and government censorship.

CANADA:
Anonymous has directly and indirectly targeted the Government of Canada, Canada's municipal governments and Canadian private corporations. Examples include:

Government of Canada:
STRATFOR (December 2011)
The federal government has been an indirect target of Anonymous activity in connection with STRATFOR. STRATFOR is a resource used by various federal departments. When usernames and passwords were released by Anonymous, some of them included those of federal employees(17).

Bill C-11, ACTA and Bill C-30 (February 2012):
The federal government was directly targeted by Anonymous in relation to the Bill-C-11 (Copyright Modernization Act), ACTA and C-30 (Lawful Access Package) through denial of service attacks and threats against the Public Safety Minister extensively covered in the media.

Municipal Governments:
Toronto (November 2011)
Anonymous threatened to take down the City of Toronto's website if officials evicted protestors from the Occupy Toronto camp. Although no known activity was conducted against the City of Toronto's website, the Toronto Police Service website was hacked and several usernames and passwords were stolen, possibly in retaliation to the continued efforts to evict the Occupy camp.

Private Corporations:
Operation Green Rights/ Project Tarmaggedon (July 2011)
In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline and the Alberta Tar Sands project.

TRADECRAFT

Anonymous has traditionally used basic, open-source-available cyber threat tradecraft against their targets. However, beginning in mid-2011, Anons have begun developing their own malware. (Comment: The exploits below do not represent a conclusive list because Anonymous has a large number of members and all of their activities cannot be tracked and attributed to Anonymous.)

DoS/DDoS:
Anonymous' usual method of choice is to launch DoS/DDoS attacks against a target's website in an effort to bring the network offline and to make the website unavailable to legitimate users. Two commonly used methods include:

- LOIC/HOIC/JS LOIC/BOIC:
Anons are encouraged to download and launch the Low Orbit Ion Cannon application enabling them to willingly participate in a botnet. The LOIC is pointed at a target of choice, which then disrupts the service of the victim's host. However, since LOIC can reveal the IP addresses of its users, its traceability has prompted Anonymous to find other means of attacks such as encouraging the use of anonymization proxy like TOR (The onion router). Other versions of the tool include a Javascript version, JS LOIC, and most recently, a Bookmark-based version coined BOIC. These versions require little more than one mouse-click to flood a target with GET and POST packets aimed at creating a denial of service condition.

- Apache Killer:
The Apache DoS tool nicknamed the "Apache Killer" exploits a vulnerability that allows remote attackers to send requests to servers via a malformed uniform resource identifier (URI)(20). It is designed to drain the web server's memory, which would then take the website offline. It also allows a remote attacker to use a single computer to wage DoS attacks against an Apache server.

DoS/DDoS via SQL Injections:
- #RefRef:
Anonymous developed and released a Perl DDoS tool in September 2011, #RefRef, that exploits SQL(21) vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline. #RefRef could be used in combination with tools such as Havij, an SQL Injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities. As a result of SQL

vulnerability exploitation, database content could be changed, or database information (such as credit card information or passwords) could be stolen.

Guy Fawkes Virus:
Malware development is also something that Anonymous members have been focusing on. The Guy Fawkes(22) virus was developed by Anon to take control of a Facebook account and use it to spread malware to other members without the users actually logging onto the site. According to security analysts at the antivirus software company BitDefender, the Guy Fawkes virus (which they have named Backdoor-Bifrose-AAJX) has the ability to inject itself in the Internet Explorer process, providing a remote attacker with unhindered access to the compromised system. It would also record keystrokes and disrupt processes of known antimalware software. (Comment: Although the Guy Fawkes virus was previously believed to be responsible for the massive pornographic spam attack against Facebook in November 2011, this was later refuted by Facebook and BitDefender. Anonymous has stated that it is still working to control the virus to be used at a later date.)

Other:
Other techniques used by Anonymous include using social engineering techniques to gain access to victims' systems (e.g. HBGary Federal), using web defacement to post embarrassing messages on victims' websites, using password cracking to exfiltrate data from a victim's database, and using a Twitter raiding tool called Universal Rapid Gamma Emitter (URGE) to hijack Twitter trending topics into topics of interest to Anonymous. It also allows Anons to tweet messages within the topics.

MITIGATION
==========

Strong IT security practices will go a long way to defending against threats such as the Anonymous hacktivist collective. Anonymous generally leverages open source or well-known vulnerabilities. The nature of the targets is also generally advertised in open forums such as Twitter and Pastebin, as well as main stream media.
Organizations are encouraged to consult CCIRC's mitigation guidelines for advanced persistent threats and DDoS attacks found here:
- http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx
- http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

In addition, the following mitigation is available for some of the tradecraft specifically noted above:

Apache Killer
- Apache has since released patches to fix this vulnerability. All users are recommended to upgrade to Apache 2.2.20 or higher.

#RefRef
- Webcode should be hardened against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users. Consult best practices references such as the Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)

ENDNOTES
==========

(1) IRC is a protocol for Internet text messaging and synchronous conferencing. It allows group communications as well as private messaging and file sharing.

(2) A distributed denial-of-service (DDoS) attack is one in which a multitude of systems attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.

(3) SQL injection is often used to attack the security of a website by injecting SQL commands into the database of an application.

(4) Zero-day threats attempt to exploit new computer application vulnerabilities not yet known to the software developer or the general public.

(5) Anon-ops provides communications for Anonymous' announcements.

(6) LulzSec was a small team that joined forces with Anonymous in the ongoing "Operation Anti-Security" or "AntiSec" campaign, which later disbanded in the summer of 2011.

(7) LulzRaft was inspired by LulzSec group and has been responsible for web defacement of the Conservative Party of Canada's website and for accessing private information about the party's donors. They have also been linked to web defacement of Calgary-based energy company Husky Energy's website.

(8) Unofficial spokespeople for Anonymous include Jake Davis (also known by his online nickname "Topiary") and Barrett Brown. For more information on Jake Davis, please see http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-ukpolice/. For more information on Barrett Brown, please see http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx.

(9) According to open source, LOIC is an open source network stress testing application that performs DoS or DDoS attacks on a target site by flooding the server with TCP or UDP packets to disrupt the service of a host.

(10) HBGary Federal is a technology security company that was working with the FBI to unmask members of Anonymous. In February 2011, the CEO, Aaron Barr, revealed an intention to release information on the identities of Anonymous members. As a result, Anonymous members compromised the HBGary website and stole and publicly released the company's documents and emails.

(11) According to open source, the Occupy movement refers to an international protest movement directed against high unemployment, social and economic inequality and perceived corruption in corporations and government.

(12) For more information, please refer to http://www.pcmag.com/article2/0,2817,2383018,88.asp.

(13) The Arab Spring refers to revolutionary protests occurring in the Arab world beginning in December 2010. Countries affected include Tunisia, Egypt, Libya, Bahrain, Syria, Yemen, Algeria, Iraq, Jordan, Kuwait, Morocco, Oman, Lebanon and Saudi Arabia.

(14) The Pirate Bay is a Swedish website known for facilitating illegal downloads and supporting the international anti-copyright movement.

(15) The Stop Online Piracy Act is proposed US legislation to combat against the online distribution of copyrighted intellectual property. This has been viewed by Anonymous as an attempt to censor the Internet.

(16) For the full explanation, please refer to Barrett Brown's statement at http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-hacked.

(17) CTEC has provided mitigation to employees of the affected departments.

(18) This legislation will be similar to previous bills: Bill C-50, Bill C-51 and Bill C-52.

(19) Operation Facebook was launched on November 5, 2011, because Anonymous believes that "Facebook is the opposite of the Antisec cause."

(20) For more information, please refer to CVE-2011-3192 at http://nvd.nist.gov/.

(21) An SQL server is a relational database server that can store and retrieve data across a network (e.g. the Internet). Queries from client machines are formatted in the SQL language.

(22) Guy Fawkes was associated with the Gunpowder Plot, a failed assassination attempt against King James I of England in 1605. The conspirators' plan was to blow up the Houses of Parliament in order to kill the King and the Members of Parliament. Coincidentally, Anons have adopted the easily available and inexpensive Guy Fawkes mask as their symbol.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquires into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

****

SÉCURITÉ PUBLIQUE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

****

NOTE D'INFORMATION

****

Numéro : IN12-501
Date : 1 mars 2012

****
Aperçu du collectif d'hacktivistes Anonymous
****

OBJECTIF
========

Le présent rapport donne un aperçu du groupe d'hacktivistes Anonymous. Il présente des renseignements sur sa structure organisationnelle, ses techniques et ses cibles, sur la menace qu'il pose pour les systèmes d'infrastructures essentielles du Canada et sur les mesures d'atténuation recommandées.

ÉVALUATION
==========

SOMMAIRE

Anonymous cible les gouvernements, les entreprises privées et les particuliers dont les activités ou les buts semblent être en conflit avec les principes énoncés par le groupe. Ces principes sont axés sur les droits civils (p. ex., régimes oppressifs), l'accès à l'information (p. ex., censure sur Internet) et d'autres causes liées aux injustices sociales perçues.

Compte tenu des cibles précédentes d'Anonymous, les systèmes des infrastructures essentielles du Canada pourraient être ciblés en raison des initiatives législatives et réglementaires du gouvernement (p. ex., Loi sur la modernisation du droit d'auteur) et d'initiatives qui pourraient provoquer une opposition militante (p. ex, enjeux sociaux ou environnementaux).

Anonymous utilise diverses capacités contre ses cibles : attaques distribuées par déni de service (DDoS) (2), craquage de mots de passe, injections SQL (3), déploiements de maliciels (virus), etc. Des organisations canadiennes ont été ciblées directement et indirectement par des activités d'Anonymous. Par exemple, le site Web du service de police de Toronto a été piraté en 2011, probablement en réponse aux expulsions du camp Occupons Toronto; des entreprises canadiennes qui participent à l'exploitation des sables bitumineux en Alberta ont été ciblées, en particulier pour manifester contre le pipeline Keystone XL; et, à la suite de l'attaque à la fin 2011 contre STRATFOR, une entreprise des É.-U. avec des liens avec les organismes de renseignement et d'application de la loi, les justificatifs utilisés par des entreprises canadiennes pour accéder aux bases de données de STRATFOR ont été publiés. Anonymous utilise diverses techniques pour réaliser ses objectifs, mais des pratiques solides en matière de sécurité de la TI aident à se protéger contre ces attaques. La majorité des attaques ne tirent pas profit de vulnérabilités du jour zéro (4).

APERÇU

Les pirates militants poursuivent de plus en plus des activités de menaces cybernétiques pour atteindre leurs objectifs. En particulier, le terme « Anonymous » fait référence à un groupe de pirates militants (hacktivistes) qui font peser un large éventail de cybermenaces sur les gouvernements et les organisations commerciales partout au monde. Le programme d'Anonymous a compris l'utilisation de cybermenaces pour manifester contre la censure gouvernementale perçue sur Internet et appuyer des mouvements militants internationaux.

STRUCTURE

Anonymous comprend un ensemble hétérogène de sous-groupes (p. ex., Anon-ops5, LulzSec6) et mène souvent des campagnes en collaboration avec d'autres groupes hacktivistes qui partagent les mêmes objectifs. Par exemple, TeaMp0isoN et le People's Liberation Front sont des groupes hacktivistes distincts qui sont libres de participer ou non à des projets conjoints avec Anonymous. Le mouvement Anonymous a aussi été imité par d'autres groupes hacktivistes, par exemple, LulzRaft7.

Anonymous n'est pas organisé hiérarchiquement et n'a pas de chefs définis. De plus, Anonymous n'a pas de porte-parole officiel, même s'il y a plusieurs porte-paroles officieux (8). La seule exigence que les membres d'Anonymous (les « Anons ») doivent respecter est de garder l'anonymat lorsqu'ils participent à des campagnes cybernétiques pour appuyer les efforts du groupe. Dans de nombreux cas, les Anons se joignent volontairement à un réseau zombie en téléchargeant et en installant l'application LOIC (Low Orbit Ion Cannon) (9) sur leur ordinateur. (Remarque : L'absence d'une structure de direction définie peut expliquer pourquoi certaines menaces associées à Anonymous sont mises à exécution, alors que d'autres n'aboutissent pas si un consensus au sujet d'une cible ne se dégage pas parmi les membres.)

SÉLECTION DE CIBLES

Puisqu'Anonymous est décentralisé, les nouvelles cibles sont fixées de diverses façons. Voici certaines méthodes souvent utilisées et bien documentées de sélection de cibles :

– Consensus des membres dégagé au moyen de sondages en ligne. Après une période de discussion par l'intermédiaire du service de clavardage IRC, un sondage en ligne est réalisé pour fixer les cibles d'attaques de déni de service (DoS) ou de DDoS. Le processus peut sembler démocratique, mais ce sont les Anons d'élite qui exploitent les canaux IRC qui prennent la décision définitive sur la cible des attaques effectuées au moyen de LOIC.
– En réponse à une provocation directe ou indirecte perçue de la part de gouvernements, d'autres groupes pirates ou d'entreprises (p. ex., HBGary (10)) contre le groupe Anonymous ou ses principes.
– Pour exposer de mauvaises pratiques en matière de sécurité. Par exemple, les membres d'Anonymous peuvent utiliser la technique « Google hacking » pour détecter des cibles intéressantes. Les résultats de ces activités de reconnaissance sont souvent publiés sur des sites tels que pastebin.com.

Ces pratiques de ciblage sont généralement mises en œuvre pour appuyer un objectif ou une campagne en particulier d'Anonymous. Par exemple, une raison d'être importante d'Anonymous est de promouvoir l'opération « Anti-Security » (ou AntiSec), une déclaration de cyberguerre contre les gouvernements et les entreprises en réponse à une corruption ou à une censure Internet perçues. Dans le cadre de cette campagne, Anonymous encourage ses membres à trouver et à divulguer des renseignements gouvernementaux confidentiels et de cibler des banques et d'autres établissements bien en vue.

CIBLES ET COMPORTEMENTS DANS LE PASSÉ

Anonymous a lancé des activités de cybermenaces pour manifester contre des décisions gouvernementales et pour appuyer ses propres principes. Plus récemment, ces efforts hacktivistes appuyaient les divers mouvements Occupons (11) et WikiLeaks et s'opposaient à la censure et au filtrage d'Internet ainsi qu'aux régimes oppressifs. Voici un aperçu de certaines de certaines campagnes :

2008 :
Projet Chanalogy (à l'échelle mondiale)
Démarche : Attaques DDoS lancées contre les sites Web de l'église de Scientologie et manifestations non violentes à l'échelle mondiale.

Raison : L'Église de Scientologie essayait de limiter l'accès à des informations disponible sur Internet qu'elle jugeait embarrassantes.

2009 :
Anonymous Iran (Iran)
Démarche : Création d'Anonymous Iran, un site d'appui du Parti vert d'Iran, pour fournir des ressources clandestines et des renseignements sur les événements aux manifestants iraniens dans le cadre de la censure des renseignements Internet imposée par le gouvernement.
Raison : Appuyer les manifestants iraniens contre un régime perçu comme corrompu.

Opération Didgeridie (Australie)
Démarche : Attaque DDoS lancée contre le site Web du premier ministre australien.
Raison : Manifester contre la politique et les lois proposées relatives à la mise en œuvre de listes noires au niveau des FSI.

2010 :
Opération Titstorm (Autralie)
Démarche : Attaque DDoS lancée contre les sites Web du Parlement australien et altération du site Web du premier ministre australien.
Raison : Manifester contre la mise en œuvre d'un filtre Internet qui bloquerait les sites Web présentant de mauvais traitements d'enfants et certains types de pornographie.

Opérations Payback et Sony (à l'échelle mondiale)
Démarche : Attaques DDoS lancées contre les sites Web de Sony PlayStation.
Raison : Appuyer le partage de fichiers en ligne et exercer des représailles sur Sony pour avoir intenté des poursuites contre deux personnes qui avaient réussi à débrider le système PlayStation 3 pour permettre aux utilisateurs d'exécuter des applications génériques (12).

Opération Riposte Assange (« Avenge Assange ») (É.-U.)
Démarche : Attaques DDoS lancées contre les sites Web d'Amazon, de PayPal, de MasterCard et de Visa.
Raison : Manifester du soutien à l'égard de WikiLeaks et manifester contre l'arrestation de son fondateur.

Opération Zimbabwe (Zimbabwe)
Démarche : Attaques DDoS lancées contre les sites Web de la République du Zimbabwe.
Raison : Manifester contre la censure des documents de WikiLeaks.

2011 :
Opération Tunisie (Tunisie)
Démarche : Attaques DDoS lancées contre les sites Web du gouvernement de la Tunisie.
Raison : Manifester contre la censure d'Internet et appuyer le printemps arabe (13).

Opération Syrie (Syrie)
Démarche : Site Web du ministère de la Défense syrien altéré.
Raison : Appuyer le Printemps arabe (soulèvement en Syrie).

Opération Égypte (Égypte)
Démarche : Attaque DDoS lancée contre les sites Web du gouvernement égyptien et du Parti national démocratique. De plus, publication des noms et des mots de passe des comptes de courriel de hauts fonctionnaires du gouvernement.
Raison : Appuyer le Printemps arabe (soulèvement en Égypte).

HBGary Federal (É.-U.)

Démarche : Altération du site Web de HBGary, suppression de fichiers de l'entreprise, publication de 68 000 courriels d'employés.
Raison : Un représentant de HBGary a provoqué Anonymous en menaçant de divulguer des renseignements sur le groupe.

Banque d'Amérique (É.-U.)
Démarche : Des documents de nature sensible de la Banque d'Amérique, qui sont censés prouver des cas de corruption et de fraude à la banque, sont publiés en ligne.
Raison : Appuyer des allégations de corruption et de fraude au sein du système bancaire aux É.-U.

Opération Malaisie (Malaisie)
Démarche : Attaques DDoS lancées contre 91 sites Web du gouvernement de la Malaisie.
Raison : Répondre à la censure par le gouvernement de la Malaisie de sites tels que Pirate Bay (14) et WikiLeaks.

Occupons Wall Street (É.-U.)
Démarche : Attaques DDoS lancées contre les sites Web du service de police d'Oakland et de maire de St. Louis.
Raison : Manifester contre l'expulsion des manifestants des sites Occupons et appuyer le mouvement Occupons international.

Opération Mayhem (É.-U.)
Démarche : Virus Guy Fawkes diffusé sur Facebook.
Raison : Manifester contre le projet de loi Stop Online Piracy Act (15), la perception de violence policière dans le cadre des mouvements Occupons et toute forme d'opposition aux activités d'Anonymous.

Cox Communications (É.-U.)
Démarche : Serveurs DNS (Domain Name System) mis hors ligne, bloquant l'accès Internet de la plupart des clients dans le sud-ouest des É.-U.
Raison : Manifester contre la restriction par Cox Communications des quotas d'utilisation de données des clients.

Opération Blackout (É.-U.)
Démarche : En novembre, menaces proférées par Anonymous contre le gouvernement des É.-U.
Raison : Manifester contre le projet de loi Stop Online Piracy Act.

STRATFOR (à l'échelle mondiale)
Démarche : STRATFOR est une entreprise des É.-U. qui fournit des services aux organismes du renseignement et d'application de la loi et à d'autres clients. 200 Go de données sont volés sur les serveurs Web de STRATFOR et ensuite publiés. L'information volée comprend des numéros de cartes de crédit actives, des adresses de courriel, des numéros de téléphone, des mots de passe chiffrés et des renseignements de nature sensible des clients (y compris des ministères gouvernementaux et des services militaires). Anonymous compte faire des dons à des organismes de bienfaisance en utilisant les renseignements volés sur les cartes de crédit.
Raison : À la suite de l'incident HBGary, Anonyme a lancé une enquête sur ce qu'elle nomme une alliance entre l'État et le secteur privé contre le mouvement de l'information libre. En raison des liaisons de STRATFOR avec les secteurs de marchés militaires et du renseignement et les organismes gouvernementaux, Anonymous croit qu'en ciblant STRATFOR, il pourra améliorer sa capacité de poursuivre cette enquête et, ainsi, de divulguer d'autres cas de corruption, de crime et de pratiques trompeuses [soi-disant] de la part d'acteurs puissants situés aux É.-U. et ailleurs (16).

En cours :
Opération AntiSec (OTAN, Tunisie, Brésil, Australie, É.-U., Turquie, Royaume-Uni et autres pays)
Démarche : Aux É.-U., attaques DDoS contre le site Web de la CIA. Piratage du site Web du Sénat des É.-U. et publication de renseignements sur sa structure interne de serveurs. Au Royaume-Uni, attaques DDoS contre le site Web du Serious Organised Crime Agency (SOCA).

Raison : Déclaration de guerre cybernétique à l'échelle mondiale contre des gouvernements et des entreprises en réponse à la corruption et à la censure par le gouvernement perçues.

CANADA :
Anonymous a ciblé, directement et indirectement, le gouvernement, des administrations municipales et des entreprises privées du Canada. En voici des exemples :

Gouvernement du Canada :
STRATFOR (décembre 2011)
Le gouvernement fédéral est une cible indirecte des activités d'Anonymous relatives à STRATFOR. Divers ministères fédéraux consultent les ressources de STRATFOR. Des noms de compte et des mots de passe d'employés fédéraux figurent parmi les renseignements publiés par Anonymous (17).

Projet de loi C-11, Accord commercial relatif à la contrefaçon (ACRC) et Projet de loi C-30 (février 2012)
Le gouvernement fédéral a été ciblé directement par Anonymous, au moyen d'attaques DoS et de menaces fortement médiatisées contre le ministre de la Sécurité publique, en réponse au projet de loi C-11 (Loi sur la modernisation du droit d'auteur), à l'ACRC et au projet de loi C-30 (accès licite).

Administrations municipales :
Toronto (novembre 2011)
Anonymous a menacé de mettre hors ligne le site Web de la Ville de Toronto si les fonctionnaires expulsent les manifestants du camp Occupons Toronto. Aucune activité n'a été effectuée contre le site Web de la Ville de Toronto, mais le site Web du service de police de Toronto a été piraté et des noms de compte et des mots de passe ont été volés, possiblement en guise de représailles aux efforts continus pour expulser les manifestants du camp Occupons.

Entreprises privées :
Opération Green Rights et projet Tarmaggedon (juillet 2011)
En réponse à des préoccupations environnementales, Anonymous a ciblé des entreprises associées au pipeline Keystone XL et au projet de sables bitumineux en Alberta.

TECHNIQUES

Anonymous a traditionnellement utilisé des techniques de cybermenaces de base disponibles de sources ouvertes contre ses cibles. Par contre, à compter de la mi-2011, des Anons ont commencé à développer leurs propres maliciels. (Remarque : La liste d'attaques ci-dessous n'est pas exhaustive, puisqu'Anonymous compte un grand nombre de membres et que leurs activités ne peuvent pas toutes être tracées et attribuées à Anonymous.)

DoS et DDoS :
La méthode privilégiée d'Anonymous est de lancer des attaques DoS ou DDoS contre le site Web de la cible pour essayer de mettre son réseau hors ligne et d'empêcher l'accès au site par les utilisateurs légitimes. Voici les méthodes le plus souvent utilisées :

– /HOIC/JS LOIC/BOIC :
On encourage les Anons à télécharger et à lancer l'application Low Orbit Ion Cannon (LOIC) pour leur permettre de participer volontairement au réseau zombie. Le LOIC est pointé vers la cible choisie pour perturber le service de l'hôte. Toutefois, puisque le LOIC peut révéler les adresses IP de ses utilisateurs, Anonymous a cherché d'autres modes d'attaque, par exemple l'utilisation d'un mandataire d'anonymisation tel que TOR (The Onion Router). D'autres versions de l'application comprennent une version JavaScript, JS LOIC, et, plus récemment, une version fondée sur les favoris (nommée BOIC). Ces versions ne demandent guère plus qu'un clic pour inonder la cible avec un grand nombre de paquets GET et POST afin de créer un déni de service.

– Apache Killer :
L'outil de DoS Apache, surnommé Apache Killer, exploite une vulnérabilité qui permet aux attaquants à distance d'envoyer des requêtes à des serveurs au moyen d'un identificateur de ressource uniforme (URI) mal formé (20. Il est conçu pour surcharger la mémoire du serveur Web et, ainsi, mettre le site Web hors ligne. Il permet aussi à un attaquant à distance de mener une attaque DoS contre un serveur Apache à partir d'un seul ordinateur.

Attaques DoS et DDoS au moyen d'injections SQL :
– #RefRef :
Anonymous a développé et publié, en septembre 2011, un outil de DDoS en Perl, #RefRef, qui exploite des vulnérabilités de SQL (21). L'outil envoie des requêtes SQL mal formées, conçues pour surcharger les ressources du serveur, à un portail Web hébergé sur un serveur SQL. Par conséquent, le site Web est mis hors ligne. #RefRef peut être utilisé avec d'autres outils, par exemple, Havij, un outil d'injection SQL qui aide les vérificateurs de pénétration à trouver et à exploiter des vulnérabilités d'injection SQL. Ces attaques contre des vulnérabilités de SQL peuvent modifier le contenu de bases de données ou voler des données de bases de données (p. ex., renseignements sur les cartes de crédit ou mots de passe).

Virus Guy Fawkes :
Les membres d'Anonymous se sont aussi axés sur le développement de maliciels. Le virus Guy Fawkes (22) a été développé par des Anons pour prendre le contrôle d'un compte Facebook et s'en servir pour distribuer des maliciels à d'autres membres sans connexion réelle de l'utilisateur au site. Selon des analystes de la sécurité de l'entreprise de logiciels antivirus BitDefender, le virus Guy Fawkes (qu'ils nomment Backdoor-Bifrose-AAJX) peut s'injecter dans le processus d'Internet Explorer, donnant ainsi un accès sans entrave au système compromis. Il peut aussi enregistrer les frappes et perturber les opérations de logiciels antimaliciels connus. (Remarque : On croyait que le virus Guy Fawkes était responsable de l'attaque pornographique massive contre Facebook en novembre 2011, mais Facebook et BitDefender ont par la suite réfuté cette hypothèse. Anonymous affirme qu'il travaille encore à contrôler le virus en vue d'une utilisation ultérieure.)

Autre :
Anonymous utilise aussi d'autres techniques : ingénierie sociale pour obtenir l'accès aux systèmes des victimes (p. ex., HBGary Federal), altération de sites Web ciblés pour afficher des messages embarrassants, craquage de mots de passe pour extraire des renseignements de bases de données, utilisation d'un outil de détournement Twitter nommé Universal Rapid Gamma Emitter (URGE) pour détourner les sujets d'actualité sur Twitter vers des sujets d'intérêt à Anonymous, etc. L'outil URGE permet aussi aux Anons de poster des gazouillis sur ces sujets.

ATTÉNUATION
==========

Des pratiques solides en matière de sécurité de la TI aident à se protéger contre des menaces telles que celles présentées par le collectif hacktiviste Anonymous. Anonymous met généralement à profit des techniques en source ouverte ou des vulnérabilités bien connues. Les cibles sont généralement annoncées dans des forums ouverts (p. ex., Twitter, Pastebin) et dans les médias.
Nous encourageons les organisations à consulter les principes de prévention contre les menaces sophistiquées et persistantes et contre les attaques par déni de service du CCRIC aux adresses suivantes :
– http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-fra.aspx
– http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

De plus, les mesures d'atténuation suivantes sont disponibles pour se protéger contre certaines des techniques susmentionnées :

Apache Killer :

– Apache a publié des correctifs pour cette vulnérabilité. Nous recommandons à tous les utilisateurs de mettre leur système à niveau à la version 2.2.20 (ou plus récente) d'Apache.

#RefRef :
– Le code Web devrait être renforcé contre les injections SQL pour empêcher le serveur d'exécuter des requêtes SQL arbitraires provenant d'utilisateurs inconnus. Consultez les références sur les pratiques exemplaires, p. ex. l'Open Web Application Security Project (OWASP) – https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet (en anglais seulement).

NOTES DE FIN
==========

(1) IRC est un protocole de communication textuelle et de conférences en temps réel sur Internet. Il assure les communications de groupe ainsi que la messagerie privée et le partage de fichiers.

(2) Dans une attaque distribuée par déni de service (DDoS), de multiples systèmes attaquent une seule cible. Le déluge de messages entrants vers le système ciblé force sa fermeture et empêche la prestation de services aux utilisateurs légitimes.

(3) L'injection SQL est souvent utilisée pour attaquer la sécurité d'un site Web en injectant des commandes SQL dans la base de données d'une application.

(4) Les attaques du jour zéro essaient d'exploiter des vulnérabilités logicielles qui ne sont pas encore connues des développeurs du logiciel ou du grand public.

(5) Anon-ops assure la communication des annonces d'Anonymous.

(6) LulzSec était une petite équipe qui s'est associée à Anonynmous dans le cadre de la campagne à long terme Anti-Security (ou AntiSec). LulzSec a mis fin à ses activités à l'été 2011.

(7) LulzRaft a été inspiré par le groupe LulzSec et est responsable de l'altération du site Web du Parti conservateur du Canada et de l'accès aux renseignements privés sur les donateurs du parti. Ils ont aussi été liés à l'altération du site Web de l'entreprise d'énergie Husky Energy, établie à Calgary.

(8) Les porte-paroles officieux d'Anonymous comprennent Jake Davis (aussi connu sous son pseudonyme en ligne, « Topiary ») et Barrett Brown. Pour en savoir plus sur Jake Davis, consultez http://www.lefigaro.fr/hightech/2011/08/01/01007-20110801ARTFIG00418-piratage-des-lulzsec-un-anglais-de-18-ans-au-tribunal.php. Pour en savoir plus sur Barrett Brown, consultez http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx (en anglais).

(9) Selon des sources d'information ouvertes, LOIC est une application d'essais sous contrainte de réseau en source libre qui permet d'effectuer des attaques DoS ou DDoS contre un site cible en l'inondant de paquets TCP ou UDP pour perturber ses services.

(10) HBGary Federal est une entreprise de sécurité de la technologie qui collaborait avec le FBI pour démasquer les membres d'Anonymous. En février 2011, le PDG, Aaron Barr, a révélé leur intention de publier des renseignements sur l'identité des membres d'Anonymous. Par conséquent, des membres d'Anonymous ont compromis le site Web de HBGary et ont volé et publié des documents et des courriels de l'entreprise.

(11) Selon des sources d'information ouvertes, le mouvement Occupons désigne un mouvement international de manifestation contre les taux de chômage élevés, l'inégalité sociale et économique et la corruption perçue au sein des entreprises et des gouvernements.

(12) Pour en savoir plus, consultez http://www.branchez-vous.com/techno/actualite/2011/04/anonymous-sony-playstation-3-piratage-geohot-cyberattaque.html.

(13) Le terme printemps arabe désigne des manifestations révolutionnaires dans le monde arabe à partir de décembre 2010. Les pays touchés comprennent la Tunisie, l'Égypte, la Lybie, Bahreïn, la Syrie, le Yémen, l'Algérie, l'Iraq, la Jordanie, le Koweït, le Maroc, Oman, le Liban et l'Arabie saoudite.

(14) The Pirate Bay est un site Web suédois notoire qui facilite les téléchargements illégaux et appuie le mouvement international contre le droit d'auteur.

(15) Stop Online Piracy Act (SOPA) est un projet de loi des É.-U. pour combattre la distribution en ligne de propriété intellectuelle protégée par le droit d'auteur. Anonymous le considère comme une tentative de censure d'Internet.

(16) Pour obtenir l'explication complète d'Anonymous, consultez la déclaration de Barrett Brown à http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-hacked.

(17) Le Centre d'évaluation des cybermenaces (CECM) a fourni des mesures d'atténuation aux employés des ministères touchés.

(18) Ce projet de soi est semblable aux projets de loi C-50, C-51 et C-52 précédents.

(19) L'opération Facebook a été lancée le 5 novembre 2011 parce qu'Anonymous croit que « Facebook est à l'opposé des valeurs d'AntiSec ».

(20) Pour en savoir plus, consultez le bulletin CVE-2011-3192 à http://nvd.nist.gov/ (en anglais).

(21) Un serveur SQL est un serveur de base de données relationnelle qui peut stocker et récupérer des données sur un réseau (p. ex., Internet). Les requêtes provenant des ordinateurs clients sont formatées dans le langage SQL.

(22) Guy Fawkes était associé à la Conspiration des poudres (« Gunpowder Plot »), une tentative infructueuse d'assassinat du roi James I d'Angleterre en 1605. Le projet des conspirateurs était de faire sauter le Parlement pour tuer le roi et les membres du Parlement. Les Anons ont d'ailleurs adopté comme symbole le masque de Guy Fawkes, facilement accessible et bon marché.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118
Télécopieur : 613-998-9589
Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: GOC-COG@OPSCEN.GC.CA

Pilon, Claude

From: Pilon, Claude s.15(1)
Sent: Thursday, March 01, 2012 1:41 PM
To: 'mark.scrivens@justice.gc.ca' (mark.scrivens@justice.gc.ca); [redacted]; Audcent, Karen (kaudcent@justice.gc.ca)
Subject: FW: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous

FYI

Claude Pilon, B.Sc., LL.L, LL.B
Counsel / Avocat
Public Safety Canada Legal Services / Services juridiques de Sécurité publique Canada
(613) 991-4364 / claude.pilon@ps-sp.gc.ca
PROTECTED: SOLICITOR-CLIENT PRIVILEGE/PROTÉGÉ: PRIVILÉGE DU SECRET PROFESSIONNEL DE L'AVOCAT

Please feel free to reply in the official language of your choice/ N'hésitez pas à me répondre dans la langue officielle de votre choix

-----Original Message-----
From: GOC-COG
Sent: March-01-12 1:25 PM
To: _GOC Distribution List / Liste de distribution du COG
Subject: CCIRC INFORMATION NOTE IN12-501: Overview of the Hacktivist Group "Anonymous" / CCRIC NOTE D'INFORMATION IN12-501: Aperçu du collectif d'hacktivistes Anonymous

(La version française suit)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
INFORMATION NOTE
****

Number: IN12-501
Date: 1 March 2012

****
Overview of the Hacktivist Group "Anonymous"
****

PURPOSE
========

The purpose of this report is to provide an overview of the hacktivist group "Anonymous." It contains information on its organizational structure, tradecraft and targets; the threat to Canadian Critical Infrastructure systems; and recommended mitigation.

ASSESSMENT

==========

EXECUTIVE SUMMARY

Anonymous targets governments, private firms and individuals whose activities or purposes appear to be in conflict with principles espoused by the group. These principles mainly focus on: civil rights (e.g. oppressive regimes); information accessibility (e.g. Internet censorship); and other causes associated with perceived social injustice.

Based on a view of previous targeting by Anonymous, Canadian critical infrastructure systems could be targeted due to government legislative and regulatory initiatives (e.g. the Copyright Modernization Act) and initiatives that may result in activist opposition (e.g. environmental or social issues).

Anonymous uses a number of capabilities against its targets. These include, but are not limited to, distributed denial-of-service attacks (DDoS)(2), password cracking, SQL injections(3) and malware (virus) deployments. Canadian organizations have been both direct and indirect targets of Anonymous activity. For example, the Toronto Police Service website was hacked in 2011, likely in response to the "Occupy Toronto" camp evictions; Canadian corporations involved with the Alberta Tar Sands have been targeted, in particular to protest against the Keystone XL pipeline; and subsequent to a late-2011 breach of STRATFOR, a US corporation with links to intelligence and law enforcement organizations, credentials used by Canadian organizations to access STRATFOR databases were published. Although Anonymous leverages a variety of tradecraft to achieve its aims, strong IT security practices will help to defend against Anonymous exploits. The majority of these exploits are not leveraging zero-day(4).

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their agendas. Most notably, "Anonymous" is a term that refers to a group of activist hackers, or hacktivists, that poses a wide range of cyber threats to government and commercial organizations around the world. Anonymous' agenda has included initiating cyber threat activities in protest of perceived government-mandated Internet censorship and in support of worldwide activist movements.

STRUCTURE

Anonymous is loosely composed of sub-groups (e.g. Anon-ops5, LulzSec6) and often conducts joint campaigns with other hacktivist groups in support of the same agenda. For example, TeaMp0isoN and People's Liberation Front are separate hacktivist groups with the freedom to opt-in or opt-out of projects conducted jointly with Anonymous. The Anonymous movement has also inspired copycat actions from other hacktivist groups, such as LulzRaft7.

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several unofficial spokespeople(8), Anonymous does not officially have a specific spokesperson. The only requirement for members of Anonymous (known as "Anons") is that they must always remain anonymous while participating in cyber campaigns supporting Anonymous' efforts. In many cases, Anons voluntarily join a botnet by downloading and installing the Low Orbit Ion Cannon (LOIC)(9) onto their computers. (Comment: The absence of a defined leadership structure is possibly why some threats associated with Anonymous are carried out, whereas others become empty threats if general consensus of a target was not agreed upon by the group at large.)

CHOOSING TARGETS

Since Anonymous is decentralized, new targets are determined in a variety of ways. Some of the most commonly used and documented methods of selecting targets are listed below.

- Through consensus among Anons using online polls. Following a discussion on an IRC, an online poll will be conducted to determine the target(s) of DoS/DDoS attacks. Although it appears to be a democratic process, elite Anons who are IRC channel operators are the ones who make the final decision about where to direct the LOIC attacks.
- As a response to perceptions of direct or indirect provocation by governments, by other hacking groups or companies (e.g. HBGary(10)), against the group as a whole, or against the principles to which Anonymous adheres.
- By exposing poor security practices. For instance, Anonymous members may use "Google Hacking" to identify vulnerable targets of opportunity. Results of such reconnaissance activities are often posted ans shared using sites such as pastebin.com .

These targeting practices are generally implemented in support of a specific Anonymous objective or campaign. For instance, one key Anonymous raison-d'être is to promote the ongoing "Operation Anti-Security" (also known as "AntiSec"), which is a declaration of cyber warfare on governments and corporations in response to perceived corruption and Internet censorship. As part of this campaign, Anonymous members are encouraged to locate and leak classified government information and to target banks or other high-profile establishments.

PAST TARGETS/BEHAVIOUR

Anonymous has initiated cyber threat activities in protest of government decisions and in support of their own principles. Recently, its hacktivism efforts have been concentrated on the various Occupy(11) movements, protesting Internet censorship and Internet filtering, protesting against oppressive regimes, and supporting WikiLeaks. These campaigns include:

2008:
Project Chanology (worldwide)
Action: DDoS attacks were launched against the Church of Scientology websites and non-violent protests worldwide.
Reason: The Church of Scientology was attempting to restrict access to information that it found embarrassing and was readily available on the Internet.

2009:
Anonymous Iran (Iran)
Action: An Iranian Green Party Support site, Anonymous Iran, was created to provide covert resources and event updates for Iranian protestors during government-imposed Internet information censorship.
Reason: To provide support to Iranian protestors against a regime perceived to be corrupt.

Operation Didgeridie (Australia)
Action: A DDoS attack was launched against the Australian prime minister's website.

Reason: To protest against proposed government policy and legislation related to the implementation of ISP-level blacklists.

2010:
Operation Titstorm (Australia)
Action: A DDoS attack was launched against the Australian parliament's website and the prime minister's website was defaced.
Reason: To protest against the implementation of an Internet filter that would block websites containing child abuse material and certain types of pornography.

Operation Payback / Operation Sony (worldwide)
Action: DDoS attacks were launched against Sony PlayStation websites.
Reason: To support online file-sharing and to retaliate against Sony for seeking legal action against two individuals who successfully hacked the PlayStation3 system to allow users to run generic applications(12).

Operation Avenge Assange (US)
Action: DDoS attacks were launched against Amazon, PayPal, MasterCard and Visa websites.
Reason: To show support for WikiLeaks and to protest against its founder's arrest.

Operation Zimbabwe (Zimbabwe)
Action: DDoS attacks were launched against the Government of the Republic of Zimbabwe's websites.
Reason: To protest against censorship of WikiLeaks documents.

2011:
Operation Tunisia (Tunisia)
Action: DDoS attacks were launched on the Government of Tunisia's websites.
Reason: To protest against Internet censorship and to support the Arab Spring(13).

Operation Syria (Syria)
Action: Website of the Syrian Defence Ministry website was defaced.
Reason: To support the Arab Spring (Syrian uprising).

Operation Egypt (Egypt)
Action: A DDoS attack was launched against the Government of Egypt's website and the National Democratic Party's website. Also, the names and passwords of email addresses of government officials were released.
Reason: To support the Arab Spring (Egyptian revolution).

HBGary Federal (US)
Action: HBGary's website was defaced, company files were deleted and 68,000 employee emails were published.
Reason: An HBGary official provoked Anonymous by threatening to expose information about the group.

Bank Of America (US)
Action: Sensitive Bank of America documents were released online, which allegedly proved cases of corruption and fraud at the bank.
Reason: To protest in support of allegations of corruption and fraud within the US banking system.

Operation Malaysia (Malaysia)
Action: DDoS attacks were launched on 91 Government of Malaysia's websites.
Reason: In response to the Malaysian government's censorship of sites such as Pirate Bay(14) and WikiLeaks.

Occupy Wall Street (US)
Action: DDoS attacks were launched on the Oakland Police Department website and the St. Louis mayor's website.

Reason: To protest evictions of protestors from Occupy sites, in support of the worldwide Occupy movement.

Operation Mayhem (US)
Action: Guy Fawkes virus was released on Facebook.
Reason: To protest the Stop Online Piracy Act(15), perceptions of police violence towards protestors in Occupy movements and any opposition to Anonymous activities.

Cox Communications (US)
Action: Domain Name System (DNS) servers were taken offline, removing Internet access for clientele in most of southwest America.
Reason: To protest Cox Communications' attempted regulation of customers' data usage quota.

Operation Blackout (US)
Action: In November, Anonymous threatened action against the US government.
Reason: To protest against the Stop Online Piracy Act.

STRATFOR (worldwide)
Action: STRATFOR is a US company that provides services to intelligence and law enforcement agencies, among others. Two hundred gigabytes of data was stolen from STRATFOR's web servers and subsequently published. The stolen information included active credit cards, e-mail addresses, phone numbers, encrypted passwords and sensitive information from clients (including government and military departments). Anonymous planned to donate to charities using the stolen credit card information.
Reason: Following the HBGary incident, Anonymous began to investigate what it refers to as a "state-corporate alliance against the free information movement." Due to STRATFOR's ties with the intelligence and military contracting sectors and government agencies, Anonymous believed that targeting STRATFOR would "improve [their] ability to continue this investigation and thereby bring to light other instances of [perceived] corruption, crime and deception on the part of certain powerful actors based in the US and elsewhere(16)."

Ongoing:
Operation Antisec (NATO, Tunisia, Brazil, Australia, US, Turkey, UK, and other countries)
Action: In the US, DDoS attacks were launched against the Central Intelligence Agency's (CIA) website, the US Senate website was hacked and information about its internal server structure was released. In the UK, DDoS attacks were launched against the Serious Organised Crime Agency's (SOCA) website.
Reason: The declaration of cyber warfare on governments and corporations worldwide in response to perceived corruption and government censorship.

CANADA:
Anonymous has directly and indirectly targeted the Government of Canada, Canada's municipal governments and Canadian private corporations. Examples include:

Government of Canada:
STRATFOR (December 2011)
The federal government has been an indirect target of Anonymous activity in connection with STRATFOR. STRATFOR is a resource used by various federal departments. When usernames and passwords were released by Anonymous, some of them included those of federal employees(17).

Bill C-11, ACTA and Bill C-30 (February 2012):
The federal government was directly targeted by Anonymous in relation to the Bill-C-11 (Copyright Modernization Act), ACTA and C-30 (Lawful Access Package) through denial of service attacks and threats against the Public Safety Minister extensively covered in the media.

Municipal Governments:

Toronto (November 2011)
Anonymous threatened to take down the City of Toronto's website if officials evicted protestors from the Occupy Toronto camp. Although no known activity was conducted against the City of Toronto's website, the Toronto Police Service website was hacked and several usernames and passwords were stolen, possibly in retaliation to the continued efforts to evict the Occupy camp.

Private Corporations:
Operation Green Rights/ Project Tarmaggedon (July 2011)
In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline and the Alberta Tar Sands project.

TRADECRAFT

Anonymous has traditionally used basic, open-source-available cyber threat tradecraft against their targets. However, beginning in mid-2011, Anons have begun developing their own malware. (Comment: The exploits below do not represent a conclusive list because Anonymous has a large number of members and all of their activities cannot be tracked and attributed to Anonymous.)

DoS/DDoS:
Anonymous' usual method of choice is to launch DoS/DDoS attacks against a target's website in an effort to bring the network offline and to make the website unavailable to legitimate users. Two commonly used methods include:

- LOIC/HOIC/JS LOIC/BOIC:
Anons are encouraged to download and launch the Low Orbit Ion Cannon application enabling them to willingly participate in a botnet. The LOIC is pointed at a target of choice, which then disrupts the service of the victim's host. However, since LOIC can reveal the IP addresses of its users, its traceability has prompted Anonymous to find other means of attacks such as encouraging the use of anonymization proxy like TOR (The onion router). Other versions of the tool include a Javascript version, JS LOIC, and most recently, a Bookmark-based version coined BOIC. These versions require little more than one mouse-click to flood a target with GET and POST packets aimed at creating a denial of service condition.

- Apache Killer:
The Apache DoS tool nicknamed the "Apache Killer" exploits a vulnerability that allows remote attackers to send requests to servers via a malformed uniform resource identifier (URI)(20). It is designed to drain the web server's memory, which would then take the website offline. It also allows a remote attacker to use a single computer to wage DoS attacks against an Apache server.

DoS/DDoS via SQL Injections:
- #RefRef:
Anonymous developed and released a Perl DDoS tool in September 2011, #RefRef, that exploits SQL(21) vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline. #RefRef could be used in combination with tools such as Havij, an SQL Injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities. As a result of SQL vulnerability exploitation, database content could be changed, or database information (such as credit card information or passwords) could be stolen.

Guy Fawkes Virus:
Malware development is also something that Anonymous members have been focusing on. The Guy Fawkes(22) virus was developed by Anon to take control of a Facebook account and use it to spread malware to other members without

the users actually logging onto the site. According to security analysts at the antivirus software company BitDefender, the Guy Fawkes virus (which they have named Backdoor-Bifrose-AAJX) has the ability to inject itself in the Internet Explorer process, providing a remote attacker with unhindered access to the compromised system. It would also record keystrokes and disrupt processes of known antimalware software. (Comment: Although the Guy Fawkes virus was previously believed to be responsible for the massive pornographic spam attack against Facebook in November 2011, this was later refuted by Facebook and BitDefender. Anonymous has stated that it is still working to control the virus to be used at a later date.)

Other:
Other techniques used by Anonymous include using social engineering techniques to gain access to victims' systems (e.g. HBGary Federal), using web defacement to post embarrassing messages on victims' websites, using password cracking to exfiltrate data from a victim's database, and using a Twitter raiding tool called Universal Rapid Gamma Emitter (URGE) to hijack Twitter trending topics into topics of interest to Anonymous. It also allows Anons to tweet messages within the topics.

MITIGATION

Strong IT security practices will go a long way to defending against threats such as the Anonymous hacktivist collective. Anonymous generally leverages open source or well-known vulnerabilities. The nature of the targets is also generally advertised in open forums such as Twitter and Pastebin, as well as main stream media.
Organizations are encouraged to consult CCIRC's mitigation guidelines for advanced persistent threats and DDoS attacks found here:
- http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx
- http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

In addition, the following mitigation is available for some of the tradecraft specifically noted above:

Apache Killer
- Apache has since released patches to fix this vulnerability. All users are recommended to upgrade to Apache 2.2.20 or higher.

#RefRef
- Webcode should be hardened against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users. Consult best practices references such as the Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)

ENDNOTES

(1) IRC is a protocol for Internet text messaging and synchronous conferencing. It allows group communications as well as private messaging and file sharing.

(2) A distributed denial-of-service (DDoS) attack is one in which a multitude of systems attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.

(3) SQL injection is often used to attack the security of a website by injecting SQL commands into the database of an application.

(4) Zero-day threats attempt to exploit new computer application vulnerabilities not yet known to the software developer or the general public.

(5) Anon-ops provides communications for Anonymous' announcements.

(6) LulzSec was a small team that joined forces with Anonymous in the ongoing "Operation Anti-Security" or "AntiSec" campaign, which later disbanded in the summer of 2011.

(7) LulzRaft was inspired by LulzSec group and has been responsible for web defacement of the Conservative Party of Canada's website and for accessing private information about the party's donors. They have also been linked to web defacement of Calgary-based energy company Husky Energy's website. s.19(1)

(8) Unofficial spokespeople for Anonymous include [redacted] and [redacted]. For more information on [redacted], please see http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-ukpolice/. For more information on [redacted] please see http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx.

(9) According to open source, LOIC is an open source network stress testing application that performs DoS or DDoS attacks on a target site by flooding the server with TCP or UDP packets to disrupt the service of a host.

(10) HBGary Federal is a technology security company that was working with the FBI to unmask members of Anonymous. In February 2011, the CEO, [redacted] revealed an intention to release information on the identities of Anonymous members. As a result, Anonymous members compromised the HBGary website and stole and publicly released the company's documents and emails.

(11) According to open source, the Occupy movement refers to an international protest movement directed against high unemployment, social and economic inequality and perceived corruption in corporations and government.

(12) For more information, please refer to http://www.pcmag.com/article2/0,2817,2383018,88.asp.

(13) The Arab Spring refers to revolutionary protests occurring in the Arab world beginning in December 2010. Countries affected include Tunisia, Egypt, Libya, Bahrain, Syria, Yemen, Algeria, Iraq, Jordan, Kuwait, Morocco, Oman, Lebanon and Saudi Arabia.

(14) The Pirate Bay is a Swedish website known for facilitating illegal downloads and supporting the international anti-copyright movement.

(15) The Stop Online Piracy Act is proposed US legislation to combat against the online distribution of copyrighted intellectual property. This has been viewed by Anonymous as an attempt to censor the Internet.

(16) For the full explanation, please refer to Barrett Brown's statement at http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-hacked.

(17) CTEC has provided mitigation to employees of the affected departments.

(18) This legislation will be similar to previous bills: Bill C-50, Bill C-51 and Bill C-52.

(19) Operation Facebook was launched on November 5, 2011, because Anonymous believes that "Facebook is the opposite of the Antisec cause."

(20) For more information, please refer to CVE-2011-3192 at http://nvd.nist.gov/.

(21) An SQL server is a relational database server that can store and retrieve data across a network (e.g. the Internet). Queries from client machines are formatted in the SQL language.

(22) Guy Fawkes was associated with the Gunpowder Plot, a failed assassination attempt against King James I of England in 1605. The conspirators' plan was to blow up the Houses of Parliament in order to kill the King and the Members of Parliament. Coincidentally, Anons have adopted the easily available and inexpensive Guy Fawkes mask as their symbol.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquires into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

****

SÉCURITÉ PUBLIQUE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

****
NOTE D'INFORMATION
****

Numéro : IN12-501
Date : 1 mars 2012

****
Aperçu du collectif d'hacktivistes Anonymous
****

OBJECTIF

Le présent rapport donne un aperçu du groupe d'hacktivistes Anonymous. Il présente des renseignements sur sa structure organisationnelle, ses techniques et ses cibles, sur la menace qu'il pose pour les systèmes d'infrastructures essentielles du Canada et sur les mesures d'atténuation recommandées.

ÉVALUATION

SOMMAIRE

Anonymous cible les gouvernements, les entreprises privées et les particuliers dont les activités ou les buts semblent être en conflit avec les principes énoncés par le groupe. Ces principes sont axés sur les droits civils (p. ex., régimes oppressifs), l'accès à l'information (p. ex., censure sur Internet) et d'autres causes liées aux injustices sociales perçues.

Compte tenu des cibles précédentes d'Anonymous, les systèmes des infrastructures essentielles du Canada pourraient être ciblés en raison des initiatives législatives et réglementaires du gouvernement (p. ex., Loi sur la modernisation du droit d'auteur) et d'initiatives qui pourraient provoquer une opposition militante (p. ex, enjeux sociaux ou environnementaux).

Anonymous utilise diverses capacités contre ses cibles : attaques distribuées par déni de service (DDoS) (2), craquage de mots de passe, injections SQL (3), déploiements de maliciels (virus), etc. Des organisations canadiennes ont été ciblées directement et indirectement par des activités d'Anonymous. Par exemple, le site Web du service de police de Toronto a été piraté en 2011, probablement en réponse aux expulsions du camp Occupons Toronto; des entreprises canadiennes qui participent à l'exploitation des sables bitumineux en Alberta ont été ciblées, en particulier pour manifester contre le pipeline Keystone XL; et, à la suite de l'attaque à la fin 2011 contre STRATFOR, une entreprise des É.-U. avec des liens avec les organismes de renseignement et d'application de la loi, les justificatifs utilisés par des entreprises canadiennes pour accéder aux bases de données de STRATFOR ont été publiés. Anonymous utilise diverses techniques pour réaliser ses objectifs, mais des pratiques solides en matière de sécurité de la TI aident à se protéger contre ces attaques. La majorité des attaques ne tirent pas profit de vulnérabilités du jour zéro (4).

APERÇU

Les pirates militants poursuivent de plus en plus des activités de menaces cybernétiques pour atteindre leurs objectifs. En particulier, le terme « Anonymous » fait référence à un groupe de pirates militants (hacktivistes) qui font peser un large éventail de cybermenaces sur les gouvernements et les organisations commerciales partout au monde. Le programme d'Anonymous a compris l'utilisation de cybermenaces pour manifester contre la censure gouvernementale perçue sur Internet et appuyer des mouvements militants internationaux.

STRUCTURE

Anonymous comprend un ensemble hétérogène de sous-groupes (p. ex., Anon-ops5, LulzSec6) et mène souvent des campagnes en collaboration avec d'autres groupes hacktivistes qui partagent les mêmes objectifs. Par exemple, TeaMp0isoN et le People's Liberation Front sont des groupes hacktivistes distincts qui sont libres de participer ou non à des projets conjoints avec Anonymous. Le mouvement Anonymous a aussi été imité par d'autres groupes hacktivistes, par exemple, LulzRaft7.

Anonymous n'est pas organisé hiérarchiquement et n'a pas de chefs définis. De plus, Anonymous n'a pas de porte-parole officiel, même s'il y a plusieurs porte-paroles officieux (8). La seule exigence que les membres d'Anonymous (les « Anons ») doivent respecter est de garder l'anonymat lorsqu'ils participent à des campagnes cybernétiques pour appuyer les efforts du groupe. Dans de nombreux cas, les Anons se joignent volontairement à un réseau zombie en téléchargeant et en installant l'application LOIC (Low Orbit Ion Cannon) (9) sur leur ordinateur. (Remarque : L'absence d'une structure de direction définie peut expliquer pourquoi certaines menaces associées à Anonymous sont mises à exécution, alors que d'autres n'aboutissent pas si un consensus au sujet d'une cible ne se dégage pas parmi les membres.)

SÉLECTION DE CIBLES

Puisqu'Anonymous est décentralisé, les nouvelles cibles sont fixées de diverses façons. Voici certaines méthodes souvent utilisées et bien documentées de sélection de cibles :

– Consensus des membres dégagé au moyen de sondages en ligne. Après une période de discussion par l'intermédiaire du service de clavardage IRC, un sondage en ligne est réalisé pour fixer les cibles d'attaques de déni de service (DoS) ou de DDoS. Le processus peut sembler démocratique, mais ce sont les Anons d'élite qui exploitent les canaux IRC qui prennent la décision définitive sur la cible des attaques effectuées au moyen de LOIC.
– En réponse à une provocation directe ou indirecte perçue de la part de gouvernements, d'autres groupes pirates ou d'entreprises (p. ex., HBGary (10)) contre le groupe Anonymous ou ses principes.
– Pour exposer de mauvaises pratiques en matière de sécurité. Par exemple, les membres d'Anonymous peuvent utiliser la technique « Google hacking » pour détecter des cibles intéressantes. Les résultats de ces activités de reconnaissance sont souvent publiés sur des sites tels que pastebin.com.

Ces pratiques de ciblage sont généralement mises en œuvre pour appuyer un objectif ou une campagne en particulier d'Anonymous. Par exemple, une raison d'être importante d'Anonymous est de promouvoir l'opération « Anti-Security » (ou AntiSec), une déclaration de cyberguerre contre les gouvernements et les entreprises en réponse à une corruption ou à une censure Internet perçues. Dans le cadre de cette campagne, Anonymous encourage ses membres à trouver et à divulguer des renseignements gouvernementaux confidentiels et de cibler des banques et d'autres établissements bien en vue.

CIBLES ET COMPORTEMENTS DANS LE PASSÉ

Anonymous a lancé des activités de cybermenaces pour manifester contre des décisions gouvernementales et pour appuyer ses propres principes. Plus récemment, ces efforts hacktivistes appuyaient les divers mouvements Occupons (11) et WikiLeaks et s'opposaient à la censure et au filtrage d'Internet ainsi qu'aux régimes oppressifs. Voici un aperçu de certaines de certaines campagnes :

2008 :
Projet Chanalogy (à l'échelle mondiale)
Démarche : Attaques DDoS lancées contre les sites Web de l'église de Scientologie et manifestations non violentes à l'échelle mondiale.
Raison : L'Église de Scientologie essayait de limiter l'accès à des informations disponible sur Internet qu'elle jugeait embarrassantes.

2009 :
Anonymous Iran (Iran)
Démarche : Création d'Anonymous Iran, un site d'appui du Parti vert d'Iran, pour fournir des ressources clandestines et des renseignements sur les événements aux manifestants iraniens dans le cadre de la censure des renseignements Internet imposée par le gouvernement.

Raison : Appuyer les manifestants iraniens contre un régime perçu comme corrompu.

Opération Didgeridie (Australie)
Démarche : Attaque DDoS lancée contre le site Web du premier ministre australien.
Raison : Manifester contre la politique et les lois proposées relatives à la mise en œuvre de listes noires au niveau des FSI.

2010 :
Opération Titstorm (Autralie)
Démarche : Attaque DDoS lancée contre les sites Web du Parlement australien et altération du site Web du premier ministre australien.
Raison : Manifester contre la mise en œuvre d'un filtre Internet qui bloquerait les sites Web présentant de mauvais traitements d'enfants et certains types de pornographie.

Opérations Payback et Sony (à l'échelle mondiale)
Démarche : Attaques DDoS lancées contre les sites Web de Sony PlayStation.
Raison : Appuyer le partage de fichiers en ligne et exercer des représailles sur Sony pour avoir intenté des poursuites contre deux personnes qui avaient réussi à débrider le système PlayStation 3 pour permettre aux utilisateurs d'exécuter des applications génériques (12).

Opération Riposte Assange (« Avenge Assange ») (É.-U.)
Démarche : Attaques DDoS lancées contre les sites Web d'Amazon, de PayPal, de MasterCard et de Visa.
Raison : Manifester du soutien à l'égard de WikiLeaks et manifester contre l'arrestation de son fondateur.

Opération Zimbabwe (Zimbabwe)
Démarche : Attaques DDoS lancées contre les sites Web de la République du Zimbabwe.
Raison : Manifester contre la censure des documents de WikiLeaks.

2011 :
Opération Tunisie (Tunisie)
Démarche : Attaques DDoS lancées contre les sites Web du gouvernement de la Tunisie.
Raison : Manifester contre la censure d'Internet et appuyer le printemps arabe (13).

Opération Syrie (Syrie)
Démarche : Site Web du ministère de la Défense syrien altéré.
Raison : Appuyer le Printemps arabe (soulèvement en Syrie).

Opération Égypte (Égypte)
Démarche : Attaque DDoS lancée contre les sites Web du gouvernement égyptien et du Parti national démocratique. De plus, publication des noms et des mots de passe des comptes de courriel de hauts fonctionnaires du gouvernement.
Raison : Appuyer le Printemps arabe (soulèvement en Égypte).

HBGary Federal (É.-U.)
Démarche : Altération du site Web de HBGary, suppression de fichiers de l'entreprise, publication de 68 000 courriels d'employés.
Raison : Un représentant de HBGary a provoqué Anonymous en menaçant de divulguer des renseignements sur le groupe.

Banque d'Amérique (É.-U.)
Démarche : Des documents de nature sensible de la Banque d'Amérique, qui sont censés prouver des cas de corruption et de fraude à la banque, sont publiés en ligne.
Raison : Appuyer des allégations de corruption et de fraude au sein du système bancaire aux É.-U.

Opération Malaisie (Malaisie)
Démarche : Attaques DDoS lancées contre 91 sites Web du gouvernement de la Malaisie.
Raison : Répondre à la censure par le gouvernement de la Malaisie de sites tels que Pirate Bay (14) et WikiLeaks.

Occupons Wall Street (É.-U.)
Démarche : Attaques DDoS lancées contre les sites Web du service de police d'Oakland et de maire de St. Louis.
Raison : Manifester contre l'expulsion des manifestants des sites Occupons et appuyer le mouvement Occupons international.

Opération Mayhem (É.-U.)
Démarche : Virus Guy Fawkes diffusé sur Facebook.
Raison : Manifester contre le projet de loi Stop Online Piracy Act (15), la perception de violence policière dans le cadre des mouvements Occupons et toute forme d'opposition aux activités d'Anonymous.

Cox Communications (É.-U.)
Démarche : Serveurs DNS (Domain Name System) mis hors ligne, bloquant l'accès Internet de la plupart des clients dans le sud-ouest des É.-U.
Raison : Manifester contre la restriction par Cox Communications des quotas d'utilisation de données des clients.

Opération Blackout (É.-U.)
Démarche : En novembre, menaces proférées par Anonymous contre le gouvernement des É.-U.
Raison : Manifester contre le projet de loi Stop Online Piracy Act.

STRATFOR (à l'échelle mondiale)
Démarche : STRATFOR est une entreprise des É.-U. qui fournit des services aux organismes du renseignement et d'application de la loi et à d'autres clients. 200 Go de données sont volés sur les serveurs Web de STRATFOR et ensuite publiés. L'information volée comprend des numéros de cartes de crédit actives, des adresses de courriel, des numéros de téléphone, des mots de passe chiffrés et des renseignements de nature sensible des clients (y compris des ministères gouvernementaux et des services militaires). Anonymous compte faire des dons à des organismes de bienfaisance en utilisant les renseignements volés sur les cartes de crédit.
Raison : À la suite de l'incident HBGary, Anonyme a lancé une enquête sur ce qu'elle nomme une alliance entre l'État et le secteur privé contre le mouvement de l'information libre. En raison des liaisons de STRATFOR avec les secteurs de marchés militaires et du renseignement et les organismes gouvernementaux, Anonymous croit qu'en ciblant STRATFOR, il pourra améliorer sa capacité de poursuivre cette enquête et, ainsi, de divulguer d'autres cas de corruption, de crime et de pratiques trompeuses [soi-disant] de la part d'acteurs puissants situés aux É.-U. et ailleurs (16).

En cours :
Opération AntiSec (OTAN, Tunisie, Brésil, Australie, É.-U., Turquie, Royaume-Uni et autres pays)
Démarche : Aux É.-U., attaques DDoS contre le site Web de la CIA. Piratage du site Web du Sénat des É.-U. et publication de renseignements sur sa structure interne de serveurs. Au Royaume-Uni, attaques DDoS contre le site Web du Serious Organised Crime Agency (SOCA).
Raison : Déclaration de guerre cybernétique à l'échelle mondiale contre des gouvernements et des entreprises en réponse à la corruption et à la censure par le gouvernement perçues.

CANADA :
Anonymous a ciblé, directement et indirectement, le gouvernement, des administrations municipales et des entreprises privées du Canada. En voici des exemples :

Gouvernement du Canada :
STRATFOR (décembre 2011)

Le gouvernement fédéral est une cible indirecte des activités d'Anonymous relatives à STRATFOR. Divers ministères fédéraux consultent les ressources de STRATFOR. Des noms de compte et des mots de passe d'employés fédéraux figurent parmi les renseignements publiés par Anonymous (17).

Projet de loi C-11, Accord commercial relatif à la contrefaçon (ACRC) et Projet de loi C-30 (février 2012)
Le gouvernement fédéral a été ciblé directement par Anonymous, au moyen d'attaques DoS et de menaces fortement médiatisées contre le ministre de la Sécurité publique, en réponse au projet de loi C-11 (Loi sur la modernisation du droit d'auteur), à l'ACRC et au projet de loi C-30 (accès licite).

Administrations municipales :
Toronto (novembre 2011)
Anonymous a menacé de mettre hors ligne le site Web de la Ville de Toronto si les fonctionnaires expulsent les manifestants du camp Occupons Toronto. Aucune activité n'a été effectuée contre le site Web de la Ville de Toronto, mais le site Web du service de police de Toronto a été piraté et des noms de compte et des mots de passe ont été volés, possiblement en guise de représailles aux efforts continus pour expulser les manifestants du camp Occupons.

Entreprises privées :
Opération Green Rights et projet Tarmaggedon (juillet 2011)
En réponse à des préoccupations environnementales, Anonymous a ciblé des entreprises associées au pipeline Keystone XL et au projet de sables bitumineux en Alberta.

TECHNIQUES

Anonymous a traditionnellement utilisé des techniques de cybermenaces de base disponibles de sources ouvertes contre ses cibles. Par contre, à compter de la mi-2011, des Anons ont commencé à développer leurs propres maliciels. (Remarque : La liste d'attaques ci-dessous n'est pas exhaustive, puisqu'Anonymous compte un grand nombre de membres et que leurs activités ne peuvent pas toutes être tracées et attribuées à Anonymous.)

DoS et DDoS :
La méthode privilégiée d'Anonymous est de lancer des attaques DoS ou DDoS contre le site Web de la cible pour essayer de mettre son réseau hors ligne et d'empêcher l'accès au site par les utilisateurs légitimes. Voici les méthodes le plus souvent utilisées :

– /HOIC/JS LOIC/BOIC :
On encourage les Anons à télécharger et à lancer l'application Low Orbit Ion Cannon (LOIC) pour leur permettre de participer volontairement au réseau zombie. Le LOIC est pointé vers la cible choisie pour perturber le service de l'hôte. Toutefois, puisque le LOIC peut révéler les adresses IP de ses utilisateurs, Anonymous a cherché d'autres modes d'attaque, par exemple l'utilisation d'un mandataire d'anonymisation tel que TOR (The Onion Router). D'autres versions de l'application comprennent une version JavaScript, JS LOIC, et, plus récemment, une version fondée sur les favoris (nommée BOIC). Ces versions ne demandent guère plus qu'un clic pour inonder la cible avec un grand nombre de paquets GET et POST afin de créer un déni de service.

– Apache Killer :
L'outil de DoS Apache, surnommé Apache Killer, exploite une vulnérabilité qui permet aux attaquants à distance d'envoyer des requêtes à des serveurs au moyen d'un identificateur de ressource uniforme (URI) mal formé (20. Il est conçu pour surcharger la mémoire du serveur Web et, ainsi, mettre le site Web hors ligne. Il permet aussi à un attaquant à distance de mener une attaque DoS contre un serveur Apache à partir d'un seul ordinateur.

Attaques DoS et DDoS au moyen d'injections SQL :
– #RefRef :

Anonymous a développé et publié, en septembre 2011, un outil de DDoS en Perl, #RefRef, qui exploite des vulnérabilités de SQL (21). L'outil envoie des requêtes SQL mal formées, conçues pour surcharger les ressources du serveur, à un portail Web hébergé sur un serveur SQL. Par conséquent, le site Web est mis hors ligne. #RefRef peut être utilisé avec d'autres outils, par exemple, Havij, un outil d'injection SQL qui aide les vérificateurs de pénétration à trouver et à exploiter des vulnérabilités d'injection SQL. Ces attaques contre des vulnérabilités de SQL peuvent modifier le contenu de bases de données ou voler des données de bases de données (p. ex., renseignements sur les cartes de crédit ou mots de passe).

Virus Guy Fawkes :
Les membres d'Anonymous se sont aussi axés sur le développement de maliciels. Le virus Guy Fawkes (22) a été développé par des Anons pour prendre le contrôle d'un compte Facebook et s'en servir pour distribuer des maliciels à d'autres membres sans connexion réelle de l'utilisateur au site. Selon des analystes de la sécurité de l'entreprise de logiciels antivirus BitDefender, le virus Guy Fawkes (qu'ils nomment Backdoor-Bifrose-AAJX) peut s'injecter dans le processus d'Internet Explorer, donnant ainsi un accès sans entrave au système compromis. Il peut aussi enregistrer les frappes et perturber les opérations de logiciels antimaliciels connus. (Remarque : On croyait que le virus Guy Fawkes était responsable de l'attaque pornographique massive contre Facebook en novembre 2011, mais Facebook et BitDefender ont par la suite réfuté cette hypothèse. Anonymous affirme qu'il travaille encore à contrôler le virus en vue d'une utilisation ultérieure.)

Autre :
Anonymous utilise aussi d'autres techniques : ingénierie sociale pour obtenir l'accès aux systèmes des victimes (p. ex., HBGary Federal), altération de sites Web ciblés pour afficher des messages embarrassants, craquage de mots de passe pour extraire des renseignements de bases de données, utilisation d'un outil de détournement Twitter nommé Universal Rapid Gamma Emitter (URGE) pour détourner les sujets d'actualité sur Twitter vers des sujets d'intérêt à Anonymous, etc. L'outil URGE permet aussi aux Anons de poster des gazouillis sur ces sujets.

ATTÉNUATION

Des pratiques solides en matière de sécurité de la TI aident à se protéger contre des menaces telles que celles présentées par le collectif hacktiviste Anonymous. Anonymous met généralement à profit des techniques en source ouverte ou des vulnérabilités bien connues. Les cibles sont généralement annoncées dans des forums ouverts (p. ex., Twitter, Pastebin) et dans les médias.
Nous encourageons les organisations à consulter les principes de prévention contre les menaces sophistiquées et persistantes et contre les attaques par déni de service du CCRIC aux adresses suivantes :
– http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-fra.aspx
– http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

De plus, les mesures d'atténuation suivantes sont disponibles pour se protéger contre certaines des techniques susmentionnées :

Apache Killer :
– Apache a publié des correctifs pour cette vulnérabilité. Nous recommandons à tous les utilisateurs de mettre leur système à niveau à la version 2.2.20 (ou plus récente) d'Apache.

#RefRef :
– Le code Web devrait être renforcé contre les injections SQL pour empêcher le serveur d'exécuter des requêtes SQL arbitraires provenant d'utilisateurs inconnus. Consultez les références sur les pratiques exemplaires, p. ex. l'Open Web Application Security Project (OWASP) – https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet (en anglais seulement).

NOTES DE FIN
==========

(1) IRC est un protocole de communication textuelle et de conférences en temps réel sur Internet. Il assure les communications de groupe ainsi que la messagerie privée et le partage de fichiers.

(2) Dans une attaque distribuée par déni de service (DDoS), de multiples systèmes attaquent une seule cible. Le déluge de messages entrants vers le système ciblé force sa fermeture et empêche la prestation de services aux utilisateurs légitimes.

(3) L'injection SQL est souvent utilisée pour attaquer la sécurité d'un site Web en injectant des commandes SQL dans la base de données d'une application.

(4) Les attaques du jour zéro essaient d'exploiter des vulnérabilités logicielles qui ne sont pas encore connues des développeurs du logiciel ou du grand public.

(5) Anon-ops assure la communication des annonces d'Anonymous.

(6) LulzSec était une petite équipe qui s'est associée à Anonynmous dans le cadre de la campagne à long terme Anti-Security (ou AntiSec). LulzSec a mis fin à ses activités à l'été 2011.

(7) LulzRaft a été inspiré par le groupe LulzSec et est responsable de l'altération du site Web du Parti conservateur du Canada et de l'accès aux renseignements privés sur les donateurs du parti. Ils ont aussi été liés à l'altération du site Web de l'entreprise d'énergie Husky Energy, établie à Calgary.

s.19(1)

(8) Les porte-paroles officieux d'Anonymous comprennent [redacted] et [redacted]. Pour en savoir plus sur [redacted] consultez http://www.lefigaro.fr/hightech/2011/08/01/01007-20110801ARTFIG00418-piratage-des-lulzsec-un-anglais-de-18-ans-au-tribunal.php. Pour en savoir plus sur [redacted], consultez http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx (en anglais).

(9) Selon des sources d'information ouvertes, LOIC est une application d'essais sous contrainte de réseau en source libre qui permet d'effectuer des attaques DoS ou DDoS contre un site cible en l'inondant de paquets TCP ou UDP pour perturber ses services.

s.19(1)

(10) HBGary Federal est une entreprise de sécurité de la technologie qui collaborait avec le FBI pour démasquer les membres d'Anonymous. En février 2011, le PDG, [redacted] a révélé leur intention de publier des renseignements sur l'identité des membres d'Anonymous. Par conséquent, des membres d'Anonymous ont compromis le site Web de HBGary et ont volé et publié des documents et des courriels de l'entreprise.

(11) Selon des sources d'information ouvertes, le mouvement Occupons désigne un mouvement international de manifestation contre les taux de chômage élevés, l'inégalité sociale et économique et la corruption perçue au sein des entreprises et des gouvernements.

(12) Pour en savoir plus, consultez http://www.branchez-vous.com/techno/actualite/2011/04/anonymous-sony-playstation-3-piratage-geohot-cyberattaque.html.

(13) Le terme printemps arabe désigne des manifestations révolutionnaires dans le monde arabe à partir de décembre 2010. Les pays touchés comprennent la Tunisie, l'Égypte, la Lybie, Bahreïn, la Syrie, le Yémen, l'Algérie, l'Iraq, la Jordanie, le Koweït, le Maroc, Oman, le Liban et l'Arabie saoudite.

(14) The Pirate Bay est un site Web suédois notoire qui facilite les téléchargements illégaux et appuie le mouvement international contre le droit d'auteur.

(15) Stop Online Piracy Act (SOPA) est un projet de loi des É.-U. pour combattre la distribution en ligne de propriété intellectuelle protégée par le droit d'auteur. Anonymous le considère comme une tentative de censure d'Internet.

(16) Pour obtenir l'explication complète d'Anonymous, consultez la déclaration de Barrett Brown à http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-hacked.

(17) Le Centre d'évaluation des cybermenaces (CECM) a fourni des mesures d'atténuation aux employés des ministères touchés.

(18) Ce projet de soi est semblable aux projets de loi C-50, C-51 et C-52 précédents.

(19) L'opération Facebook a été lancée le 5 novembre 2011 parce qu'Anonymous croit que « Facebook est à l'opposé des valeurs d'AntiSec ».

(20) Pour en savoir plus, consultez le bulletin CVE-2011-3192 à http://nvd.nist.gov/ (en anglais).

(21) Un serveur SQL est un serveur de base de données relationnelle qui peut stocker et récupérer des données sur un réseau (p. ex., Internet). Les requêtes provenant des ordinateurs clients sont formatées dans le langage SQL.

(22) Guy Fawkes était associé à la Conspiration des poudres (« Gunpowder Plot »), une tentative infructueuse d'assassinat du roi James I d'Angleterre en 1605. Le projet des conspirateurs était de faire sauter le Parlement pour tuer le roi et les membres du Parlement. Les Anons ont d'ailleurs adopté comme symbole le masque de Guy Fawkes, facilement accessible et bon marché.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118
Télécopieur : 613-998-9589
Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: GOC-COG@OPSCEN.GC.CA

Shogilev, Matthew

From: Shogilev, Matthew
Sent: 2012-Oct-02 2:49 PM
To: Wong, Normand
Subject: FW: **s.23**
Attachments:

[redacted]

Matt

From: Shogilev, Matthew
Sent: 2012-Sep-24 6:23 PM
To: Wong, Normand; Angers, Lucie; Audcent, Karen; Sansom, Gareth; Nguyen, Trang Dai
Subject: FW: **s.23**

Hi everyone.

[redacted]

Best.

Matt

From: Covo, Pierre [mailto:Pierre.Covo@ps-sp.gc.ca]
Sent: 2012-Sep-24 3:42 PM
To: Shogilev, Matthew
Cc: Kousha, Hasti; Pilon, Claude (PSEPC-SPPCC)
Subject: **s.23**

Hello Matthew,

[redacted]

[redacted]

Please don't hesitate to contact us if you need more information.

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

From: Clow, Patrick
Sent: Tuesday, September 18, 2012 11:01 AM
To: Slatkoff, Ari
Cc: Pilon, Claude; Anderson, Windy
Subject: [redacted]

Good morning Ari,

[redacted]

[redacted]

Please feel free to contact me directly if you have any questions or concerns. Your assistance in this matter if greatly appreciated.

s.21(1)(a)

Thank you

s.23

Patrick Clow, CISSP
Manager, Technical Analysis | Gestionnaire, Analyse Techniques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-944-4074 Facsimile | Télécopieur +1 613-991-3574
Patrick.Clow@ps-sp.gc.ca
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

Pages 40 to / à 44

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Shogilev, Matthew

From: Shogilev, Matthew
Sent: 2012-Oct-04 1:12 PM
To: Covo, Pierre (PSEPC-SPPCC)
Subject: memo
Attachments: [redacted] **s.23**

Hi Pierre,

[redacted]

Best,

Matthew Shogilev
Counsel | Avocat
Criminal Law Policy Section | Section de la politique en matière de droit pénal
Department of Justice Canada | Ministère de la Justice Canada
Ottawa, Canada K1A 0H8
matthew.shogilev@justice.gc.ca
Telephone | Téléphone 613-948-7418
Facsimile | Télécopieur 613-941-9310
Government of Canada | Gouvernment du Canada

Pages 46 to / à 57

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Covo, Pierre

From: Covo, Pierre
Sent: October-04-12 2:04 PM
To: 'Pilon, Claude'; Kousha, Hasti
Subject: FW:
Attachments:

s.23

From: Shogilev, Matthew [mailto:Matthew.Shogilev@justice.gc.ca]
Sent: October-04-12 1:12 PM
To: Covo, Pierre
Subject:

s.23

Hi Pierre,

Best,

Matthew Shogilev
Counsel | Avocat
Criminal Law Policy Section | Section de la politique en matière de droit pénal
Department of Justice Canada | Ministère de la Justice Canada
Ottawa, Canada K1A 0H8
matthew.shogilev@justice.gc.ca
Telephone | Téléphone 613-948-7418
Facsimile | Télécopieur 613-941-9310
Government of Canada | Gouvernment du Canada

Pages 59 to / à 61

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Pilon, Claude

From: Clow, Patrick
Sent: Monday, October 15, 2012 4:00 PM
To: Covo, Pierre
Cc: Pilon, Claude
Subject: Study
Attachments: Report PS-SP Ethical HackingFINAL.DOC

Hi Pierre,

Please find attached a copy of the Ethical Hacking article discussed last week.

Thank you

Ethical Hacking

A Report for the National Cyber Security Division of
Public Safety Canada

2012

Alana Maurushat

Contents

1. Executive Summary

1.1 What is ethical hacking?

In its traditional form, hackers were people who used clever technical solutions to solve problems. Ethical hacking then is the non-violent use of a technology in pursuit of a cause, political or otherwise which is often legally and morally ambiguous. [1] Ethical hacking is also referred to as electronic civil disobedience, hacktivism, grey hat hacking, intrusion and penetration testing, counter-attacks, and politically motivated hacking/computer crime.

This report discusses ethical and legal issues with four types of ethical hacking: hacktivism, online civil disobedience, penetration/intrusion testing & security activism, and counter-attack.

1.2 Methodology

This report examines different types of ethical hacking. It includes a multi-disciplinary literature review, interviews from hacker researchers, caselaw charted over the last ten years in Canada, the United States, the United Kingdom, Australia, New Zealand, Hong Kong, France, Germany and Russia, and a recent time-line of important ethical hacking incidents. A more detailed description of the methodology is found in section 3.

Abbreviated references are found in the footnotes. Full references are found in the Reference Section at the end of this Report.

1.3 Key Findings and Recommendations

Key findings are listed below:

- Online protests will increase and the type and size of such attacks will escalate in order to continue to capture the interest of the media.

- There is a growing movement in some online communities (hackers) to ensure that "backdoors" (ways to exploit a program) are inserted into computer programs and then kept quiet as a means of ensuring access to future information (especially government websites). These types of "attacks" are not done for instant media attention.

- Technologies such as LOIC will evolve to allow for encryption and anonymity. This will parallel similar developments that took place with peer to peer file-sharing networks.

- The most popular discussion threads in hacking forums are "beginner hacking" and "hacking tools and programs" indicating the likelihood of increased hacking, both ethical and for criminal purposes.

- Deterrent effect of laws and sentences only works with beginners and with younger hackers. These individuals will generally quit illegal hacking after first conviction (under 25).

---

[1] Samuel 2004.

- The law does not have a deterrent effect for highly skilled and often older hackers (over 25).

- Some individuals involved in hacking are considered be have an addiction in the same way that an individual may become addicted to gambling, video games, drugs or alcohol.

- A significant portion of corporations and organisations are engaged in some form of counter-attack.

- Many ethical hacking incidents are closely tied with the objective of protecting human rights and promoting an open, transparent democracy.

- Many ethical hackers view their work as acts of civil disobedience and align their actions with traditional civil disobedience as espoused by Ghandi, Martin Luther King Jr. And Henry David Thoreau.

- Other hackers identify with an ethos of hacking that developed in the 1980s forward and look to technical gurus and the writings of "Hacktivismo Declaration" by the Cult of the Dead Cow, "The Hacker Manifesto", "The Anonymous-Anonops", The Electrohippies "Client-Side Distributed Denial-of-Service" and the "Gospel According to Tux".

- Other groups are less ideal in their philosophy citing motivation as "for the laughs". However, further probing of such hackers reveals that their hacking is done out of "a streak of sense of wrongdoing" without always being able to clearly articulate what that wrongdoing is.

- Denial of Service Attacks by movements such as Anonymous require critical mass in order for an operation to be successful.

- There is often a correlation between the number of participants in a denial of service attack, and the worthiness/morality of the cause.

- Which causes will acquire critical mass is unpredictable.

- It would be incorrect for governments or organisations to assume that members of ethical hacking groups come from one type of community, race, or age.

- Many ethical hackers are not aware that their activities are illegal, especially those participating in politically motivated denial of service attacks.

- Elite hackers tend to work alone due to the higher risk of "getting caught" when groups are involved. This may support the proposition that a technically sophisticated attack may in fact be the work of only one individual, or few individuals.

- While many instances of ethical hacking may be illegal, it is interesting to note that some methods used by law enforcement and by security firms contracted to perform criminal intelligence gathering may also be illegal, or at best highly controversial.

The report concludes by making a number of recommendations. These are:

- Develop and publicise guidelines for online civil disobedience and hacktivism.
- Run an education campaign once these guidelines are finalised.
- Allow and encourage a legitimate "space" for virtual protests.
- Investigate the licensing of security experts.
- Implement a security research exemption for computer offences.
- The idea of a public interest exemption for hacking offenses should be given further consideration. This could be done in a multi-party working group on both security research and public interest exemptions.
- Develop a code of conduct for counter-attack and have a legislative review of how principles of self-defence might apply to a counter-attack situation.
- Any governmental engagement with ethical hacking should be legal and transparent. These activities should not be contracted out to security firms unless they are closely scrutinised and held accountable in some form of safeguard or compliance mechanism.
- Ensure that data owned or generated by Canadians is protected and that such data, if collected and stored, is deleted after a reasonable period when using foreign services such as Google, Facebook and Twitter (United States based). Currently, any person who uses Google, Facebook, Twitter and similar services is subject to US Internet monitoring by governments and law enforcement, and potentially is exposed to subpoenas to release personal information, even in the *absence* of a transparent criminal investigation.

1.4 Research Acknowledgements

This research would not have been possible without the research assistance of Lauren Loz, ,Taylor Hall, Bodil Diederichsen, Nazar Sharunenko, Patrick Webster, and several individuals who have chosen to remain anonymous. Additional thanks to Suelette Dreyfus and Alexandra Samuel for agreeing to share their expertise in this area.

2. Introduction and Background

In its traditional form, hackers were people who used clever technical solutions to solve problems. Ethical hacking then is the non-violent use of a technology in pursuit of a cause, political or otherwise which is often legally and morally ambiguous. Ethical hacking is also referred to as electronic civil disobedience, hacktivism, grey hat hacking, intrusion and penetration testing, counter-attacks and politically motivated computer crime (discussed in detail in section 4). The current most popular term used by media to describe ethical hacking is hacktivism.

Civil activists in the 1960s and 1970s had sit-ins and protests for civil rights and anti-war. Many people equally thought that this civil disobedience could lead to change. Change would lead to rational and critical discussion of citizens with governments in a move towards more open and transparent democratic governance. In the late 1970s and early 1980s many governments enacted laws around freedom and access to information to better ensure open disclosure and government transparency. Prior to such enactment of freedom and access to information laws, it was difficult to obtain copies of government documents. These laws were devised in an attempt to move the disclosure of information default from private to public. In this sense, a government employee

would not ask when something should be made public, but rather, when something should be made private (in other words, transparency by default).

While freedom and access to information laws have shifted the line of transparency, they did not achieve transparency by default. Internal guidelines for when information should remain private or public were muddled with bureaucratic wording, and confusion. The end result was government employees began to self-censor. This took place in two main ways. The first, when classifying documents employees erred on the side of caution and thus over-classified documents as private/secret and under-classified documents as public/transparent. The second, when access to information requests were granted, often documents were so blacked out that it was difficult to ascertain with any certainty what decision or policy was adopted or why. The "black pen" effect began.

The first part of the 21st Century will likely go down in history as the era when ethical hackers opened governments. The line of transparency is moving by force. The twitter page for Wikileaks demonstrates this ethos through its motto "we open governments" and its location to be "everywhere". Hacktivism is a form of civil rights activism in the digital age. In principle hacktivists believe in two general but spirited principles: respect of human rights and fundamental freedoms including freedom of expression and personal privacy, and the responsibility of government to be open, transparent and fully accountable to the public. In practice, however, hacktivists are as diverse in their backgrounds as they are in their agendas.

Ethical hacking is not new. In the late 1980s Australian hacktivists penetrated the NASA computer system releasing a worm known as WANK – Worms Against Nuclear Killers.[2] The worm was written and released as a form of protest for the NASA launch of the rocket Galileo which was to navigate itself to Jupiter using nuclear energy. The infamous German hacker group "Chaos Club" was also busy in the late 1980s attacking German government systems to protest against collecting and storing of census information; the groups believed that the government should not collect or store the personal information of its citizens.[3]

Moving forward to the first decade of the 21st Century, ethical hacking, while not new, has fundamentally changed in one distinct manner – the ability to participate in attacks (denial of service attacks) is no longer limited to an elite group of people with excellent computer skills; the technology is available to the masses in an accessible format for those with limited technical skill. People follow tweet feeds of Anonymous and LulzSec where operations are suggested. If the person decides to participate in an operation, they simply click the download button for LOIC software, select the demonstration they wish to participate in by typing in the URL (Eg. www.alana.com), then click again. Fait accompli. The individual is now participating in a denial of service attack. It must be noted that denial of service attacks using LOIC require a critical mass to be effective. This means that many people must deliberately choose to participate in an event.

People around the globe are participating in denial of service attacks on many types of websites for a variety of causes. Websites that have been attacked to date include the Australian Parliament's website, Paypal, Mastercard, Mexican government website, paedophilia websites, the New York Stock Exchange, the Toronto Stock Exchange, News of the World, Oakland City Police, Ecuadorian government, Peruvian government and the list goes on and on (see **Appendix B**).

One of the most well-known hacktivism "groups" is Anonymous. The word group here is arguably used incorrectly as Anonymous is more like an umbrella name or a movement for a plethora of

---

[2] Dreyfus and Assange 1997.
[3] Dreyfus and Assange 1997.

smaller groups and operations. In addition to performing denial of service attacks, members of some of the smaller groups participate in more sophisticated forms of hacktivism that require a higher range of computer skills. Instances of these more sophisticated attacks include the release of names and details of the Mexican drug cartel, Los Zetas, the names and details of individuals who use child pornography sites, and the capturing of secret documents held by governments around the world – some of these documents are then given and released by Wikileaks.

Hacktivism isn't limited to attacking information systems and retrieving documents. It also extends to finding technical solutions to mobilise people. At the height of the Egyptian e-revolution the major Internet service providers and mobile phone companies shut down the Internet (the kill switch) preventing people from using the Internet and mobile phones. This, in turn, affected the people's ability to mobilise. Anonymous worked around the clock to ensure that images from the revolution were still being sent to the international press. Hacktivists also work to penetrate the Iranian government's firewall to tunnel passages allowing Iranian citizens to view blocked sites. I myself have been involved with a similar firewall penetration when I organised some of the internal testing of the Chinese firewall for the Open Net Initiative – a collaborative research project between the Citizen Lab, at the University of Toronto, The Berkman Centre for Internet and Society at Harvard, and the University of Cambridge. There are similar initiatives for Saudi Arabia and other parts of the world with strong censorship. Keeping secrets and preventing citizens from accessing information may no longer be an achievable goal. The question becomes, should governments adopt heavy-handed policies and law to investigate and prosecute ethical hackers to deter such activity and keep the status quo? Or should governments enact an appropriate legislative response that reflects the reality of this new era – the forced line of transparency?

Other forms of ethical hacking are rooted in ensuring the security of networks. This has taken shape in four main ways. The first is through intrusion or penetration testing where experts are invited to expose any security vulnerabilities of an organisation's network. The second is somewhat more controversial as it involves hackers who, without authorisation, illegally access a network, software or hardware to expose security vulnerabilities. Sometimes these hackers will go so far as to fix the vulnerability or to report it to the system's owner. Third, there is a growing concern that many organisations including corporations and governments are engaging in counter-attack efforts to deter attacks to their systems. Last, many security experts are forming self-organised security communities to actively engage in intelligence gathering, and counter-attacks – this will be called security activism.

This report discusses moral and legal issues of ethical hacking. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. There are no exceptions to the cybercrime/computer crime provisions for security research or public interest in most jurisdictions around the globe. Equally difficult will be how civil rights will apply to hacktivism. This question is shrouded with uncertainty. How will governments and courts manoeuvre in this new era of activism meets computer within the boundaries of protected civil liberties?

3. Methodology

This report examines four types of ethical hacking:

- Hacktivism,
- Online civil disobedience,
- Penetration/intrusion testing, & Security activism, and

- Counter-attack

Each category will be defined and a series of related aspects will be examined. These include:

- Selected Case Studies
- Motivation
- Main Targets
- Relation Between Targets and Motivations
- Fundamental Principles of "Hacker-Ethics"
- Perceptions of the Illegality of Activity
- Deterrence Effects of Case Law and Convictions
- Relevant Case Law Convictions
- Observations

An ethical hacking case law summary for the last 10 years will be provided looking at cases in Canada, the United States, the United Kingdom, Australia, New Zealand, Hong Kong, Singapore, France, Germany and Russia. The summary is found in **Appendix A**.

Recent ethical hacking incidents for the last two months of 2011 is provided in **Appendix B**.

Technical and legal challenges to the investigation and prosecution of hackers will additionally be analysed. This portion of the study borrows heavily from my own PhD in cybercrime entitled, "Botnet Badinage: Regulatory Approaches to Combating Botnets" (PhD Thesis, The University of New South Wales, 2011) where I interviewed people involved in the cyber security industry (including law enforcement), some cybercriminals and attended conferences around the world including Eastern Europe, the United Kingdom, Canada, Australia, Hong Kong and the United States. The technical and legal challenges are the same for hacking activities in general. Any specific technical or legal challenges specific to ethical hacking will also be analysed.

As there have been few interviews or empirical studies on ethical hacking (though there are several studies now underway which have not yet been published), studies that have looked at hacking in general will be utilised. Three of the most significant studies of hackers to date have been:

1) Dr. Suelette Dreyfus and Julian Assange in their book, *Underground* (William Heinemann, first published in 1997, with a reprint and update in 2011).

2) Raoul Chiesa, Stefania Ducci and Silvio Ciappi in their UNICRI study, *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* (CRC Press, 2009).

3) Dr. Alexandra Samuel, *Hacktivism and the Future of Political Participation* (PhD Thesis, Harvard, 2004).

Suelette and Alexandra have agreed to be interviewed for their views on the topic. The interview questions are included in **Appendix C**. Some of their responses are incorporated into the main body of the report. Raoul was not able to be interviewed but I have gratefully borrowed some statistics and other information from his profiling of hackers study.

An extensive multi-disciplinary literature review (information systems, psychology, fiction, risk management, computer science, law, political science) was conducted and is included in the reference section.

4. Typology

The terminology around ethical hacking is confusing as terms mean different things according to their disciplines and often these terms are used interchangeably. For instance, the technical world distinguishes between a hacker and a cracker whereas the mainstream media lump both terms under the umbrella of "hacker". Expressed differently, the distinction is sometimes made by referencing black hat, grey hat and white hat hackers. For clarity these terms are defined below:

Hacker: "A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term.[4]"

Cracker: "A cracker is an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system.[5]"

Black Hat Hacker: (also referred to as a cracker), is "someone who uses his computer knowledge in criminal activities in order to obtain personal benefits. A typical example is a person who exploits the weaknesses of the systems of a financial institution for making some money.[6]"

White Hat Hacker: "Although white hat hacking can be considered similar to a black hacker, there is an important difference. A white hacker does it with no criminal intention in mind. Companies around the world, who want to test their systems, contract white hackers." [7]" They will test the security of a system, and are often hired to make recommendations to improve such systems.

Grey Hat Hacker: "A grey hat hacker is someone who is in between these two concepts. He may use his skills for legal or illegal acts, but not for personal gains. Grey hackers use their skills in order to prove themselves that they can accomplish a determined feat, but never do it in order to make money out of it. The moment they cross that boundary, they become black hat hackers."[8]

People who participate in ethical hacking are predominantly grey hat hackers. The differentiation, however, between hackers, crackers, and colours of hats plays little importance when looking at these concepts from a legal perspective. Any form of unauthorised access, modification or impairment of data, a network or computer is a crime. There are no exemptions in most jurisdictions; hackers and crackers alike rely on the discretion of law enforcement as to whether to prosecute or turn a blind eye. Another fallacy in classifying hackers is that an individual falls solely into one definition. Each single attack must be characterised, not the person behind the attack. For example, you might have a hacker who predominantly breaks into systems to learn, sometimes she might even fix a security flaw in a system. The same hacker might also break into a system to collect data on individuals who are actively engaged in viewing and downloading child pornography, and then make this data publicly

---

[4] RFC 1392 Internet Users Glossary.
[5] RFC 1392 Internet Users Glossary.
[6] Hacking Alert, "White Hat and Grey Hat Hacking: What is the Real Difference?" http://www.hackingalert.com/hacking-articles/grey-hat-hackers.php. *See also* Hafele 2004.
[7] Hacking Alert, "White Hat and Grey Hat Hacking: What is the Real Difference?" http://www.hackingalert.com/hacking-articles/grey-hat-hackers.php
[8] Hacking Alert, "White Hat and Grey Hat Hacking: What is the Real Difference?" http://www.hackingalert.com/hacking-articles/grey-hat-hackers.php

available to law enforcement and the public at large. Yet this same hacker might also accept a fee to break into a corporation's (who they view as unethical) database and steal a trade secret that is handed over to a competitor. Each of these examples involves unauthorised access. The difference with each attack goes to intent, motive, and involves the individual's subjective notion of what is ethical or moral. Ethical hacking is, therefore, difficult to define.

Ethical hacking is also a term that is used interchangeably with hacktivism in the media, but which has a distinct meaning in the computer science discipline. For example, in the computer science field "ethical hacking" is used to describe what is known as penetration or intrusion testing (white hat hacking). Similarly, someone who merely participates in a denial of service attack for political reason would not be considered a hacker within the computer science community. This type of action would be more akin to online civil disobedience.

For this report, "ethical hacking" will be used in its broadest sense to include the following activities:

Hacktivism: is the clever use of technology which involves unauthorised access to data or a computer system in pursuit of a cause or political ends. [9]

Online Civil Disobedience: is the use of any technology that connects to the Internet in pursuit of a political ends.

Penetration/Intrusion Testing: is a type of information systems security testing on behalf of the system's owners. This is known in the computer security world as "ethical hacking". There is some argument, however, as to whether penetration testing must be done with permission from a system's owners or whether a benevolent intention would suffice in the absence of permission. Whether permission is obtained or not obtained, however, does not change the common cause, that of improving security.

Security Activism: is similar to penetration/intrusion testing in that the cause is to improve security. Security activism goes beyond mere testing of security, however, to gather intelligence on crackers, and to launch active attacks to disrupt criminal online enterprises. One example is the taking down of a botnet (see section 7).

Counter-Attack: is also referred to as hackback or strikeback. Counter-attack is when an individual or organisation who is subject to an attack on their data, network or computer takes similar measures to attack back at the "hacker/cracker". For example, when an individual or organisation is subject to a denial of service attack, that organisation might initiate their own denial of service attack on the responsible party's website.

<u>Ethical Hacking:</u> Ethical hacking then is the non-violent use of a technology in pursuit of a cause, political or otherwise which is often legally and morally ambiguous.[10]

The use of a technology which resulted in acts of violent or physical harm would fall outside of the scope of ethical hacking, and may even be considered as cyber-terrorism (attack to critical infrastructure). The ambiguous legal and moral nature of ethical hacking will be explained in sections 5 through 8.

---

[9] Samuel 2004.
[10] Samuel 2004.

5. Online Civil Disobedience

5.1 Description

Online Civil Disobedience is the use of any technology that connects to the Internet in pursuit of a political end. There are many forms of online civil disobedience. A person or groups of individuals may block access to a website, redirect web traffic to a spoof website, deface a website, or flash messages on someone's computer screen. The offline equivalents would be a sit-in blocking access to a building, a protest which prevents people from using a street such that they are redirected down another path, protesting with signs and images, handing out flyers or placing such flyers in mailboxes.

Online civil disobedience incorporates a variety of techniques to carry out activities. These technologies are described below:

SQL Injection
Defacing a website involves the insertion of images or text into a website. This is often done via a SQL injection (structured query language). A SQL injection is an attack in which computer code is inserted into strings that are later passed to a database.[11] A SQL injection can allow someone to target a database giving them access to the website. This allows the person to deface the website with whatever images or text they wish.

DNS Highjacking
DNS hijacking allows a person to redirect web traffic to a rogue domain name system server.[12] The rogue server runs a substitute IP address to a legitimate domain name. For example, www.alanna.com's true IP address could be 197.653.3.1 but the user would be directed to 845.843.4.1 when they look for www.alanna.com. This is another way of redirecting traffic to a political message or image.

Adware/Spyware
Adware refers to any software program in which advertising banners are displayed as a result of the software's operation. This may be in the form of a pop-up or as advertisements displayed on the side of a website such as Google or Facebook.

Distributed Denial of Service Attack (DDoS)
A DDoS is the most common form of online civil protest. A denial of service attack is distributed when multiple systems flood the channel's bandwidth and/or flood the host's capacity (e.g. overflowing the buffers) .[13] This technique renders a website inaccessible.

Distributed denial of service attacks are performed with a botnet with several of the compromised computers sending packets to the target computer simultaneously. A DDoS attack may also be distributed by use of peer-to-peer nodes.[14] The importance of botnets is explained below.

---

[11] Security Spotlight 2010.
[12] Security Spotlight 2010.
[13] Denial of Service Attack is well defined on http://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack
[14] Athanasopoulos et al. 2006. E., Anagnostakis, K., and Markatos, E., "Misusing Unstructured P2P Systems to Perform DoS attacks: The Network that Never Forgets".

Botnet: A botnet is a collection of compromised computers that are remotely controlled by a bot master.[15]

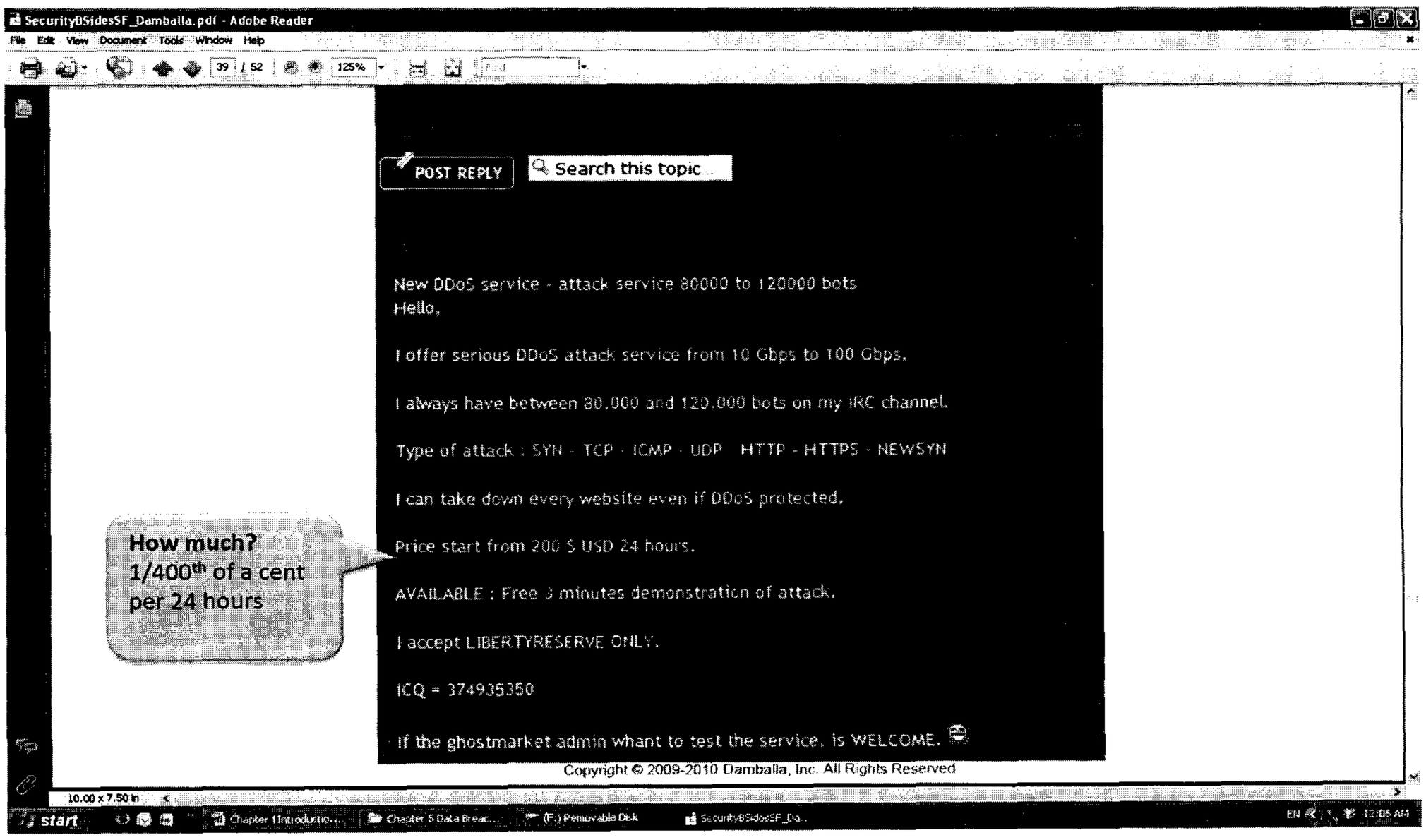
There are three ways of using a botnet to perform a denial of service attack:

Make the Botnet: In the first, a person would have to physically make a botnet through painstaking hours of labour as it would involve compromising several hundred if not thousands of computers. This type of botnet would require the botnet master to have a high level of computer skills.

Hire/Rent a Botnet: T he second type is whereby the person merely hires someone to execute a denial of service attack. This requires no computer skills but for the ability to use Google. Bot agent design and bot delivery have become a commoditized service industry.[16] A small botnet is sufficient to launch an effective denial of service attack causing much damage and costs as little as $200 USD for a 24 hour attack.[17] A person does not require any special computer skills to use a botnet to commit a crime. **Figure 1** on the following page is a sample of the commercialisation of denial of service attacks with a botnet. The customer would merely specify the targeted website to attack, pay a nominal fee of $200 USD, and a denial of service attack (DOS attack) would be launched for 24 hours against the website.

[15] Maurushat 2011.
[16] Ollmann 2010.
[17] Ollmann 2010.

Figure 1 Denial of Service Attack as Commercial Service[18]

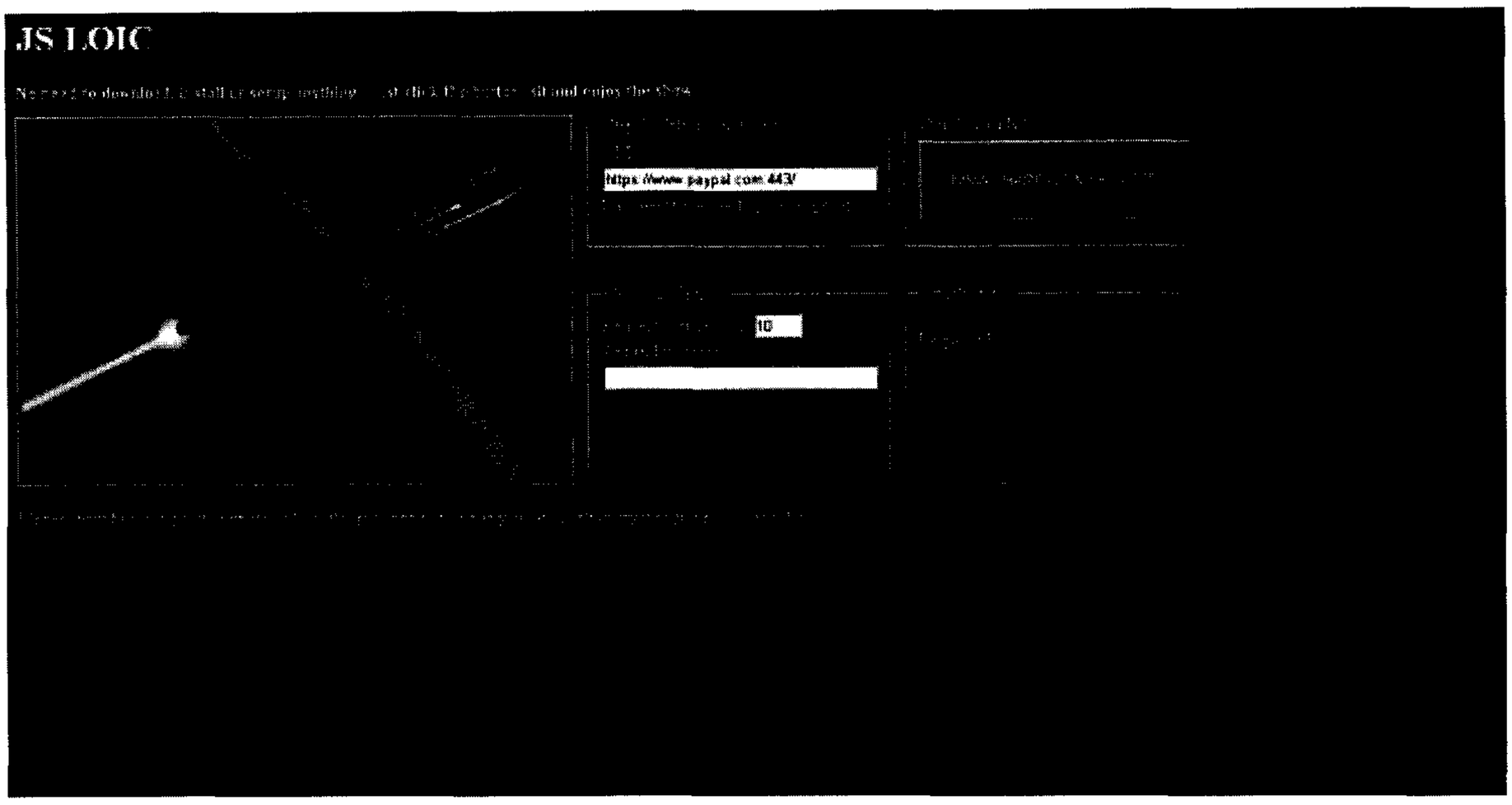


Commercialisation is also occurring within another context known as crime kits. In this instance a person is able to purchase a copy of the botnet code in the form of a crime kit. The kit comes with a licence to use the botnet, and instructions. ZeuS, for example, is a popular crimeware kit that may be purchased for $700 USD.[19] Expert computer skills are not required for botnet usage. A criminal may elect to purchase a crimeware kit with simple instructions on how to execute an attack.

LOIC or Similar Software: The last botnet involves a free software program known as LOIC (Low Orbit Ion Canon). LOIC is used for most of the denial of service attacks performed by members of Anonymous. **Figure 2** on the following page captures an image of LOIC executing a denial of service attack against Paypal. Use of LOIC requires minimal computer skills. One googles LOIC, downloads the software with a click, types in the URL (Eg. www.paypal.com), and presses start. The denial of service attack then commences and people join in from all over the world using LOIC.

[18] Image from Ollmann 2010.
[19] *See* Trend MICRO 2010.

Figure 2 LOIC DDoS Attack Against Paypal[20]



Differentiating between these three types of botnets has legal implications. In the instance of making a botnet, the botnet master would have had to acquire control over user's computer without their authorisation thereby attracting cybecrime provisions for unauthorised access, modification or impairment to data. Hiring or renting a botnet also attracts similar criminal sanction. Using LOIC, however, would not necessarily attract criminal sanction for unauthorised access. This is because the computers connected to LOIC are doing so voluntarily. The issue of whether the actual attack involves unauthorised access as opposed to a form of legitimate civil disobedience is contentious (see below for caselaw).

5.2 Case Studies

Wikileaks Operation Payback

Wikileaks founder Julian Assange was arrested in London on charges of sexual crime under Swedish law. Many viewed this as a false arrest and indirect way of incarcerating Assange for the release of secret US cables to Wikileaks. A legal defence fund was quickly established where people could make donations via Mastercard or Paypal to help the cause. Mastercard and Paypal disallowed any payments to be made to the Assange legal defence fund causing an international uproar, and in particular, within hacktivism communities. Members of LulzSec launched a denial of service attack against Mastercard and Paypal which took down their capabilities in December 2010 and then again in June 2011. As will later be seen in section 8, there was a denial and counter-denial of service attack showdown which might best be seen as gunfire between warring factions, with evidence that the US government contracted security firms to perform attacks against Wikileaks and other journalists.

---

[20] Image from http://www.wired.com/threatlevel/2010/12/web20-attack-anonymous/

Anonymous Operation Titstorm

In 2010 the Australian government sought to introduce a mandatory internet filter. This was unofficially referred to as 'Clean Feed'. Internet filtering in this context would mean requiring Internet Service Providers (ISPs) such as Optus, Telstra and iiNet to implement technical means to filter out a set list of illegal websites, most notably websites with images of child abuse and child pornography. Internet filtering techniques are commonly used in authoritarian regimes such as China and Iran, as well as in Western democracies such as Canada, the United Kingdom, France and Sweden. Although Australia will not be the first country, authoritarian or democratic, to implement internet filtering, the proposed filtering system has many unique features, separating it from other regimes.

Australia would have been the first western democracy to mandate internet filtering through formal legislation. ISPs would have been required legally to block illegal material. In countries such as France, Belgium, and Germany, courts have mandated ISPs to block hate speech and the illegal peer-to-peer filesharing of copyright protected materials.[i] In countries such as Canada and the United Kingdom informal government pressure led to voluntary internet filtering frameworks by the countries' major ISPs.

There is no Australian legislation yet on internet filtering, therefore, important details of the scheme are unknown. As Australia's filtering system has yet to be implemented, it stands to reason that its details, configuration and scope may change.

The criteria for evaluation of websites to be blocked remain equally uncertain and ambiguous. As it stands, the Clean Feed proposal had two tiers.

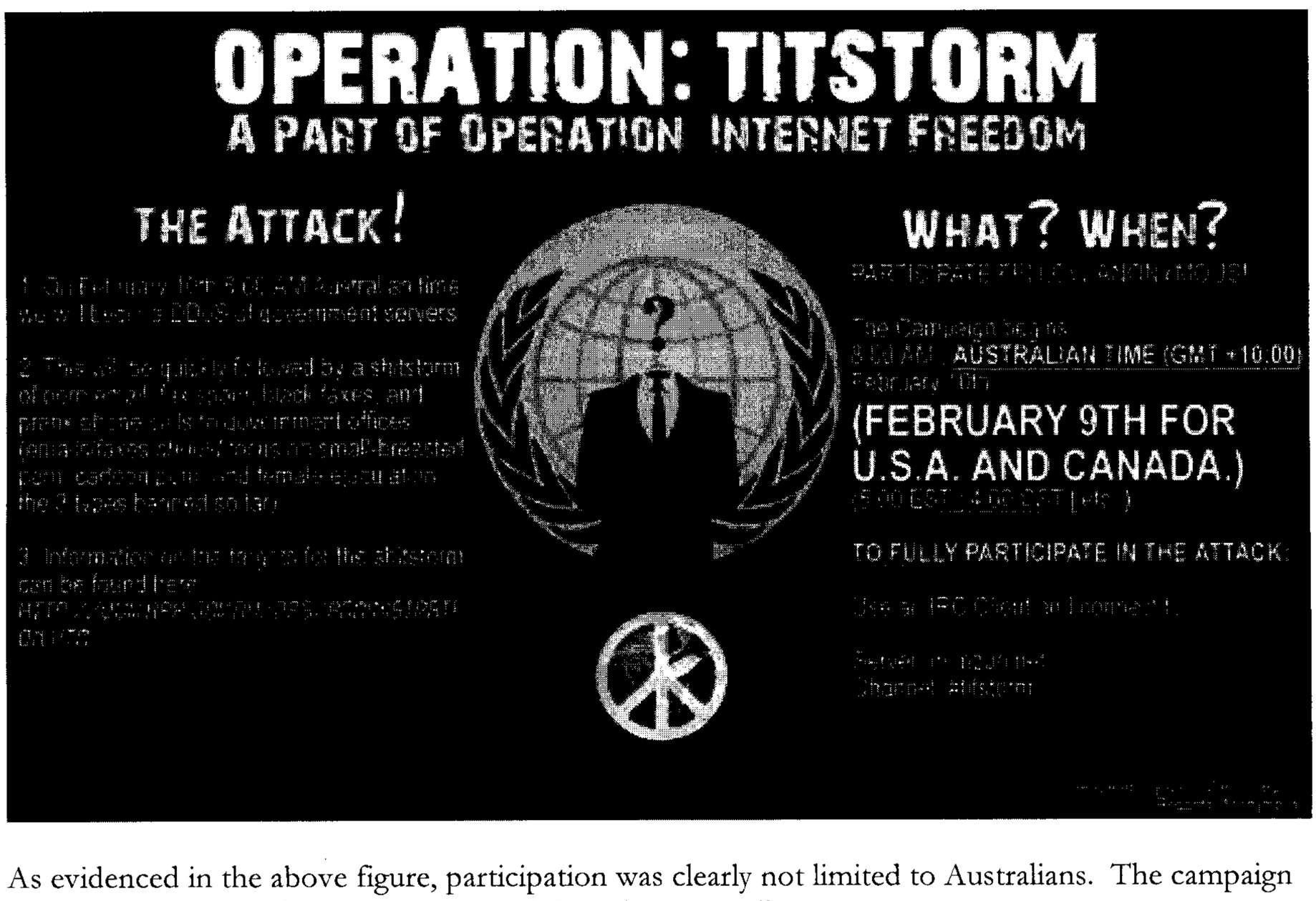
1) **Blacklist Filtering:** The first tier is an ACMA issued blacklist of 'child pornography' websites and 'other prohibited' materials to be blocked by Internet Service Providers at the URL level. The scope of 'other prohibited' materials in unknown. This will be mandatory for all Australians with no ability to opt-out of the scheme. Circumvention of the blacklist will be illegal. The blacklist will only block those URLs found on the ACMA Blacklist. It will **not** block websites with 'child pornography' and 'other prohibited content' found on:
   - Peer-to-peer systems (Eg. bit torrent, Winnie),
   - Encrypted channels,
   - Chatrooms,
   - MSN Instant Messaging;
   - Mobile phones, and
   - Unknown whether a blocked URL will block every website operating on a domain name or merely the specific offending material (Eg. www.youtube.com versus a specific video on www.youtube.com).

2) **Content Filtering:** The second tier will block types of materials which are legal but potentially unwanted. The scope of such material has not been delineated but examples would likely include adult pornography and other 'R' rated material – material inappropriate for children but clearly legal for adults. It remains unknown what types of filtering techniques would be used. Potentially these could include URL blacklists, deep packet inspection, peer-to-peer content inspection, and URL and http content inspection. Users will be able to opt-out as well as legally circumvent this type of filtering.

In response to the Australian government's decision to introduce a mandatory filter there were a number of offline marches and online acts of protest. One of these protests was the online defacement and DDoS attack of the Australian Parliamentary Website in 2010.

The Anonymous operation was dubbed Operation Titstorm (see **Figure 3** below). The operation saw the Parliamentary website taken down and images of penises and breasts were portrayed on the Parliamentary website's screen. Australians have a long history of both censorship and opposition to censorship. Unlike Canada, the United States and many parts of Europe, human rights are not protected in a Charter of Human Rights, Bill of Rights or within the Constitution.[21] The courts in Australia have less ground to strike down legislation that infringes civil liberties.

Figure 3 Operation Titstorm



As evidenced in the above figure, participation was clearly not limited to Australians. The campaign sought participation from Americans and Canadians as well.

[21] Cook et al 2011.

5.3 Motivations

Online civil disobedience participants are motivated by the same reasons as participants in traditional offline acts of civil disobedience. For example, consider the following offline and online acts of civil disobedience:

Sit-ins	Virtual Sit-ins
Barricades	Denial of Service Attacks & Website Redirection
Political Graffiti	Website Defacements
Wildcat Strikes	Denial of Service Attacks & Website Redirection
Underground Presses	Site Parodies, Blogs, Facebook Protest
Petitions	Web-Petitions (Eg. Facebook Likes)

The motivation is derived from a strong desire to protest that which is seen to be immoral, corrupt, undemocratic and above all, to send a strong message to ensure transparent governance. There is a strong link between the protection of civil liberties and online civil disobedience activity.

5.4 Main Targets

The main targets are the websites and databases of governments and organisations linked to government (Eg. Stratfor), including departments of defence, intelligence agencies and law enforcement. The other main target is organisations that are viewed as corrupt.

5.5 Relation Between Targets and Motivations

The main relation between motivation and targets is perception of the target behaving immorally. In many instances "immoral" means infringing civil liberties, whether this be freedom of the press, freedom of expression, or privacy. Police brutality is another common link between target and motivation. There are many videos of police brutality that are shown in Anonymous, LulzSec and CabinCr3w tweet feeds. For instance, there is a video on a Tweet Feed from January 3, 2012 showing the beating of a 15 year old by Harris, Texas police after the accused turned himself in.[22] It remains to be seen if the incident will gain popular consensus amongst Anonymous members to provoke protest.

In other instances, "immoral" is a combination of violation of civil liberties as well as more severe instances where tyrant governments stand in the way of democracy.

Not every possible event that could be received as "immoral" however qualifies for hacktivism action. This is a crucial point in that hacktivism movements require critical mass. Generally speaking, the stronger the cause, the more likely the action to be perceived as "ethical".

It must further be stated that there are many attacks which are being categorised as performed by Anonymous which don't appear to be linked to civil liberties or other types of political cause. One such example is the French hacker known as "Carl" who was arrested after he appeared in the French television program "Complément d'enquête" where he demonstrated that he had gained access to the French Army and Thales (security corporation that provides information systems to

[22] See http://twitter.com/#!/search?q=%23CabinCr3w

defence departments).[23] He has also stolen and used credit cards and bank account numbers to purchase personal possessions. Carl claims to be part of the Anonymous group. However, shortly after Carl's arrest, Anonymous issued a statement claiming that Anonymous does not associate with cybercriminals who use credit cards to benefit themselves.

5.6 Fundamental Principles of "Hacker-Ethics"

In hacktivism blogs and tweet feeds there are repeated references to pirates, Robin Hood, Billy the Kid, Ned Kelly, and famous civil disobedience activists such as Martin Luther King.[24] Members of groups such as LulzSec and other Anonymous affiliates, unlike earlier hacktivism groups in the late 1990s such as the Hong Kong Blondes (provided Internet access to ensure free flow of information in China) and the Cult of the Dead Cow, don't publish ethical hacking manifestos or similar documents. Ethical statements appear to be more limited such as "opening governments", "fighters for internet freedom", "exposing corruption", and so forth.

One interesting aspect, however is that Anonymous quickly issued a public statement after the French TV "Carl" incident disassociating itself with credit card and bank account theft for personal use. The post-Christmas operation to donate money to charity was orchestrated by members of Anonymous. The difference here is not one of whether or not personal information, and credit cards are copied, but how they are used. Under Anonymous culture, there cannot be a connection to self-benefit such as seen in the "Carl" incident. This is similar to the Sony incident where personal information and credit card numbers were copied, but this information was not used to purchase products or for blackmail purposes. There is a strong sense of Robin Hood tradition. What is equally interesting is that cybercriminals in Eastern Europe have also described their activities along the Robin Hood line where they will only steal money from rich Western countries, and then, only money from people who have more than a $1000 in their account.[25]

5.7 Perceptions of the Illegality of Activity

Unlike participants in hacktivism as will be seen in section 6, many participants in online civil disobedience believe their activity to be legal. They assume that a virtual sit-in or denial of service attack is a legitimate form of protest similar to regular picketing, barricading, protesting and sit-ins. Meanwhile, many users of the LOIC software are unaware that the software provides no anonymity even though they are participating in an act under the umbrella movement Anonymous. Many of the arrests of members of Anonymous were LOIC users. As will be seen in section 6, hacktivism as defined in this report, requires good computer skills and involves more than the ability to use LOIC.

5.8 Deterrence Effects of Case Law and Convictions

Online civil disobedience became popular in 2009. Since then there have only been a handful of arrests internationally. Whether pressure from law enforcement has a deterrent effect has not been the study of any criminological research yet – we may have to wait a few more years. Anecdotal evidence does yield some interesting observations.

With the case of Operation Titstorm, the arrested and convicted Matthew George has publicly stated that it was his first and last experience with online protests.

---

[23] Zorz 2011.
[24] *See for example* http://anonops.blogspot.com .
[25] Zenz 2008.

Arrests of LulzSec members in the US and the UK has had the opposite effect. Other members of the group as will be seen in section 8, have met the arrests with counter-attacks of law enforcement databases, and any organisation who they see as having aided in the arrest of these individuals. It is important to note that some companies such as Twitter have fought court orders to reveal account details and other information about their clients. The Twitter case against Wikileaks members is likely to be taken to the Supreme Court of the United States. Further, academics from around the United States will appear in a Senate hearing in the latter part of January 2012 to give evidence of the acute lack of transparency in the American regulation of Internet matters and they will express their concerns of a growing surveillance state.

In conducting interviews for this report, neither Samuel nor Dreyfus thought that hacktivism should be met with a heavy handed response. Samuel noted that the actions of Anonymous and similar hacktivists "were problematic when people with technical skills highjack the political process". Samuel herself has participated in a quasi/form of disobedience when she established a website which aggregated tweet feeds from around Canada displaying election results. Samuel, however, is quick to note that there needs to be legitimate room in politics to allow for virtual participation and virtual protests. Samuel, Dreyfus and I unanimously believe that governments should actively establish, publish and promote some form of guidelines for virtual protesting. Guidelines or a Code of Conduct is a priority recommendation.

5.9 Relevant Case Law and Convictions

Germany

In 2001 two civil rights activist groups, Libertad and "Kein Minch ist illegal" had called for protests against Lufthansa for their policy of helping to identify and deport asylum-seekers. There was an offline protest at the Lufthansa shareholders meeting. This was met with an online protest. The online protest consisted of a DDoS attack where over 13,000 people participated in the online attack temporarily shutting down Lufthansa's server for two hours (this is pre LOIC).[26]

One of the protest organisers, Andreas-Thomas Vogel, was convicted of coercion by a regional German court. On Appeal, the higher court found that there was no coercion under §240 of the German criminal law. They reasoned that there was no violence or threatening behavior. Further, the court reasoned there needs to be a permanent and substantial modification of data to be found guilty of incitement of alteration of data. The Court viewed the DDoS attack as a modern form of non-violent blockade fully within the right to freedom of expression. In Australia, a similar attack attracted comments from the court as falling within terrorist activity. There was no mention of freedom of expression or freedom of assembly.

Australian

Matthew George was an Australian member of Anonymous who participated in "Operation Titstorm". He was charged and convicted of incitement. The Magistrate stated that George had incited others to attack government websites and went so far as to liken his activities to cyber-terrorism – a claim that is truly outrageous given the context of the protest. George was given a $550 fine. George was not a ring-leader but merely a participant using LOIC software. Taken from statements made by George to the Sydney Morning Herald, he states:

> "We hoped to achieve a bit of media attention to why internet censorship was wrong ...
>
> I didn't think that I would ever get caught. I was actually downloading connections from other computers in America, so I didn't think the Australian government would be able to track me down."
>
> "I had no idea that what I was doing was illegal. I had no idea that there was incitement and it was illegal to instruct others to commit a legal [sic] act."[27]

There is an underlying theme here whereby many DDoS users do not realise that they are participating in an illegal activity.

5.10 Observations

The issues with online civil disobedience are in many ways the same issues as with offline civil disobedience. One commenter asks, "If a building is blockaded by protestors, is it civil disobedience or infringement on freedom of assembly? Is a book burning activism or censorship? Are causes

---

[26] Vendrath 2006.
[27] Whyte March 14, 2011.

more important than rights?"[28] There have been a paucity of cases addressing the issue; therefore, the issues are very much open for debate.

Critical mass is important as to which causes get taken up.

Which causes are taken up by a critical mass remain unpredictable.

6. Hacktivism

6.1 Description

Hacktivism was defined as the clever use of technology which involves unauthorised access to data or a computer system in pursuit of a cause or political ends. Hacktivism is more than the online equivalent of sit-ins and protesting which might be considered acts of online civil disobedience. Hacktivism still involves hacking for a cause, often political. Hacktivism, however, is taking that one step further from an online protest such as the collection and disclosure of personal emails, extortion or blackmail for a political cause.

Common forms of hacktivism include information theft (Eg. copy emails, account information, government documents, credit card information, viewing habits of Internet users – child pornography), virtual sabotage (SQL injection whereby content on the website is replaced with new content of the attacker), insertion of backdoor, and software development. The latter two require further elaboration.

It is often assumed that incidents of hacktivism and online civil disobedience are done in order to attract media attention to a cause. While that is true in many incidents, there is also a growing movement of silent activists who view the current political landscape as a long-term information war.[29] When security vulnerabilities are found in government and corporate databases, this information is kept secret. They are not looking for media attention, but wish to ensure that there continue to be backdoors available for accessing information. In some instances software or hardware is purposefully developed with a backdoor included in its coding for this purpose. In this instance, the software company and contractor are not aware of the default when the product is shipped out and received (Eg. surveillance software used by governments and corporations). This type of insertion of a deliberate vulnerability is performed by security experts working in the field. Their active participation in hacktivism is not publicized. They do not seek media attention and there are no media stories on their activities. Their goal is to fly under the radar. They possess the highest level of computer skills. This type of hacktivism has a particular focus on information related to democracy – censorship, government surveillance, and war efforts.

Software development is another critical form of hacktivism. The technologies used in Wikileaks for example ensure the integrity of the document, and the anonymity of the informant. Additionally Wikileaks has developed technology that allows people in non-democratic jurisdictions such as China a way to access their otherwise filtered content. Other hacktivism technologies include anonymisers such as the Tor proxy, and Track-Me-Not which allow people to view online content anonymously.

---

[28] Thomas 2001.
[29] Interviews with Wikileaks members. For example, Pilger 2012.

6.2 Case Studies

There are many instances of online civil disobedience spilling beyond into hacktivism. Two of the most interesting examples, however, are the Christmas charity donation drive by Anonymous, and the exposure of key officials linked to the neo-Nazi movement in Europe.

Anonymous Post-Christmas Charity Donations

The 2011 post-Christmas Anonymous attack targeted credit card information of the clients of U.S. based security think tank, Stratfor. In this instance, members of Anonymous were able to access and steal credit cards of Statfor's clients. Clients included members of intelligence agencies, law enforcement and Fox news journalists. The credit card numbers were later used to give away money as Christmas donations to charities such as the Red Cross, Care and Save the Children.[30]

According to Anonymous postings, the personal information, credit card details and emails of Statfor were not encrypted. This echoes a reoccurring theme of poor and sub-par security practices of large corporations, governments and even security think tanks entrusted with sensitive data.

Neo-Nazi Website

Anonymous claimed responsibility for an attack of a neo-Nazi website in Finland, and stole the information of the websites members then released it to the public. The list of members included a Parliamentary aide who later resigned from her post. It was later reported that Anonymous had issued a statement claiming:

> "We have no tolerance for any group based on racial, sexual and religion discrimination as well as for all the people belonging to them and sharing their ideologies, which is the reason why we decided to carry out last Monday's attack."

Similar types of attacks have been launched to reveal membership of child paedophilia groups, and organised crime cartels.

6.3 Motivations

There is no singular motivation at the heart of hacktivism. The motivation of such players may often not be well articulated, if articulated at all. There are, however, some reoccurring themes amongst many hacktivism activities. At the heart of all hacktivism is a sense of some sort of moral wrongdoing that either needs to be exposed and/or needs to be punished, and a wider sense of public loss of confidence in their institutions.[31] Many hacktivism activities expose corruption and/or humiliate the establishment.

Some hacktivists are motivated to expose insecure practices of corporations and governments handling personal information as seen in the Sony and Statfor attacks (see Section 7 and Appendix B).

---

[30] AnonOps Communications December 2011.
[31] Interview with Dreyfus and Samuel. *See also* Chiesa et al. 2009.

Most hacktivism, however, is related to a political cause. For example, many hacktivists are motivated by exposing censorship and surveillance of individuals by governments and corporations. Wikileaks, for example, has posted documents outlining the surveillance activities of governments around the world. Secret filtering blacklists of websites blocked by internet service providers on behalf of governments frequently find their way to the Internet. Other hacktivists target oppressive governments and enable the free flow of information in and out of areas where media coverage and access to local and foreign press is restricted. These include areas in Iran, China, Egypt, Syria, Libya, and include more local venues in the recent Occupy movements that are occurring globally. Other hacktivism efforts target underworld child paedophile websites and both the Internet Service Providers that host such repugnant content and the customers of this material. Religions such as Scientology have also been targeted with claims that such groups disseminate misinformation and have a corrupt hand in lobbying efforts of US governments.

Hacktivism and online civil disobedience are linked to empowerment and the strongest desire to find an effective public voice. This also applies equally to social media movements including online petitions. The motivation of much hacktivism is closely linked to whistleblowing. Generally, critical mass is important in determining which causes get taken up. In this sense it is very democratic. Hacktivism is not anarchy nor does it have a top down leadership which steers its course. Critical mass is required and generally speaking, the stronger the cause, the more likely any hacktivism activity will be seen as ethical. Equally important, however, is predictability. Dr. Suelette Dreyfus, expert researcher in both hacking, hacktivism and whistleblowing, indicates hacktivism targets are not predictable. Which causes are taken up by a critical mass remain unpredictable.

6.4 Main Targets

The main targets are the websites and databases of governments and organisations linked to government (Eg. Stratfor), including departments of defence, intelligence agencies and law enforcement. The other main target is organisations that are viewed as corrupt.

6.5 Relation Between Targets and Motivations

The main relation between motivation and targets is similar to online civil activism perception of the target behaving immorally. In many instances "immoral" means infringing civil liberties, whether this be freedom of the press, freedom of expression, privacy. Surveillance, intelligence gathering and contracting security firms to discredit hacktivist groups is currently a strong motive. In other instances, "immoral" is a combination of violation of civil liberties as well as more severe instances where tyrant governments stand in the way of democracy.

Many operations by LulzSec, however, are difficult to qualify as ethical hacking when the release of innocent third party personal information is disclosed on the Internet, and no motive other than "just for the laughs" is apparent in many of LulzSec attacks.

6.6 Fundamental Principles of "Hacker-Ethics"

Principles in hacktivism parallel those in online civil disobedience. When Anonymous member Barrett Brown (former journalist, and now Founder of the Project PM) was asked to comment on television whether the activities of Anonymous were ethical, he encouraged the public to make a comparison chart. Chart what is good versus what is bad about each Anonymous Operation then compare it with the issue that Anonymous sought to bring attention to. In other words, compare it with the actions of the traditional institution. For example, the actions of hacktivists must be

compared with Arab states' governments trying to 'turn off' the internet and to control social media; the treatment of WikiLeaks after publishing controversial information and continuing to assert its right of free speech; the heavy handed crackdown on the non-violent worldwide Occupy Movement by various regional and federal governments; and the lack of law around the shutting off of critical payment services as in the case of Mastercard and Paypal. Conversely, many hacktivism activities run the risk of being perceived as immoral, especially when personal information of innocent parties is released to the Internet.

Transgressive forms of hacking may be viewed as illegal yet ethical. It remains to be seen whether in 10 years time these same forms of transgressive hacking will become a legal part of the civil disobedience landscape.

6.7 Perceptions of the Illegality of Activity

Unlike many people who participate in online civil disobedience, participants in hacktivism are well aware that their actions are legal, and take precautions to ensure their anonymity online. As will be seen with online civil disobedience groups, many participants are unaware that using software such as LOIC to take part in a denial of service attack is illegal; they assume that it is a lawful protest. When hacktivists hack, copy, view and disclose the personal information of others they are clearly aware of that their actions are illegal and they have taken a calculated risk in spite of the threat of criminal sanction.

6.8 Deterrence Effects of Case Law and Convictions

Historical evidence shows that some hackers who are caught and later convicted of conspiracy or unauthorised use, will either give up such activities or use their talents in a legitimate matter such as working as a security expert or in some form of technology field. This is well documented in Suelette Dreyfus and Julian Assange's interviews with hackers in *Underground.* Raol Chiesa's work in *Profiling Hackers* also notes that the law offers deterrence to younger hackers (script kiddies) but not other levels of hacking. Both studies, however, reveal that the law offers no deterrence to future generations of hackers; the deterrence value is only individualised and is limited to the person who has been charged with a crime. Criminal prosecutions and convictions fuel the underworld of hackers and have the sole effect of driving the hacking world further underground, and have led to the development of many obfuscation technologies that make traceback to the source of an attack difficult (see section 9). As Dreyfus and Assange note, prosecutions and convictions have not had the message "don't hack" but, rather, have had the message of "don't get caught."

The studies that have been done to date, however, have been about hacking in general and not about ethical hacking. It is unknown whether the prosecution and conviction of ethical hackers will act as a deterrent sending the message, "ethical hacking is wrong" or whether such prosecutions will act as a catalyst to even more ethical hacking as a sign of protest. When members of Anonymous were arrested in the United States this past year, there were a series of attacks of law enforcement, news channels (FOX) and university websites as a form of public protest. Similar attacks were performed on security firms who contract with governments and corporations to attack Anonymous, LulzSec and Wikileaks. This is explored further in section 8.

6.9 Relevant Case Law and Convictions

Members of LulzSec and Anonymous have been arrested in the UK and the US, charges pending, and outcomes unknown at this time.

Nineteen year old Ryan Cleary was arrested in Essex in the United States and has been charged under the Computer Misuse Act for his hacking effort of the UK's Serious Organised Crime Agency. He is also alleged to have broken into many other law enforcement agencies both in the United Kingdom and the United States. Cleary is said to be a member of LulzSec. Cleary is said to suffer from agoraphobia and he has been diagnosed with aspergers and attention deficit disorder. Similar cases against hackers in the United Kingdom, Australia and New Zealand in the last ten years have involved people addicted to computers, those who suffer from agoraphobia and others who have autism spectrum disorder or attention deficit disorder. A hacker who went by the handle Wandii was acquitted on all counts of computer misuse in the United Kingdom due to a computer addiction.[32] A 19 year old New Zealand hacker, Owen Walker was brought up on several charges of computer misuse. The first charge was under s. 252(1) of the New Zealand *Crimes Act 1961* with accessing a computer system without authorization. The second charge related to interfering with a computer system under s. 250(2)(c) of the *Crimes Act 1961*. The third charge was the use of a computer system for dishonest purpose under s. 249(2)(a) of the *Crimes Act 1961*. Lastly, under s. 251(a) and (b) for possession of software for the purpose of committing a crime. Walker pleaded guilty to all charges. He could have been sentenced to up to 16 years of imprisonment under the four offences that he was charged with but was instead discharged without conviction, and was ordered to pay $9 526 NZD in reparation as well as to relinquish any assets acquired as a result of gains he achieved through use of his botnet.[33] The court noted that Walker committed the crimes over a two year period when he was aged 16 to 18. The court heard evidence of Walker's difficulty in socializing due to having Asperger's syndrome. Walker now works in Melbourne, Australia for Telstra (the largest telephone and Internet Service Provider in Australia). There has been no study that has looked at the link, if any, between agoraphobia, aspergers or attention deficit disorder and hackers.

Arizona college student Cody Kretsinger, alleged member of LulzSec, was arrested and charged with multiple counts of conspiracy and unauthorised impairment of a protected computer in the United States for allegedly hacking Sony Pictures Entertainment. The hacking is said to be that of Sony's computer system, which was compromised in May and June in 2011. LulzSec, unlike Anonymous, performs hacks both for political reasons and "just for fun" or "just for laughs" (lulz is computer slang for laughs). LulzSec has not formally announced any political reason for the Sony hack. Interesting, however, are the many media comments and blog responses that sympathise with LulzSec and find the lapse security measures of such corporations to be the worst offender. As one blogger writes:

> "The main offender here is Sony. They were fully aware of the vulnerability of their current system. They were just too lazy to fix it. All it took was a Google search and some script kiddies entered in one SQL line and broke into the system. This wasn't a "zero day attack," it was a well known vulnerability to their system that was public. It's like having a stack of money just behind a gate with no lock. All it takes is one simple well known action and you are in. Why do you think class action lawsuits were charged against Sony if it wasn't their fault?"[34]

Other members of LulzSec have been arrested and detained in Italy, Switzerland, and the United States for computer offences for hacking a number of different websites. It is much more difficult to see any public benefit or ethical conduct in many of LulzSec's operations, other than the media coverage exposing the poor security habits of most corporations and governments. Security experts have been urging companies and governments to improve their outdated and insecure protection of

---

[32] Dreyfus and Assange 1997.
[33] R. *v. Walker*, HC HAM CRI2008-0750711 [2008] NZHC 1114.
[34] Herpderp1189, Huffington Post January 5, 2012

their systems for decades. During the last decade, however, many corporations still don't use basic encryption to protect personal information of their customers, nor do they adequately protect their own assets. The LulzSec attacks may act as a catalyst for corporate improvement to security.

6.10 Observations

At the heart of all hacktivism is a sense of some sort of moral wrongdoing that either needs to be exposed and/or needs to be punished, and a wider sense of public loss of confidence in their institutions – even if the actions of LulzSec are poorly articulated if at all (the membership of this group seems to be confined to young males unlike the membership of Anonymous with participants of all ages and walks of life).

Hacktivism and online civil disobedience are linked to empowerment and the strongest desire to find an effective public voice. This equally applies to social media movements such as online petitions.

The motivation of much hacktivism is closely linked to whistleblowing.

7. Penetration / Intrusion Testing and Security Activism

7.1 Description

Penetration/Intrusion Testing is a type of information systems security testing on behalf of the system's owners. This is known in the computer security world as "ethical hacking". There is some argument, however, as to whether penetration testing must be done with permission from a system's owner or whether a benevolent intention would suffice in the absence of permission. Whether permission is obtained or not does not change the common cause, that of improving security.

Most penetration or intrusion testing occurs when a security expert is hired to test the security of an organisation's network. In this sense, the security expert has permission to hack into the organisation's network such that the law will view this as authorised, thereby not attracting criminal sanction. The legal ambiguity arises when these same security experts stumble across security vulnerabilities, then actively investigate further without permission or authorisation from the system's owner. It is only this latter form of act which would be considered as legally and morally ambiguous thus qualifying as ethical hacking.

Security Activism is similar to penetration/intrusion testing in that the cause is to improve security. Security activism goes beyond mere testing of security, however, to gather intelligence on crackers, and to launch active attacks to disrupt criminal online enterprises. A good example of security activism involves botnet tracking and takedown.

These two types of ethical hacking are considered here together as they share similar if not identical attributes in motivation, cause, and techniques.

7.2 Case Studies

Australian White Hat Security Expert Patrick Webster

Australian security expert Patrick Webster was threatened with legal action and criminal charges for disclosing a serious security flaw in First State's Superannuation System.[35] When Webster went to log into the First State system to check on his superannuation he noticed that the URL contained his individual identity information linking to his superannuation account. He found this odd, and investigated further, Patrick ran a simple for loop script to check for other anomalies. The script started with the scan of one account number then continued to scan by incremented numbers. In the time that it took to initialise the script (computer program), make tea and come back to the computer, the script revealed hundreds of megabytes of account numbers. Upon seeing this, Patrick ascertained that potentially every account was exposed to the Internet. He quit running the program. In the scanning time, the script automatically saved the details of the first 500 accounts.[36]

Alarmed at this security flaw, Webster notified the information technology personnel at First State Superannuation. Some of the IT staff sent him emails thanking him.[37] However, the Chief Information Officer and others at First State Superannuation reacted differently alleging that by accessing not just his own account but the accounts of others he had committed a crime. Webster was served with legal papers and was told that the police might press charges against him. What is more alarming is the fact this security flaw should have been picked up through basic security compliance checks. It is further alarming that over 770 000 FSS accounts were vulnerable, as well as the details of another 1.2 million accounts from other companies who outsourced their data storage to Pillar Administration. The alarming rate of corporations having their data compromised has sparked Data Breach Notification laws around the globe yet corporations and organisations still have not implemented many basic security mechanisms. First State Superannuation is reviewing its data storage contract with Pillar as well as its own personal handling of personal information.

It has become standard industry practice to thank and often reward those individuals who alert companies to security flaws. Corporations such as Facebook and Google send their thanks and offer a small reward. Anti-virus and anti-spyware companies also pay money for zero day threats. In this instance, however, First State's reaction was to threaten Webster with civil and criminal proceedings if he didn't turn his computer over to the IT personnel at First State for them to verify that he had deleted the information from those 500 accounts.[38] The charges were later dropped. This incident has set off alarm bells for security researchers in Australia and perhaps even abroad.

In the words of Patrick Webster:

> "I am genuinely disappointed the government legislation will not provide safeguards for security researchers, though I am not the least bit surprised.
>
> I've encountered clients who are actively being attacked by a compromised legitimate website and considered counter attacking in self defence to protect my client and the comprised organisation... I haven't, but it would be nice if we could.

---

[35] Moses 2011.
[36] Email correspondence with Patrick Webster.
[37] Grey 2011.
[38] Grey 2011.

> My only hope is that my incident with First State Superannuation sets a precedent for future researchers. Obviously not in Australian law as the NSW Police stated that no laws were broken and I was providing a civil duty, and Minter Ellison halted proceedings, but with any luck the media attention will convince corporations that not everybody is acting with malicious intent. If it helps just one researcher in the future I'll be happy."[39]

The incident is a timely reminder of the lack of legitimate exemptions for security research.

Botnet Removal Communities

There exist a number of undocumented small independent research communities that were (or still are) actively involved with botnet harm mitigation, interdiction, counter-attack and take-down. This may include attempts by the command & control (C&C) source to program and re-program its bots, altering payloads of malicious applications delivered on botnets, and launching a denial of service attack on C&C servers.[40] Offense-in-Depth Initiative (OID) was launched in 2008 as a small group targeted approach to fighting cybercrime. OID is comprised of volunteers who work within smaller subset groups dedicated to botnet countermeasures. Each subgroup specialises in one particular botnet. So, for example, there was the OID-Kraken and OID-Torpig small working groups targeting the Kraken and Torpig botnets. The main goal of the OID teams is to erode the profit model of specific major cybercriminals, while obtaining intelligence for use by law enforcement.[41] Each specialist subgroup divides their roles into reverse-engineer operations specialist, coder, social-engineer linguist and information warrior. In some instances the same person could fulfil multiple roles, and in other instances the roles are somewhat superficial.

The group's aim was to form small working groups singling out one botnet or criminal operation with the purpose of long-term disruption *(Note: the group has disbanded and no longer performs botnet takedowns).* Other small independent research groups have performed counter-measures for a few weeks or a month, then the countermeasures stop, allowing the criminal operation a chance to regroup and get back to "business as usual."[42] OID's focus was on long-term countermeasures aimed at disrupting the profitability of the botnet operations. Whether a cybercriminal continues operating depends on many factors. OID has singled out three major factors: complexity of the operation, risk of getting caught, and reward/profit of the crime.[43] OID uses methods aimed to increase the complexity of the criminal's organisation, forcing them to spend more time, effort and money into maintaining their criminal operations. For instance, techniques include subverting the command and control or by either increasing or decreasing the size of the botnet. There has been some research done on optimal botnet size for certain types of activities.[44] Compromised machines can be remediated so that they are no longer part of a botnet. If you remediate enough machines, the size of the botnet becomes untenable for criminal operations. Likewise, if you grow a botnet from 100 000 to 10 000 000 it becomes very difficult to effectively manage the botnet without constantly writing new instructions for the command and control. The botnet master ends up spending extraordinary amounts of time and effort to control the bots. Just as one person may only successfully tend to a set amount of sheep or cattle within a set amount of land, an increase in the size of the herd requires more land, water, and labour. Similar to caring for livestock, taking care of botnets is often referred to as "herding" bots.

---

[39] Email correspondence with Patrick Webster.
[40] Smith 2005.
[41] Observations from email orrespondance with members of the OID Initiative.
[42] ISOI is one such group. Members complained of the unfocused, ad hoc short-term approach of ISOI.
[43] Observations from founder of OID in listserve correspondance.
[44] Li, et al. 2009.

When a botnet's operations are interrupted it may create the need for more complex operations in order to adapt to the new environment. In the case of botnets, if the complexity becomes too great for the criminal, more expertise may be needed in the form of hiring a programmer to develop new encryption methods or programs. It is believed that, in turn, this forces the cost of business to rise. It is hoped that if the disruption is continuous, and that costs of doing business rise so that profitability will be reduced, then this will correspond with a lower level of criminal activity. There is no evidence to suggest that this has worked to date. Botnet activity remains a growth industry. Nonetheless, this is the belief of groups such as OID. As stated in the OID mission, it is about long-term disruption. It may be too early to ascertain whether such countermeasures are effective.

OID tactics are decided by looking at effectiveness, stealth, ethics and ability to avoid collateral damage to third parties. Such an approach to tactics is not an official code but represents a rough understanding between members of the group.[45] Ultimately what tactics are used depends on the decisions of the specialist group. While the operations of the OID groups are not openly discussed, many of its operations have involved working with select individuals working for computer security companies. Such companies, unlike OID, often will make available to the public information on botnet infiltration and countermeasures taken against a botnet. This was the case with the Kraken botnet, which OID members infiltrated and took down in December of 2008. OID members have not publicly discussed how the botnet was taken down. Researchers with the security corporation, TippingPoint, however, have provided publicly available information about the Kraken botnet and infiltration process available from their security blog.[46]

Researchers at TippingPoint infiltrated Kraken by starting with a sample of the code provided by Offensive Computing. The various protocols of the botnet were noted. The command and control instructions were encrypted. Researchers had to reverse engineer the computer code which entailed decrypting the encryption routes. TippingPoint created a fake server (sinkhole) to redirect Kraken traffic. TippingPoint played a somewhat passive role in that they did not rewrite instructions and send alternative instructions via the command and control. In their words, "we are not talking back to any of the Kraken zombies that are phoning home to us. We are simply listening passively, decrypting the request and recording statistics."[47] As such they were able to then redirect traffic to their server (often referred to as a sinkhole). Researchers at TippingPoint recorded the list of all uniquely infected IP addresses and applied a reverse DNS lookup to ascertain what types of computers and locations of IP addresses were part of the botnet. The majority of the compromised computers were home broadband users with compromised machines predominantly based in the USA, Spain, United Kingdom, Colombia, Mexico, Peru and Chile.[48]

TippingPoint wrote an update code capable of cleaning up the compromised computers of Kraken. They have even provided a video demonstrating their capability of removing the Kraken botnet altogether. TippingPoint researchers have not cleaned up the botnet for ethical and legal reasons, chiefly that there is no security research exemption.

7.3 Motivations

Self-organised security communities recognise that there is great need for action to alleviate some of the non-functionality in an attempt to reduce cybercrime. When viewed in this light, the work of

---

[45] Observations from listserve correspondance.
[46] TippingPoint.
[47] TippingPoint.
[48] TippingPoint.

self-organised communities may be seen by those involved with these communities as an act of "doing justice" where justice has otherwise proven to be non-functioning.

The motto "to do justice"[49] is potentially applicable to both self-help security communities and botnet communities. There is, for example, mounting evidence that Eastern European communities have likened internet crime such as fraud to a legitimate activity – Robin Hood stealing from the rich Western countries to give to the poor developing nations. Many types of malware and botnets for hire are now distributed with end-user license agreements and some have even been registered for copyright protection. Conversely, anti-botnet communities have justified breaking the law where required to achieve justice. The motto "to do justice" parallels the actions of many self-organized security communities who are "fighting malware and botnets" under the motto of "doing justice" in the absence of effective regulatory response to the problems. In fact, regulation may never effectively deal with botnets. The point is, rather, that the perception of the absence of regulation or the presence of ineffective regulation motivates people to take matters into their own hands.

7.4 Main Targets

Main targets vary for security activists. In some instances the target might be simply to gather intelligence in a honeypot. In other instances, it may mean actively taking down a botnet, or removing malware from infected websites, or sending information to companies whose security has been compromised, to collecting information and handing it over to law enforcement.

7.5 Relation Between Targets and Motivations

Targets are either performing illegal criminal functions (running a botnet, stealing credit cards) or they are organisations whose security practices are poor (and often not fully compliant with security standards). The underlying link between target and motivation is inept security and the ability to exploit vulnerabilities.

7.6 Fundamental Principles of "Hacker-Ethics"

Security activists almost always have excellent computer skills. There is no one set of hacker ethos that applies to any group of hackers though anecdotal evidence and in the opinion of Dr. Suelette Dreyfus (interviewed), expert security activists share a common set of ethics that can best be described as responsible engagement.[50] This does not, however, imply that all actions are within the law. Security activism and research is a grey and murky area of the law.

7.7 Perceptions of the Illegality of Activity

It is difficult to qualify or quantify perceptions without empirical research. Nonetheless, my observations from my research and with interviews of cybersecurity experts is that they are highly skilled individuals who are acutely aware that what they are doing is illegal in many jurisdictions but view their activities are necessary and ethical. For example, university researchers investigating the Torpig botnet invaded the privacy of those individuals whose computers had been compromised in order to gain intelligence about the botnet propagation trends.[51] They did so without consent of the

---

[49] Tamanaha 2001.
[50] Chiesa et al. 2009.
[51] Torpig.

computer owner and in clear violation of the law. Law enforcement was notified of these violations and did not press charges. If anything, they condoned the actions.[52]

7.8 Deterrence Effects of Case Law and Convictions

As a general proposition, security activists are not deterred by the law; if anything the law turns a blind eye and encourages ethical hacking for these purposes. Security researchers are imperative in any initiative to combat cybercrime. For example, there has yet to be a single takedown of a botnet that didn't involve cooperation from a number of entities including security researchers from specialised security software companies and universities, Internet Service Providers, Domain Name Service Providers, and often law enforcement – often these parties are located in different parts of the world.

7.9 Relevant Case Law and Convictions

There have been few incidents where security activists have been the target of criminal investigations though there have been many security researchers who have been threatened with criminal sanction. There have, however, been several instances of civil law suits against security activists. Two of these civil (quasi-criminal) cases are discussed below.

Spamhaus Project

Spamhaus Project, an organisation of volunteers in the computer industry, composes blacklists of some of the worst spam propagators to aid ISPs and businesses to better filter spam. The company E360insight.com sued Spamhaus Project in the Northern District of Illinois Federal Court alleging it was a legally operating direct marketing company and should not be blacklisted as a spam provider. Spamhaus did not file a response and did not appear before the court. As such, the arguments presented before the court were unilateral such that the court issued a default judgment.[53] The court ordered Spamhaus to pay $11.7 million USD, to post a notice that E360 was not a spammer, and ordered that the Spamhaus Internet address be removed from the Internet Corporation for Assigned Names and Numbers (ICANN). Spamhaus ignored the ruling, did not pay the money, and did not post a notice on its website that E360 was not a spammer, nor did ICANN remove the Spamhaus website from its root server. In a similar situation, the anti-virus and anti-spyware company Symantec was taken to court in California by a company which it defines and reports in its services as spyware. Hotbar.com claims that the classification of its software as spyware is in violation of trade libel laws, and constitutes interference with contract. The suit was reported as settled with Symantec agreeing to classify Hotbar as 'low risk'.[54] A series of cases of a similar nature have been filed and heard between 2005 and 2009, with most settling.[55]

---

[52] Torpig.

[53] E360 Insight, LLC et al v. The Spamhaus Project US District Court, Norther District of Ilinois, 13 Deptember 2006 (Case no. 06 C 3958). Access to default judgment at http://www.spamhaus.org/archive/legal/Kocoras_order_to_Spamhaus.pdf.

[54] Messmer 2006.

[55] 1-800 Contacts v WhenU., 1-800 Solutions v. Zone Labs, Cassav (CasinoOnNet) v Sunbelt Software, Glaria (Gator) v Internet Advertising Bureau.

Sierra vs. Ritz

The US trial court decision of *Sierra v. Ritz*[56] involved unauthorised use of a domain name system zone transfer. Zone transfers are, generally speaking, open access public information. They provide data about all of the machines within a domain. Without zone transfer, you would literally have to type in an IP (internet protocol) address every time you went to a website – it is one factor contributing to the convenience of the Internet. The information may be retrieved by the use of 'host command' with the 'I' option. Zone transfers contain public information to varying degrees depending on the protocols used by an organization. Zone transfers may be disabled to the greater public with only trusted machines and senior administrators having access on a 'need to know' basis. This is a form of limited authorised public access. In Sierra's case, the zone transfer was more widely available in the sense that the system allowed zone transfers to everyone, thereby publicizing potentially private data into a public forum. There would be no way for a person accessing the zone transfer in the latter context to know whether Sierra was truly allowing shared access or whether it was merely a mis-configuration. From a technical perspective, this is a situation of authorised access to the information found in the zone transfer. From a legal perspective, the judge ruled that access was unauthorized with a large emphasis placed on the defendant's intention to obtain and divulge information found in the zone transfer.[57] David Ritz is a well-known anti-spammer. There has been debate as to whether Sierra has facilitated spam in the past. Neither of these two facts appeared to weigh into the decision. While *Sierra v. Ritz* is a civil suit, Ritz has been criminally charged with unauthorised access to a computer in North Dakota. Although the charges were later dropped, Ritz lost the civil suit and court reasoned that "Ritz's behaviour in conducting a zone transfer was unauthorized within the meaning of the North Dakota Computer Crime Law".

The case illustrates how the terms 'unauthorised' and 'access' do not produce a similar set of shared assumptions in the technical, legal or ethical fields. A technical researcher may falsely assume that they are operating within safe legal parameters only to discover that such parameters do not translate across fields. The technical researcher would likely assume that he/she is authorised to perform an act where technical protocols and programming convention allow for it. From a legal standpoint, authorisation and consent involve a number of factors including intention, damage, and the bargaining position of affected parties. One commentator on the decision noted that it is the equivalent of, "Mommy, *can* I have a cookie? Sure you can have a cookie, but you *may* not."[58] The case foregrounds a recurring theme: if a user interacts with a server in a way that the protocol does not prohibit but which is upsetting to the server's operator, should this be construed as "unauthorized access" as a matter of law?[59] The scope of unauthorized access in computer fraud statutes is an old question.[60] Whether or not this would constitute a "hack" is one question, and if it is a "hack" then surely the motives appear to be somewhat ethical.

7.10 Observations

Exemption from liability and criminal prosecution has been argued for application to security researchers, and for acts that threaten to cross technical and accepted protocols. A resounding

---

[56] The judgment is unreported. A copy of the decision is accessible from private list-serves as well as from the webpages of SpamSuite.com. *Sierra Corporate Design Inc. v. David Ritz*, (2007) District Court, County of Cass, State of North Dakota, File No. op-05-C-01660 *See* www.spamsuit.com.com/node/351.

[57] A detailed analysis of the case can be found on SpamSuite.com available at http://www.spamsuite.com/node/351.

[58] Rash 2008.

[59] Original idea expressed by Paul Ohm in the cyberprof list serve.

[60] Kerr 2003.

question underlies the debate: do the ends justify the means? Some examples might include the Recording Industry's proposal to hack into users' computers to find infringing material and cyber-activists placing Trojans on child pornography to track and record the contents of offenders hard-drives for evidential purposes. These examples go to the question of intent as well as whether or not an act may be justified as social utility for the good of the public similar to how public interest exemptions work for the admissibility or otherwise inadmissible evidence in court.

For example, if one argues that David Ritz has indeed accessed the zone transfer without authorization, inevitably one must question his motive, intent and whether such activities were performed in the public interest. Peering into the zone transfer to document illegal spamming activity may indeed be in the public interest. If one successfully concludes that no unauthorized access was performed due to the public nature of the zone transfer and DNS, it seems equally perverse to not consider motive and intent. By way of analogy, if I have equipment to make false passports along with a stack of 200 shell passports (no photos or false names inserted), the trajectory towards the commission of a crime is called into question. Accessing information in the zone transfer for illicit purposes should attract attention, if not a penalty. The implication, however, of criminalizing an act of accessing publicly available information without illicit intent, calls into question the utility of 'unauthorized access' provisions. The inconsistency of the courts' interpretation of 'unauthorised access' makes the use of the provision unpredictable as well as malleable to prosecutorial will. The scope of 'unauthorized access' is ripe for reconsideration and debate.

There is no public interest exemption for computer offences. A public interest exemption refers to unauthorised access, modification or impairment where it is in the public interest to break the law. Typically, this might relate to security research but there are other instances that go beyond mere research which may justify the law being broken. There are reasons to allow for a public interest exemption. However, in my opinion these reasons are not sufficiently compelling at this point in time as to open up the exemption beyond security research. The idea of a public interest exemption, however, should be given further consideration by governments.

8. Counter-Attack

8.1 Description

Counter-Attack is also referred to as hackback or strikeback. Counter-attack is when an individual or organisation who is subject to an attack of their data, network or computer takes similar measures to attack back at the "hacker/cracker".

Counter-attack also refers to a self-help measure used in response to a computer offence. In most instances computer offences refers to an act that is or has already occurred such as a cyber attack (Eg. deliberate actions to alter, disrupt, or destroy computer systems), or specific types of cyber attacks such as unauthorised access or modification to data or computer system (Eg. this may merely mean accessing a computer system), installing malware onto a computer system, or launching a denial of service attack.

Consider the example of a denial of service attack launched against a corporation's website. A botnet has been used to launch the DDoS. The corporation would have several options to pursue:

1. Implement passive measures to strengthen its defensive posture (Eg. upgrade security software, firewalls, and training to staff).
2. Report the cyber attack to law enforcement authorities, and leave it to the law enforcement authorities to take appropriate action. If the DOS attack has been done for blackmailing purposes, the corporation may elect to pay the sum.
3. Do nothing and wait for the attack to be over. Purchase insurance against cyber attack to mitigate against future attacks.
4. Contact a third party specialising in cyber attacks to assist in the matter (Eg. AusCERT, SANS Institute, National Cyber Forensics and Training Alliance).
5. Take self-help measures to gather information and investigate the source of the attack with the view of mitigation of damage and traceback to the source
6. Take actions to actively neutralize the incoming attack through forms of counterstrike such as a counter of denial of service attack

Often an organisation will use a combination of options in dealing with the matter. Mitigation of damages is the key priority of most corporations when under cyber attack.[61] The most important component in mitigating against damage is protecting assets not already compromised. This could mean protecting data that has not yet been stolen. This could mean stopping the denial of service attack as soon as possible through various means – technical measures, paying a bribe, or launching a counter denial of service attack. Damage control may also mean ensuring that there is no media attention to the matter in order to keep stock prices from falling. Corporations and organisations are taking self-help measures such as counter-attack.

8.2 Case Study

LulzSec, Mastercard & Paypal, and Barr

The Lulzsec DDoS attacks against Mastercard and Paypal were motivated by the treatment of Mastercard and Paypal's refusal to accept online donations for the Wikileaks situation. Someone (perhaps members of the Mastercard and Paypal team, or perhaps other security researchers upset with Wikileaks) launched a counter denial of service attack at the LulzSec website. One DDoS attack was met with a counter-attack.

Additionally, law enforcement were on the hunt for the members of LulzSec who had launched the attacks against Mastercard and Paypal. During this time, security researcher Aaron Barr, CEO of HBGary Federal, was privately investigating the matter and claimed that he had identified the members who had performed the attacks, and had proof of the matter. Aaron Barr's emails on the matter were leaked to the Internet and may be found on a number of websites.[62] According to the leaked emails, Barr used Internet Relay Chat (public channel) to obtain the handle names of those members involved in the attack. He then used social media such as Facebook and LinkedIn to allegedly look at friends and family of the hacker group. He then made inferences to the point where he claimed he had identified members who launched the attack. Members of LulzSec retaliated claiming he had put many innocent individuals in danger. If Barr had indeed used social media to retrieve this information, his methodology remains unclear. Most people are unable to view one's Facebook account unless they befriend them. There are, however, methods to hack into a Facebook account without authorisation.[63] It is likely that Barr had indeed accessed this information without

---

[61] Email correspondence with Ron Plescoe, Director of the National Cyber Forensics and Training Alliance (NCFTA). *See also* Purdy 2009.

[62] For example, the emails are provided on The Old Computer at http://www.theoldcomputer.com/blog/index.php?start=60

[63] AusCERT 2011 presentation.

authorisation. Members of LulzSec responded to Barr's claims by allegedly copying 40,000 emails and making it available on piratebay, launching a denial of service attack to his company's website, and posting the message, "now the Anonymous hand is bitch-slapping you in the face".

According to the UK newspaper The Guardian, the exposed emails from HBGary revealed that they, along with security firms Palantir and Berico, "were discovered to have conspired to hire out their information war capabilities to corporations which hoped to strike back at perceived enemies, including US activist groups, WikiLeaks and journalist Glenn Greenwald."[64] An interview with Dreyfus revealed a similar theme of corporations and governments engaging "cowboy security firms" to perform attacks either directly on hacktivism websites and other targets. Dreyfus also revealed that there were several recent attacks performed by cowboy security firms who have made it look as though such attacks came from Anonymous. The contracting out of intelligence services, "for hire cyber-attack services" by governments to security firms was also exposed in the Canadian television program The Agenda.[65] Identifying attack sources is a difficult proposition as will be seen in section 9."

8.3 Motivations

Counter-attacks are launched as a form of self-defence or as a means of retribution. The LulzSec and Paypal example certainly highlights the retribution motive. However, most organisations perform acts of counter-attack as a form of self-defence. In 2001, researchers surveyed 528 IT managers in Western Australia and Victoria to obtain their views on counter-attack. Those surveyed were asked a variety of questions including whether strike-back should be allowed if their organisation was subject to an attack (65% replied yes, 30% no, and 5% were undecided).[66] This question was then broken down into specific types of attacks such as attempt at network access and attempt to destroy or alter data where the yes response rates increased to ranges between 70% and 93%.

8.4 Main Targets

The main targets are the IP addresses (often websites or computer) that initialise the attack. Information may also be gathering and collected where possible of those individuals who perform the attack though this is often very difficult to trace as will be seen in section 9.

8.5 Relation Between Targets and Motivations

Again, the motivation is either to defend or retaliate against the origin of the attack. The target is normally a website, and does not typically involve the individual per se behind the attack (because identification is often difficult).

8.6 Fundamental Principles of "Hacker-Ethics"

There are a variety of ethical and moral issues at play with counter-attack. One principle could be seen as defending one's property against attack. The other main principle is retribution. There appears to be an additional principle of hacking to discredit an organisation, typically by deliberately launching an attack to make it look as though it has come from another organisation. There appears to be foul play by most parties involved with hacktivism counter-attack.

---

[64] Huffington Post October 2, 2011.
[65] The Agenda, October 25, 2011
[66] Hutchinson, et al. 2001.

8.7 Perceptions of the Illegality of Activity

There is no consensus as to whether corporations and organisations engaged in counter-attack are aware of the illegality of their activity. Some security software will automatically initialise a counter-attack whereby the organisation may or may not be aware. It may be the case that those individuals running the security of the organisation are aware of the illegality of the action, but that the Board of Directors is kept in the dark. There is also evidence that many organisations employ former black hat hackers under strict control and surveillance yet this type of arrangement is rarely publicised.[67]

8.8 Deterrence Effects of Case Law and Convictions

Unknown and untested. There are no cases against a corporation or organisation that has engaged in counter-attack.

8.9 Relevant Case Law and Convictions

None. In section 5 it was noted that there are ongoing investigations, and arrests had been made against two members of LulzSec for participation in the Mastercard and Paypal attacks. There has been no public investigation nor charges laid against those responsible for the DDoS attack against the LulzSec website. Furthermore, there has not been a public investigation made or charges laid in relation to how Aaron Barr obtained his supposed information of members of LulzSec through social media. There have not been any arrests made for those members of LulzSec/Anonymous responsible for releasing Aaron Barr's personal email, and for the DDoS attack of his website. It would appear that investigations and charges are highly, and perhaps unfairly, discretionary in this area of law.

8.10 Observations

Self defence may apply to some forms of counter-attack. There are no cases that deal with defending oneself against an online attack. There is likewise little literature on the topic. In this instance the Australian Model Criminal Code (MCC) provides guidance as to the scope of self-defence in such situations. The MC discussed at length the growing trend in the United States for corporations' use of computer software with counter-strike abilities. The MC stated that:

> "It is possible that the defence of self-defence in Chapter 2, s.10.4 of the Model Criminal Code might extend to some instances of computerised counterattack against cybernet intruders. Self-defence includes conduct which is undertaken "to protect property from unlawful appropriation, destruction, damage or interference". It is possible that a strikeback response to the hacker's attack could be characterised in this way.
> In practice, counterattack involves serious risk s since hackers are likely to adopt precautions which divert the counterattack to innocent third parties.
> It is apparent that principles of self defence of persons, which extend without undue strain to include protection of tangible property, are inadequate for the purpose of regulating computerised counterattack against hackers. The familiar concepts of necessity and reasonable response, which excuse or justify counterattack against physical threats, are next to useless as guides in this field."[68]

---

[67] For example, former botnet master Owen Walker is now employed by Telstra. *See* Maurushat 2011.
[68] MCC, note 5 above, page 108.

The MC committee concluded that "legislative intervention would be "premature". They further noted that corporations who resorted to self-help / hackback "would be left to the uncertain promise of a merciful exercise of prosecutorial discretion."[69] The concluding sentence provides even more ambiguity to the MC where it is stated:

> "The familiar criteria of necessity and proportionality which govern self defence in other applications have no obvious application here. Reliance on a test of what is or is not reasonable in the way of counterattack against hackers would place an inappropriate legislative burden on courts to determine issues of telecommunications policy."[70]

The conclusion seems to echo a recurring theme of "This is a tough one so let's wait and see." The MCC declared that legislation was premature and that courts should not be the ones to determine issues of telecommunications policy. So who should make these determinations? The reality is that individuals and corporations are making these determinations as a matter of internal policy. An anonymous survey on self-help/hackback measures was put to the attendees of the AusCERT 2009 conference. Over 20% of the audience indicated that their corporation or organisation used hackback. Another 25% stated that their corporations are currently considering the use of hackback[71]. In closed conference sessions with Chatham house rules, chief information officers from banks, internet service providers, Internet auction sites and Internet payment companies have all indicated that they employ blackhat hackers whose work is closely scrutinized. Counterstrike against a denial of service attack was a common hackback method – some hackback was performed with authorisation from the Board of Directors, but mostly circumstances are kept quiet and unreported to the Board of Directors.[72] However, the report came out in 2001 and the prevalence of self-help remedies may not have been the same as it is in 2012. There have been no Parliamentary statements since 2001 on hackback.

9. Technical and Legal Challenges in Investigation and Prosecution

There is often a false belief amongst law makers that if the right legislation is enacted and if enough resources are allocated to the task that law can rise up to the challenge and overcome a myriad of obstacles to combat cybercrime. Cybercrime investigations, whether it be for online identity theft, selling counterfeit products via spam, or hacking (unauthorised access, modification of impairment/interference with data or data systems), involve unique challenges. The challenges involve difficulty with harmonisation of laws, jurisdictional issues, resource implications, lack of training, ambiguity in terms of how a criminal provision will be interpreted alongside human rights protections, and, above all, a host of technical hurdles making tracing back to the "offender" difficult.

The following sections *assume* that investigation and prosecution of an ethical hacker is desirable; there are good arguments as previously discussed for exemptions to apply to ethical hacking, especially in situations where the online activity corresponds with legal

---

[69] MCC, note 5 above, page 109
[70] MCC, note 5 above, page 109
[71] Survey on file with the author.
[72] Contemporaneous notes by author filed with research materials from closed panel sessions at AusCERT 2008 Conference, AusCERT 2009 Conference, and Internet Security and Intelligence Operations 5 Workshop 2007, Estonia.

offline activity. This typically occurs at the intersection of the act with protection of human rights / civil liberties.

9.1 Obfuscation Technologies

Many different techniques exist to make traceback of an attack to the original source difficult. These technologies/techniques will be described as "obfuscation tools", as such tools allow people to evade technological controls and legal sanction.[73]

Commonplace obfuscation techniques include dynamic DNS, multihoming, FastFlux DNS, distributed command and control (superbotnet), encryption, proxy servers, virtual platforms, rootkits, and the use of peer-to-peer channels. These tactics allow people to hide behind a cloak of anonymity and low possibility of traceback of an attack to its source. These key terms are defined below:

Multihoming involves the configuration of a domain to have several IP addresses. If any one IP address is blocked or ceases to be available, the others essentially back it up. Blocking or removing a single IP address, therefore, is not an effective solution to removing the content. The content merely rotates to another IP address.

Dynamic DNS is a service that enables the domain name entry for the relevant domain-name to be updated very promptly, every time the IP address changes. A dynamic DNS provider enablers a customer to either update the IP address via the provider's web page or using a tool that automatically detects the change in IP address and amends the DNS entry. To work effectively, the Time to Live (TTL) for the DNS entry must be set very short, to prevent cached entries scattered around the Internet serving up outdated IP-addresses.

FastFlux is a particular dynamic DNS technique used by botnet masters whereby DNS records are frequently changed. This could be every five minutes.[74] Essentially, large volumes of IP addresses are rapidly rotated through the DNS records for a specific domain. This is similar to dynamic DNS tactics. The main difference between dynamic DNS and FastFlux is the automation and rapidity of rotation with a FastFlux botnet.[75] Some FastFlux botnets rotate IP addresses every hour, and others every day.

Distributed Command and Control (or Superbotnets) is a type of botnet that draws on a small botnet comprised of 15-20 bots. The botnet herders may have anywhere from 10 000 to 250 000 bots at their disposal, but use a select few for a particular purpose. The smaller botnet is then used to issue commands to larger botnets (hence the term distributed command and control).[76]

Encryption is the conversion of plain text into ciphertext. Encryption acts to conceal or prevent the meaning of the data from being known by parties without decryption codes. Encrypted instruction can then not be analysed making investigating, mitigation and prevention much more difficult. Public

---

[73] Lovet 2009.
[74] *See* The Honeynet Organisation at http://www.honeynet.org/node/132.
[75] Dunham 2009.
[76] Barakat et al.

key cryptography is often used. In public key cryptography, a twin pair of keys is created: one key is private, the other public. Their fundamental property is that, although one key cannot be derived from the other, a message encrypted by one key can only be decrypted by the other key.

Proxy servers refer to a service (a computer system or an application) that acts as an intermediary for requests from clients by forwarding requests to other servers. One use of proxy servers is to get around connection blocks such as authentication challenges and Internet filters. Another is to hide the origin of a connection. Proxy servers obfuscate a communication path such that User M connects to a website through proxy server B which again connects through proxy server Z whereby the packets appear to come from Z not M. Traceback, however to Z yields information of an additional hurdle as packets also appear to come from B. Other proxy servers such as Tor are anonymous. Tor is also known as an onion router. Tor is described as follows:

> "Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody from watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location."[77]

Tor is described as onion routing due to the use of multiple layers of proxy servers. This is similar to the multiple layers of an onion. Tor is used by users in heavily Internet-censored countries like China and Iran to access blocked websites as well as being used by some criminals to prevent law enforcement from traceback to the source.

Virtual Private Network Service (VPN) is a network that uses a public telecommunications infrastructure (usually the Internet) to connect remote sites or users together[78]. This connection allows a secure access to an organisation's network. Instead of a dedicated, real-world connection such as a leased line, a VPN uses "virtual" connections routed through the Internet from an organisation's private network to the remote site or employee."[79] VPN is made secure through cryptographic tunnelling protocols that provide confidentiality by blocking packet sniffing and interception software.

Rootkits are software or hardware devices designed to gain administrator-level control and sustain such control over a computer system without being detected.[80] A rootkit is used to obscure the operation of malware or a botnet from monitoring and investigation. It may also be used as a way for an ethical hacker (if he or she has installed it) to monitor the actions of a government or corporation, as well as to look and copy documents on others' servers.

Peer-to-peer Communications (P2P) "is any distributed network architecture composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances."[81] A P2P network relies on the capacity of multiple participants' computers, each of which has both client and server capabilities. This differs from conventional client-server

---

[77] Tor available at https://www.torproject.org

[78] Virtual Private Network available at http://www.en.wikipedia.org/wiki/Virtual_private_network

[79] Tyson 2009.

[80] Pfleeger 2007..

[81] The author looked any many different definitions of peer-to-peer and found the Wikipedia definition had the best description. *See* Wikipedia "Peer-to-peer" available at http://en.wikipedia.org/wiki/Peer-to-peer

architectures where a relatively low number of servers provide the core function of a service or application.[82] Such networks are useful for many purposes such as sharing of scientific information amongst researchers, file-sharing of videos and music, and for telephone traffic. P2P operates on peer nodes[83]. P2P may be used to send content in clear or encrypted format. The ad hoc distribution of P2P makes it an ideal bot server location for command and control. The use of P2P channels allows an additional layer of rapid IP address fluctuation. For this reason, botnets that use in P2P channels are seen as offering the equivalent of "double fast-flux".

Security researcher Lovet describes the difficulty of traceback to the IP address of the botnet master in the following persuasive manner:

> "To put it simply, when a stateful Internet connection (a.k.a. a TCP connection) is established between Alice and Bob, Alice sees Bob's IP address. Thus if Bob does bad things to Alice via this connection, his IP address can be reported. Now, if Cain connects to Bob, and from there, connects to Alice with bad intentions, Alice will still only see Bob's IP address. In other words, Cain has masked his IP address with Bob's. The component which allows Cain to use Bob as a relay is called a proxy (there are various types of proxies, though in cybercriminal schemes socks4 and socks5 proxies are mostly used). Such a component, of course, may have been installed on Bob's computer without his knowledge, by Cain. Or by Daniel, and Cain just rented or purchased access to it. As a matter of fact, most trojans and bots embed a proxy, and in any case, have the capability of loading one after prime infection. Given the prevalence of bot-infected machines (a.k.a. zombie computers), that makes a virtually endless resource of proxies for cybercriminals, all sitting on machines of innocent, unaware users. This is something cybercriminals understand perfectly and exploit ruthlessly, sometimes on a large scale."[84]

When an obfuscation method such as a proxy or fast-flux is utilised, traceback will often only lead back to the infected bots that form part of a botnet, or to the IP addresses of the C&C. Once the IP address is known for the bot, the individual who has registered the Internet connection from that computer to the ISP may be contacted. An IP address does not, however, tell you who used a computer to perform a crime. If a computer is used by several people, identifying the botnet master will require additional evidence other than a mere IP address. The botnet master may only be targeted upon discovering where the command and control is occurring and tracing back through proxies to the original source. Discovering the C&C point where a botnet receives its instructions from, however, neither reveals the exact computer source nor the identity of the botnet master. In the rare chance that the identity of a botnet master can be traced back, the botnet master can always use the "Trojan horse" or "bot" defences which may or may not prove successful (see section 9.4).

Many online civil disobedience participants do not have the computer skills required to use such obfuscation techniques. They are more limited to using LOIC. An encrypted version of LOIC is now being developed. This will present a further challenge to law enforcement to identify those participants in DDoS attacks using LOIC.

---

[82] Clarke 2004.
[83] Oram 2001.
[84] Lovet 2009.

9.2 Integrity, Volatility of Evidence and the Trojan Horse Defence

Digital evidence suffers from volatility. Volatility refers to the ease by which one may alter or damage evidence whether it is done accidentally or intentionally. This in turn makes it relatively easy to expunge volatile evidence and to create 'reasonable doubt'. For example, the mere making of a copy of a file and putting it onto a USB memory stick interferes with the integrity of the digital evidence. Another common example is when an employee with a company's technical division takes it upon herself to view a quick online tutorial then proceeds to install and use forensics software on the company's computer or server. When forensics software and equipment are used without proper training it is probable that the integrity of the evidence will be jeopardized. Forensics investigators, by way of example, use a device which makes tampering with evidence impossible, and take a virtual snapshot of a computer or server (if possible) which can then be analysed at a later date. Without such preventative measures, digital evidence is subject to being expunged from evidence.[85] Forensics investigators have these basic technologies which allow for proper collection and preservation of data. The concern, therefore, is not that such technologies are not widely available or that their cost is prohibitive. The concern is one of education and training. When proper forensics techniques are not used, the integrity of the evidence is lost.

Where technology is involved in a crime, the accused will often use the "Trojan horse" or "bot" defence. In this instance, a party claims that they are not responsible for an action, but rather, a malicious software program such as a "Trojan" was unknowingly downloaded to their computer by a third party. In a "bot" defence, the argument is that the defendant's computer became a bot and controlled by a malicious third party. Thus the "Trojan" or the "bot" is to blame. In the case of a botnet, it may seem odd that a "Trojan horse" defence would be tried when the criminal act is often the very installation of an unauthorised 'Trojan' onto someone else's computer. This, however, is not necessarily the case. A botnet master, for example, could argue that his/her computer was being used as a proxy to make it look as though the botnet was installing Trojans. This argument could conceivably extend to the claim that command and controls were orchestrated to come through his/her computer via malware where the bots (software programs) were installed by a third party. Alternatively, a botnet master might claim to operate a botnet but could make the argument that a third party (another botnet master) took over his/her botnet through issuing an unauthorised bot (software code) to perform illegal acts.

An example of a prosecution failure for these reasons is a judgement in the United Kingdom against Aaron Caffrey. As reported, Aaron Caffrey was a 19 year old who launched a distributed denial-of-service attack on September 20, 2001 affecting computers serving the Port of Houston, Texas.[86] The attack caused major havoc with shipping logistics. The accused claimed that a malicious program had been installed on his computer, and that he did not perform such acts. The jury acquitted in spite of the fact that upon examination, common hacker tools were found on the defendant's computer, the defendant was a known hacker who regularly participated in discussion of how to launch DDoS attacks and other types of malware, while possible forms of malware were absent on

---

[85] Klein 2010.

[86] The case is not reported in law databases but was covered by the British media and is mentioned by several cybercrime researchers. *See* BBC News, "Questions Cloud Cyber Crime Cases" October 11, 2003 available at http://www.bbc.co.uk/2/hi/technology/3202116.stm (last accessed April 27, 2010). The case is mentioned as R *v. Caffrey* (2006) in Clayton, R. "Complexities in Criminalising Denial of Service Attacks" written for the Legal Subgroup of the Internet Crime Forum (Feb. 2006) available at www.cl.ram.ac.uk/~rncl/complexity.pdf.

the defendant's computer.[87] The evidence was overwhelmingly in favour of a successful prosecution, but the technical evidence was presented in a confusing manner which one journalist describes as:

> "Had the jurors been technology experts, or even computer-literate, I wonder if the ruling would have been the same. I spent most of the first week of the trial in the public gallery and found it didn't take long before the jury's eyes glazed over because the technical arguments sounded like a Russian version of Moby Dick that had been translated into English using Babelfish. By the third day, one of the jury members had to be discharged because of a severe migraine, which was indubitably brought on by the jargon."[88]

This case reinforces that while digital evidence is volatile, even sound evidence is subject to the "Trojan horse" and "bot" defences due to the inability of jurors and judges to understand the technical complexities of some cyber crime cases.[89]

9.3 Real Time Forensics and Interception

The value of real-time forensics is perhaps best illustrated by way of analogy. CCTV surveillance cameras are installed for example, in public spaces and on highways. The cameras are used in two capacities. First, when monitored they may be used to identify potential problems before a crime is committed, or to actively alert law enforcement while the crime is being committed. Second, they might not be monitored but footage from the cameras may be used as evidence post-crime. Of course, such cameras also perform surveillance functions collecting personal information of non-criminals, potential in breach of privacy and surveillance laws.

Real-time forensics operates on a similar premise. Real-time forensics can operate in two ways: general evidence collection without a suspect in mind or specific evidence collection with a suspect in mind. Let us first consider general collection of real-time evidence. ISPs routinely monitor their networks using technologies such as Netflow for suspicious or abnormal Internet traffic. Where a crime is committed, a warrant may be issued allowing law enforcement agents to access ISP data logs (if any) stored at the time of the crime. The value of evidence collected post-crime is dependent on the monitoring and detection technologies used by the ISP. Many ISPs use medium packet inspection technologies such as Netflow. Netflow does not maintain data logs for long before they are deleted. Where more invasive technologies such as deep packet inspection are used there is potentially more value-rich information for post-crime investigations. This is either because the monitoring is more substantive or it could merely mean that the data traffic logs are stored and retained for longer periods of time. Both medium packet inspection technologies such as Netflow and deep packet inspection technologies are capable of collecting evidence in real time.

The term "real-time evidence" is not very useful. The importance lies in what type of information is collected by the packet inspection technologies, the length of time that it is stored and retained (typically data traffic logs), and the ability of law enforcement to use this information. This type of information request by law enforcement agents to ISPs is referred to colloquially as a "data dump" – any information that an ISP may have stored relevant to an IP address or range of IP addresses.

---

[87] Grabosky 2007.
[88] Brenner 2004.
[89] Walden 2010.

General ISP evidence collection without a suspect in mind is often of little value to law enforcement agents. This may be due to a number of reasons: 1) the type of data collected was not useful, or 2) the type of data was useful but was not stored, or 3) the volume of data collected is too large a quantity to be of timely use in an investigation.

The second scenario looks at real-time evidence collection when there is a suspect in mind. In this instance, a law enforcement agent may apply for an appropriate content warrant. The communications of the suspect could then be intercepted. Depending on the type of warrant, this could include website contents and email mail-box contents (stored communications warrant), or information about IP traffic to and from a target IP address/address range or VOIP traffic to and from a phone number.

Unlike crimes in the physical world, often there is little physical evidence after a cyber- crime is committed unless there is real-time data collection and retention. Real-time forensics is also known as live forensics as distinct from post-mortem forensics.[90] Real-time data collection allows the capturing of:

> "Volatile information that would not normally be present in a post-mortem investigation. This information can consist of running processes, event logs, network information, registered drivers, and registered services. Running services tell us the types of services that may be running on a computer. These services run at a much higher priority than processes ... Viewing running processes with the associated open network ports is one of the most important features of analysing the system state."[91]

Without real-time evidence, there is heavy reliance on the physical memory (RAM) of a computer. As previously seen with obfuscation tools, dynamic methods are used where information is neither stored centrally nor statically. The likelihood of stumbling on physical memory after the fact is negligible. Real-time data collection allows entire contents of an email mail-box to be captured, whether the information is local or remote.[92] Where real-time data is stored, law enforcement agents are potentially able to peer at the email mail-box pre-crime, post-crime and during the commission of a crime. The capturing and storing of real-time data requires the assistance of ISPs who are the middle men or information conduits. The co-opting of ISPs to assist law enforcement is contentious.

9.4 Damages

In theory, if there has been unauthorised access, modification or impairment of data an investigation may be mounted and perpetrators prosecuted. In practice, often a victim must be able to prove that a certain amount of money was lost or damage suffered in order to prompt an investigation.[93] The amount is often pure conjecture. Many jurisdictions have predetermined thresholds amounts in order for an investigation to be launched. Arguably, many forms of unauthorised access or a DOS attack for two hours may not cause enough damage to attract investigation. These thresholds are determined by internal police working committees. Not all law enforcement investigation units have minimal monetary amounts. In some jurisdictions, a decision to launch an investigation in the case of computer related cybercrimes is dependent on a wide range of factors which include whether the

---

[90] Reyes 2007.
[91] Reyes 2007.
[92] Reyes 2007.
[93] de Villiers 2003.

crime is serious or organised crime and whether the investigation is within the capabilities of the local police. [94]

9.5 Jurisdiction

Computer crimes often involve parties located overseas. These crimes may involve many people located in different jurisdictions whether they are different states or provinces within a country, or different countries altogether. Each jurisdiction will have its own laws dealing with an issue as well as its own unique set of evidence procedures in courts. Uniformity is a real problem. A successful prosecution often involves assistance and cooperation of authorities from an outside jurisdiction. For a variety of reasons, some jurisdictions may or may not be willing to cooperate. Such cooperation generally must proceed through the cogs of bureaucracy in cases where time and access to good digital evidence (unaltered) is of the essence. This often means applying for warrants in multiple jurisdictions which may translate into a loss of valuable time and perhaps a loss of obtainable evidence.

The greatest challenge, however, remains in identifying and determining the physical location of the computer, and then the actual individual(s) who used the computer/network to commit a crime. The Canadian police, for example, cannot obtain a warrant to wire-tap someone in Mongolia and they cannot compel an ISP in Papa New Guinea to provide data logs. This type of international policing requires the cooperation of law enforcement and courts in other jurisdictions. Law enforcement could contact law enforcement in the location of the hacker but cooperation may not be forthcoming. First, inter-jurisdictional investigations rely on the offence being given similar priority in both jurisdictions. For truly repugnant cases such as child pornography, jurisdictions tend to have similar strong mandates.[95] In the case of hacking (unauthorised access), the priorities are often disparate. This is especially true in jurisdictions without computer misuse offenses. It is of no coincidence that Wikileaks servers are located in protective jurisdictions. The LulzSec website is hosted on a cloud computing space.

The situation is somewhat reversed when subpoenas for data logs are sent to US based communication services such as Google, Twitter or Facebook. In this instance, the law of the server prevails. For example, if I am a Twitter user located in Australia, an American law enforcement entity may issue an administrative subpoena without a warrant or transparent declaration of the scope of a criminal investigation, to actively retrieve all data logs connected to a hashtag. For example, one could request all communications, IP addresses, and subscriber information for everyone who communicated in the Occupy Wallstreet movement, including those of people located around the globe. In this sense, the international criminal justice system by way of established treaties, and data protection of citizens in foreign countries, is subverted. The law of server (often the United States) prevails.

The second challenge is related to the first in that police tend to use their resources to respond to local problems. Where there is no victim in the locale of the police force, priority will not be given to an overseas investigation. Third, there is again the de minimus rule whereby in order to justify valuable police resources, a certain threshold of damages must be met. The jurisdictional hurdles stem from practical considerations as well as a lack of criminalisation of an act across jurisdictions.

---

[94] Correspondence with Detective Van der Graf, head of the Fraud Squad, New South Wales Police. Notes are on file.
[95] Wall 2007.

9.6 Issues in Ethical Hacking

One of the greatest challenges for ethical hacking prosecutions will be how the evidence was obtained. If governments are outsourcing intelligence to security firms, it is likely that many of such firms will use hacking methods to obtain their information. There is no legal mechanism that allows such firms to perform such actions. There is furthermore no way to ensure accountability of such firms at present. One assumes that evidence collected by law enforcement would have been done according to the law but this too turns out to be a murky legal area. For example, in 2001 the US Federal Bureau of Investigation ('FBI') lured two Russian criminal hackers to Seattle under the guise of a job offer with an FBI invented corporation, Invita. Alexey Ivanov and Vasily Gorshkov were promptly arrested when they arrived on US soil. What they thought would be a job interview quickly turned into an interrogation from law enforcement. The two allegedly broke into the networks of bank and other companies. The FBI remotely installed keylogging Trojans on the suspects' computers and collected evidence including the passwords to email accounts. Incriminating evidence from the suspects' computers and servers utilised for email were used to convict the two on charges under the *Computer Fraud and Abuse Act* 18 USC § 1030 (1986), as well as 20 counts to conspire and a number of fraud counts.[96] The evidence was collected without a warrant, but the Court nonetheless deemed the evidence valid, rejecting motions for its suppression. The Court ruled that the right against unreasonable search and seizure under the Fourth Amendment was not violated because the accused had no right to privacy when using computers at the fictitious offices of Invita.

On a similar note, it remains to be seen if Twitter users outside of the United States will be afforded the protection of free speech and privacy of data when they are not themselves the object of investigation, but where law enforcement solely seeks to acquire personal information. It remains unknown if a non-US Twitter user would have standing in an American court. As seen in the Invita situation, free speech and privacy protection will likely not extend to non-Americans.

A most problematic theme has emerged with hacktivism. Many hacktivists seek to rebel against what they perceive to be unjust policies or measures that infringe against civil liberties. As a consequence of the flury of hacktivist activities, however, governments around the globe are using more and more forms of surveillance, and civil liberties are eroding further than in the pre-hacktivism era. At this point, it is a vicious circle with laws being broken by both sides.

It is curious to see so much law enforcement resources being allocated to hacktivist investigations, yet so very little resources allocated to the fight of online organised crime such as mass fraud, identity theft and corporate espionage.

10. Key Findings

- Online protests will increase and the type and size of such attacks will escalate in order to continue to capture the interest of the media.

- There is a growing movement in some online communities (hackers) to ensure that "backdoors" (ways to exploit a program) are inserted into computer programs and then kept

[96] *United States v Gorshkov* (2001) WL 1024026 (Western District Washington).

quiet as a means of ensuring access to future information (especially government websites). These types of "attacks" are not done for instant media attention.

- Technologies such as LOIC will evolve to allow for encryption and anonymity. This will parallel similar developments that took place with peer to peer file-sharing networks.

- The most popular discussion threads in hacking forums are "beginner hacking" and "hacking tools and programs" indicating the likelihood of increased hacking, both ethical and for criminal purposes.

- Deterrent effect of laws and sentences only works with beginners and with younger hackers. These individuals will generally quit illegal hacking after first conviction (under 25).

- The law does not have a deterrent effect for highly skilled and often older hackers (over 25).

- Some individuals involved in hacking are considered be have an addiction in the same way that an individual may become addicted to gambling, video games, drugs or alcohol.

- A significant portion of corporations and organisations are engaged in some form of counter-attack.

- Many ethical hacking incidents are closely tied with the objective of protecting human rights and promoting an open, transparent democracy.

- Many ethical hackers view their work as acts of civil disobedience and align their actions with traditional civil disobedience as espoused by Ghandi, Martin Luther King Jr. And Henry David Thoreau.

- Other hackers identify with an ethos of hacking that developed in the 1980s forward and look to technical gurus and the writings of "Hacktivismo Declaration" by the Cult of the Dead Cow, "The Hacker Manifesto", "The Anonymous-Anonops", The Electrohippies "Client-Side Distributed Denial-of-Service" and the "Gospel According to Tux".

- Other groups are less ideal in their philosophy citing motivation as "for the laughs". However, further probing of such hackers reveals that their hacking is done out of "a streak of sense of wrongdoing" without always being able to clearly articulate what that wrongdoing is.

- Denial of Service Attacks by movements such as Anonymous require critical mass in order for an operation to be successful.

- There is often a correlation between the number of participants in a denial of service attack, and the worthiness/morality of the cause.

- Which causes will acquire critical mass is unpredictable.

- It would be incorrect for governments or organisations to assume that members of ethical hacking groups come from one type of community, race, or age.

- Many ethical hackers are not aware that their activities are illegal, especially those participating in politically motivated denial of service attacks.

- Elite hackers tend to work alone due to the higher risk of "getting caught" when groups are involved. This may support the proposition that a technically sophisticated attack may in fact be the work of only one individual, or few individuals.

- While many instances of ethical hacking may be illegal, it is interesting to note that some methods used by law enforcement and by security firms contracted to perform criminal intelligence gathering may also be illegal, or at best highly controversial.

11. Recommendations

- Develop and publicise guidelines for online civil disobedience and hacktivism.

- Run an education campaign once these guidelines are finalised.

- Allow and encourage a legitimate "space" for virtual protests.

- Investigate the licensing of security experts.

- Implement a security research exemption for computer offences.

- The idea of a public interest exemption for hacking offenses should be given further consideration. This could be done in a multi-party working group for both security research and public interest exemptions.

- Develop a code of conduct for counter-attack and have a legislative review of how principles of self-defence might apply to a counter-attack situation.

- Any governmental engagement with ethical hacking should be legal and transparent. These activities should not be contracted out to security firms unless they are closely scrutinised and held accountable in some form of safeguard or compliance mechanism.

- Review the insecure practices of corporations and organisations that hold sensitive personal data and consider implementing more effective legislation such as data breach notification and the obligation to encrypt all personal information held by such entities.

- Ensure that data owned or generated by Canadians is protected and that such data, if collected and stored, is deleted after a reasonable period when using foreign services such as Google, Facebook and Twitter (United States based). Currently, any person who uses Google, Facebook, Twitter and similar services is subject to US Internet monitoring by governments and law enforcement, and potentially is exposed to subpoenas to release personal information even in the *absence* of a criminal investigation.

12. Future Research

12.1 Canadian Charter of Human Rights and Freedoms

This report has not considered arguments that could be made to challenge charges made against ethical hackers under the Canadian *Charter of Human Rights and Freedoms*.

12.2 Internet Service Providers and Communication Companies (Facebook, Google and Twitter) Revealing Account Information

This report has not considered in any depth the thorny issues involved with revealing the account information and personal information of accused ethical hackers by social media companies such as Twitter, Facebook and Internet Service Providers.

The interim order for Twitter to produce detailed account records of Julian Assange and Bradley Manning is expected to be appealed to the Supreme Court of the United States on multiple grounds, including issues of privacy.[97] Similar requests in Canada could be fought on privacy grounds.

In a more disturbing instance, subpoenas to Twitter have been issued by Boston law enforcement to reveal personal information of any party connecting to tweet hashes connected to the Occupy Boston movement (including information communicated by journalists). This has included information of citizens around the globe. No warrants were sought nor has there been any information given as to the illegality of the criminal investigation.

This report has merely flagged some of these issues which are ripe for greater consideration and research.

12.3 Security Research Exemption or Public Interest Exemption

This report has not provided list of factors and considerations which are vital to any introduction of a security research or public interest exemptions to unauthorised access and modification provisions in criminal law. Likewise, this report has not analysed or considered recent European initiatives of licensing information security experts.

12.4 Full Exploration of Government Contracting of Surveillance and Intelligence Gathering

Anonymous has announced that, due to inadequacy of the media to report on surveillance and intelligence gathering issues, and due to the government lack of transparency, they will be targeting documents from security companies known to perform such functions under contract from the government or organisation. Further investigation into whether such studies exist, along with the exposure of such contracting as not been considered in depth in this report.

---

[97] *In re § 2703(d) Order, 2011* U.S. Dist. LEXIS 25322

13. Appendix A – Case Law Summary

The extensive caselaw review revealed a paucity of reported cases in the world on ethical hacking. In most instances, there was only media coverage on the arrest and charges laid in connection with the incident. The lack of criminal caselaw is caused by three key factors:

1) the currency of the actions (not enough time has elapsed for a trial to have occurred and a decision to have been reported in caselaw databases),
2) the accused may have settled the case, or
3) the accused may have agreed to act as an informant in exchange for all charges being dropped against him/her

The Appendix below details reported criminal caselaw, as well as reported arrests of ethical hackers in the media.

Germany

Andreas-Thomas Vogel

CaseName:	„libertad.de" - case
Citation:	File reference 1 Ss 319/05, 22nd March 2006
Jurisdiction:	decision of the Higher Regional Court, Frankfurt am Main
Main URL:	http://www.libertad.de/service/downloads/pdf/olg220506.pdf
Charged With:	Coercion, and incitement of alteration of data
Legislative Provisions:	§240 German Criminal Law: Coercion § 111 in conjunction with § 303a German Criminal Law: Incitement of alteration of data
Main Target:	
Motivation:	Denial of service attack against the websites of the German Airline "Lufthansa", in order to protest against the company. They deport illegal immigrant and make profit with this. The accused wanted to achieve more publicity of these grievances. He planned a denial of service attack at the 20th of June 2001 and programmed a small protest-software, downloadable for protestants to enable loads of pageviews. The demonstration had 13614 participants with different IP-adresses and encompassed 1,126,200 pageviews. The damages were about 5,500 € for personal costs and 42,000 € for further impairments.
Convicted Of:	Andreas-Thomas Vogel was indicted and convicted of coercion in the Frankfurt court of first instance. The Frankfurt Appellate Court reversed the decision stating the DDoS attack was a legitimate exercise of free speech.
Sentence:	Acquittal in the second instance
Additional	In the court of first instance the district court sentenced the accused with a

Important Information:	financial penalty of 90 days à 10 Euro in the first instance. The Higher Regional court reversed the verdict in the appeal

United States

United States Army v. Bradley Manning

The defendant was arrested after allegedly accessing and providing classified U.S. Government documents to Wikileaks. He was a U.S. Army soldier based in Iraq. He was charged in 2010 and is still awaiting a hearing.

ITEM	NOTES
CaseName:	United States Army v. Bradley Manning
Citation:	
Jurisdiction:	Army's Military District of Washington
Main URL:	http://en.wikipedia.org/wiki/United_States_v._Bradley_Manning, http://www.cbsnews.com/htdocs/pdf/ManningPreferralofCharges.pdf http://www.msnbc.msn.com/id/41876046/ns/us_news-security/ http://www.nytimes.com/2011/04/30/us/30brfs-PANELSAYSWIK_BRF.html?_r=1&ref=bradleyemanning
Charged With:	Transferring U.S. Government documents to a party not entitled to receive them (allegedly, Julian Assange of Wikileaks).
Legislative Provisions:	Uniform Code of Military Justice Arts. 104 (aiding the enemy), 92 (failure to obey a lawful order or regulation), and 132 (general article, including counts of offenses against the Computer Fraud and Abuse Act 1986 (U.S. Code s1030(a)), and 793, for communicating, transmitting and delivering national defence information to an Unauthorized source.
Main Target:	
Motivation:	United States Army
Convicted Of:	Public disclosure of U.S. Government (including foreign policy) documents in order to "change something" (according to the transcript of his chats with Adrian Limo, see Wikipedia).
Sentence:	
Additional Important Information:	Possibly life sentence if convicted of the most serious charge against him, aiding the enemy.
	22 charges including aiding the enemy and improperly obtaining a classified gunsight video. Proceedings have commenced in Forte Mead, Maryland.

US v Kevin George Poe

An Anonymous-affiliated Connecticut man, Poe, was arrested and charged with conspiracy and unauthorized impairment of a protected computer, after allegedly disabling Gene Simmons' website with a denial of service attack.

ITEM	NOTES
CaseName:	US v Kevin George Poe
Citation:	CR 11 01166
Jurisdiction:	Federal – US District Court for the Central District of California

Main URL:	http://techlaw.justia.com/wp-content/uploads/2011/12/poe-gene-simmons-12082011ind.pdf http://techlaw.justia.com/2011/12/14/indictment-alleges-ddos-attack-on-gene-simmons-web-site/ http://www.guardian.co.uk/technology/blog/2010/oct/14/gene-simmons-anonymous-attack-filesharing
Charged With:	Conspiracy and unauthorized impairment of a protected computer
Legislative Provisions:	18 USC 371: Conspiracy; 18 USC 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I): Unauthorized impairment of a protected computer
Typology:	
Main Target:	Gene Simmons via his website
Motivation:	Likely to be protest or retribution as it occurred shortly after Gene Simmons criticised file sharing encouraged copyright owners to commence litigation and seek extensive damages against file sharers. (See Guardian article for screenshot of Anonymous message about Gene Simmons' views).
Convicted Of:	
Sentence:	If convicted of both counts, up to 15 years in federal prison
Additional Important Information:	

Member of LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems

"A member of the LulzSec hacking group was arrested … for his role in an extensive computer attack against the computer systems of Sony Pictures Entertainment. … On September 2, 2011, a federal grand jury returned an indictment filed under seal in U.S. District Court in Los Angeles charging Kretsinger with conspiracy and the unauthorized impairment of a protected computer." [1st and 2nd paras]

ITEM	NOTES
CaseName:	
Citation:	Public Affairs Specialist Laura Eimiller, 'Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems' (FBI Press Release, 22 September 2011).
Jurisdiction:	Los Angeles, U.S. District Court
Main URL:	http://www.fbi.gov/losangeles/press-releases/2011/member-of-hacking-group-LulzSec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems
Charged With:	Conspiracy and the unauthorized impairment of a protected computer (using an SQL injection and a proxy server)
Legislative Provisions:	
Main Target:	Sony Pictures Entertainment's computer systems
Motivation:	
Convicted Of:	
Sentence:	"If convicted, Kretsinger faces a statutory maximum sentence of 15 years in prison." [8th para]
Additional Important Information:	"This case is being prosecuted by the United States Attorney's Office in Los Angeles." [2nd to last para]

Two Men Charged in New Jersey with Hacking AT&T's Servers

"Two self-described Internet "trolls" were arrested … for allegedly hacking AT&T's servers and stealing e-mail addresses and other personal information belonging to approximately 120,000 Apple iPad users who accessed the Internet via AT&T's 3G network" [1st para]. The defendants are alleged to be associates of the group Goatse Security, which according to Wikipedia is a grey-hat hacker group that exposes security flaws. (So in this sense, vaguely "ethical").

ITEM	NOTES
CaseName:	
Citation:	U.S. Attorney's Office, 'Two Men Charged in New Jersey with Hacking AT&T's Servers' (FBI Press Release, 18 January 2011).
Jurisdiction:	Newark, New Jersey
Main URL:	http://www.fbi.gov/newark/press-releases/2011/nk011811.htm
Charged With:	"Each defendant is charged with one count of conspiracy to access a computer without authorization and … fraud in connection with personal information" [14th para]
Legislative Provisions:	
Main Target:	AT&T's servers
Motivation:	unclear
Convicted Of:	Possibly to publicise security faults in AT&T's 3G network, or "criminal gain or prestige among peers in the cyber-hacking world" [5th to last para].
Sentence:	
Additional Important Information:	"Each count with which the defendants are charged carries a maximum potential penalty of five years in prison and a fine of $250,000." [4th to last para].

Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks

"Fourteen individuals were arrested ... on charges related to their alleged involvement in a cyber attack on PayPal's website as part of an action claimed by the group 'Anonymous,'" [1st para]. "In addition ... Arciszewski, 21, was arrested today ... on charges of intentional damage to a protected computer [for] allegedly access[ing] without authorization the Tampa Bay InfraGard website and upload[ing] three files... then tweet[ing] about the intrusion and direct[ing] visitors to a separate website containing links with instructions on how to exploit the Tampa InfraGard website." [8th & 9th paras]

ITEM	NOTES
CaseName:	
Citation:	Office of Public Affairs, 'Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks' (FBI Press Release, 19 July 2011).
Jurisdiction:	San Jose, Northern District of California; Orlando, Middle District of Florida. (New Jersey arrest mentioned in this press release regarding a hack of AT&T's servers is detailed above).
Main URL:	http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks
Charged With:	California charges: conspiracy and intentional damage to a protected computer Florida charges: intentional damage to a protected computer.

Legislative Provisions:	
Main Target:	California: DDoS attacks on Paypal Florida: Tampa Bay InfraGard website (which is sponsored by the FBI).
Motivation:	California: retaliation against Paypal's termination of Wikileaks' donation account Florida: disclosure of security flaws (as the defendant tweeted about the intrusion and posted instructions on how to exploit the flaws)
Convicted Of:	
Sentence:	"The charge of intentional damage to a protected computer carries a maximum penalty of 10 years in prison and a $250,000 fine. Each count of conspiracy carries a maximum penalty of five years in prison and a $250,000 fine." [5th to last para].
Additional Important Information:	

US v. Steiger (2003)

This case concerns a hacker that obtained evidence that the defendant was producing and collecting child pornography, and passed it on to law enforcement in the USA. The issue in this case was whether "the evidence was obtained in violation of the Fourth Amendment as the hacker was a government agent."

ITEM	NOTES
CaseName:	US v. Steiger (2003)
Citation:	318 F. 3d 1039
Jurisdiction:	Court of Appeals 11th circuit
Main URL:	http://scholar.google.com.au/scholar_case?case=5611821785646747519
Charged With:	(hacker not charged as he was not being prosecuted here)
Legislative Provisions:	The Fourth Amendment (right against unreasonable searches and seizures)
Typology:	
Main Target:	Steiger – producer and possesser of CP
Motivation:	To help law enforcement officers catch child predators
Convicted Of:	n/a
Sentence:	
Additional Important Information:	For a search by a private person to implicate the Fourth Amendment, the person must act as an instrument or agent of the government.[98]

US v. Jarrett (2003)

This case concerns a hacker that obtained evidence that the defendant was producing and collecting child pornography, and passed it on to law enforcement in the USA. The issue in this case was "whether evidence obtained by a hacker and used in a prosecution implicates the 4th amendment, and there has been communication between the hacker and law enforcement about the evidence".

[98] *United States v. Ford*, 765 F.2d 1088, 1090 (11th Cir.1985).

ITEM	NOTES
CaseName:	US v. Jarrett
Citation:	338 F. 3d 339
Jurisdiction:	Court of Appeals 4th circuit
Main URL:	http://scholar.google.com.au/scholar_case?case=7704360326371177621
Charged With:	(hacker not charged as he was not being prosecuted here)
Legislative Provisions:	The Fourth Amendment (right against unreasonable searches and seizures)
Typology:	
Main Target:	Steiger – producer and possesser of CP
Motivation:	To help law enforcement officers catch child predators
Convicted Of:	n/a
Sentence:	
Additional Important Information:	Whether the hacker's search was a Government search turns on "(1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation" [344]. There must be more than knowledge or acquiescence – there must be participation or affirmative encouragement.

United Kingdom

ITEM	NOTES
CaseName:	
Citation:	John E Dunn, 'Alleged LulzSec Hacker 'Kayla' Arrested By UK Police' *csoonline.com* 2 September 2011
Jurisdiction:	UK
Main URL:	<http://www.csoonline.com/article/689060/alleged-LulzSec-hacker-kayla-arrested-by-uk-police> at 10 November 2011.
Charged With:	Implied to be offenses under Computer Misuse Act (1990) (with which others arrested in similar circumstances were charged).
Legislative Provisions:	
Main Target:	"The arrests relate to our inquiries into a series of serious computer intrusions and online denial-of-service attacks recently suffered by a number of multi-national companies, public institutions and government and law enforcement agencies in Great Britain and the US," [4th para]
Motivation:	
Convicted Of:	
Sentence:	
Additional Important Information:	

British teenager charged over cyber attack on CIA as pirate group takes revenge on 'snitches who framed him'

The defendant was arrested and charged with offenses under the Computer Misuse Act 1990 in relation to a denial of service attack on the website of the Serious Organized Crime Agency.

ITEM	NOTES
CaseName:	
Citation:	Rebecca Camber, Colin Fernandez & Lucy Collins, 'British teenager charged over cyber attack on CIA as pirate group takes revenge on 'snitches who framed him" *dailymail.co.uk* 22 June 2011
Jurisdiction:	UK
Main URL:	http://www.dailymail.co.uk/sciencetech/article-2006118/Ryan-Cleary-charged-cyber-attack-CIA-LulzSec-takes-revenge.html
Charged With:	Five offences under the Computer Misuse Act
Legislative Provisions:	
Typology:	
Main Target:	Britain's Serious Organized Crime Agency website
Motivation:	
Convicted Of:	
Sentence:	
Additional Important Information:	

Australia

Matthew George, Anonymous member charged in NSW

Matthew George was an Australian member of Anonymous who participated in "Operation Titstorm". He was charged with inciting others to attack government websites and the Magistrate likened his activities to cyber-terrorism.

ITEM	NOTES
CaseName:	
Citation:	Sarah Whyte, 'Meet the hacktivism who tried to take down the government' (March 14, 2011) *smh.com.au* <http://www.smh.com.au/technology/security/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html> at 7 November 2011.
Jurisdiction:	Newcastle Local Court
Main URL:	http://www.smh.com.au/technology/security/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html
Charged With:	Inciting others to attack government websites
Legislative Provisions:	
Main Target:	Denial of service attack against the websites of the Prime Minister and Steven Conroy, in order to protest the Internet Censorship Bill and the presence of certain URLs on the proposed blacklist
Motivation:	
Convicted Of:	
Sentence:	$550 fine
Additional Important	

Information:	

Israel

Anat Kam

The defendant secretly copied thousands of classified (many confidential) military files during her military service, which she leaked.

ITEM	NOTES
CaseName:	State of Israel vs Anat Kam
Citation:	
Jurisdiction:	Israel – Tel Aviv District Court
Main URL:	http://en.wikipedia.org/wiki/Anat_Kamm-Uri_Blau_affair http://www.maannews.net/eng/ViewDetails.aspx?ID=275114 http://www.ynetnews.com/Ext/Comp/ArticleLayout/CdaArticlePrintPreview/1,2506,L-4141015,00.html
Charged With:	Severe espionage
Legislative Provisions:	
Typology:	
Main Target:	Israel Defence Forces
Motivation:	
Convicted Of:	Leaking classified materials
Sentence:	4.5 years imprisonment (from a maximum of 15 years), and 18 months probation
Additional Important Information:	

14. Appendix B – Ethical Hacking Time-Line Chart of Recent Activity (2011)

.....

1. Anonymous - OpIndependencia

Target	Mexico Government
Date:	15th September 2011
Source:	Comlay, E 15/9/2011, "Hackers target mexico government websites", Reuters: http://www.reuters.com/article/2011/09/15/us-mexico-hackers-idUSTRE78E7AC20110915 , "Operation OpIndependencia: Anonymous hit Mexican government official websites", The Hacker News 16/9/2011: http://thehackernews.com/2011/09/operation-opindependencia-anonymous-hit.html
Motivation:	None given
Type of Attack:	DDoS
Any other groups claiming responsibility:	No.
Damage Caused	Government websites offline for a number of hours.
Additional Important Information:	

2. Anonymous - New York Stock Exchange

Target	New York Stock Exchange - http://www.nyse.com/
Date:	4th-10th October 2011
Source:	Grant, D 10/10/2011, "NYSE Hacked! Is The Anonymous Infrastructure Crumbling?", New York Observer: http://www.observer.com/2011/10/nyse-remains-unhacked-is-the-anonymous-infrastructure-crumbling-video/ , Chiaramonte, P & Winter, J 4/10/2011, "Hacker Group Anonymous Threatens to Attack Stock Exchange", Fox News: http://www.foxnews.com/scitech/2011/10/04/hacker-group-anonymous-threatens-to-attack-stock-exchange/
Motivation:	Occupy wall street protest
Type of Attack:	DDoS
Any other groups claiming responsibility:	No
Damage Caused	New york stock exchange off line for 2 minutes – no trading
Additional	Conflicting information over whether the attack was successful or whether it

Important Information:	occurred at all.

3. Anonymous - OpCartel

Target	Alleged associates of Los Zetas drug cartel in Mexico – corrupt law enforcement, those involved in managing and participating in operations.
Date:	5th November 2011
Source:	**Mandell, N 31/10/11, "Anonymous hacker group threatens Mexican drug cartel Zetas in online video", New York Daily News: http://www.nydailynews.com/news/world/anonymous-hacker-group-threatens-mexican-drug-cartel-zetas-online-video-article-1.969859#ixzz1d4sAfvE6 , CBS news, CNET, SlashDot, Anonymous website, various others.**
Motivation:	Retaliation for alleged kidnapping of an anonymous activist. General threat posed by criminal organizations.
Type of Attack:	DDoS attack. Unauthorized access to communications. Threatens release of personal information of others involved in cartel operations.
Any other groups claiming responsibility:	No
Damage Caused	If information is released (or even if not released), more likely to pose a threat to Anonymous members depending on the nature and importance the cartel places on the information. Likely to retaliate on basis of increased publicity alone.
Additional Important Information:	• Current reports indicate conflicting rumours whether "Opcartel" will go ahead. Little belief that Anonymous has the ability to do any kind of damage. • Interesting note – "Anonymous likely won't be able to turn up more information than the U.S. government already has, but they are able to publicize more information than the U.S. government can." - Dispatch: Anonymous' Online Tactics Against Mexican Cartels | STRATFOR • UPDATE – No attack occurred. Pastebin - http://pastebin.com/XZRpjUZq , still confusion over whether any aspects of this crusade are actually truthful.

5. Anonymous – Operation Darknet

Target	Those in possession of child pornography and CP websites on the darknet
Date:	3rd November 2011
Source:	Liebowitz, M 3/11/2011, "Anonymous releases IP addresses of alleged child porn viewers", MSN Today: http://today.msnbc.msn.com/id/45147364/ns/today-today_tech/t/anonymous-releases-ip-addresses-alleged-child-porn-viewers/ , "Anonymous busts Internet pedophiles", RT: http://rt.com/usa/news/anonymous-child-tor-porn-513/ , "Hacktivist group

	shuts down child porn sites", Canoe Technology: http://technology.canoe.ca/2011/10/24/18871656.html
Motivation:	Expose those who are 'ruining Tor for the majority of legitimite users'. Lay ground work for investigations.
Type of Attack:	Spyware, brute force attack, Social engineering – phishing, Release of identifying information of active CP site visitors and those in possession of CP, unauthorised access.
Any other groups claiming responsibility:	No
Damage Caused	No reported damage as of yet. Reputational damage to those identifiable, however, it is up to law enforcement to validate alleged paedophiles.
Additional Important Information:	• Claims that the add-on was created with Mozilla's permission, seemingly unsubstantiated. • No differentiation between those who merely have CP on their computer, whether this is known to users.

6. Anonymous - BART

Target	San Francisco's Bay Area Rapid Transit (BART)
Date:	August 15th 2011
Source:	"BART drafts new policy on disruption of cellphone service", LA Times: http://latimesblogs.latimes.com/lanow/2011/10/bart-outlines-cell-phone-service-disruption-policy.html , Limer, E 15/8/2011, "Anonymous follows through on BART hack, organises protest", Geekosystems: http://www.geekosystem.com/anon-hacks-bart/ , Jardin, X 14/8/2011, "Anonymous hacks BART after wireless shutdown; protests planned for Monday", BoingBoing: http://boingboing.net/2011/08/14/anonymous-hacks-bart-after-wireless-shutdown-protests-planned-for-monday.html
Motivation:	Perceived breach of 1st amendment rights – restricting freedom of speech by disabling telecommunications services.
Type of Attack:	Unauthorised access, modification of data, website defaced, release of personal information.
Any other groups claiming responsibility:	no
Damage Caused	Defaced myBART website, leaked info on myBART user database which also included non-BART employees. Also 'assured' non-BART employees that "the only information that will be abused from this database is that of BART employees."
Additional Important Information:	• Undifferentiated/disorganized release of information. Though they claimed only BART employees would be abused would, it uses this as a blanket term and makes no distinction between those who may or may not have even been involved in the phone disruption. • Circumstances would include "destruction of district property" – needs much more clarification as almost anything can be twisted to fit such criteria.

7. Anonymous / TeaMp0isoN

Target	Oakland city police
Date:	October 28th
Source:	Fogarty, K 28/10/2011, "Hackers come out of shadows to attack police, support Occupy protests", IT world: http://www.itworld.com/security/217561/hackers-come-out-shadows-attack-police-support-occupy-protests
Motivation:	Retaliation against police injuring a protester.
Type of Attack:	DDoS, SQL injection, unauthorised access, modification of data, website defaced, release of personal information.
Any other groups claiming responsibility:	TeaMp0isoN – not really claiming responsibility, just engaging in different aspects of the activity.
Damage Caused	Anonymous – Took main Oakland Police Department website offline for a number of hours, infiltrated Oakland government security server and posted personal information of officers as well as information on the structure of the servers, themselves. TeaMp0isoN - Released a list of police-department web sites that are vulnerable to MSAccess SQL injections along with encouragements to participate.
Additional Important Information:	No indication of collaboration between Anonymous and TeaMp0isoN

8. Anonymous - Operation Rainbow Dark

Target	Document assets connected to Rainbow Medical Associates, Dr. Carlo Musso.
Date:	4th November 2011
Source:	Seltzer, S 22/8/2011, "For-Profit Company Oversaw Davis's Execution, Had Prompted Complaint for Illegal Purchase of Lethal Injection Drugs", Alternet: http://www.alternet.org/newsandviews/article/670237/for-profit_company_oversaw_davis%27s_execution,_had_prompted_complaint_for_illegal_purchase_of_lethal_injection_drugs/ , http://anonnews.org/?p=press&a=item&i=1162
Motivation:	Retaliation for execution of Troy Davis, alleged use of illegally-imported drugs for execution.
Type of Attack:	Possible unauthorised access, modification of data, website defacement, release of personal information.
Any other groups claiming responsibility:	No.
Damage Caused	No such attack seemingly occurred.
Additional Important Information:	• Same post that something will be done pasted into various blogs and anonymous-related sites. • No indication that they followed through or even that claims were valid.

9. Latin Hack Team – Ecuador presidential website

Target	Rafael Correa, Ecuador Government
Date:	June 20 2011
Source:	"Website of the Presidency of Ecuador suffered cyber attacks", ElUniverso: http://www.eluniverso.com/2011/06/20/1/1355/pagina-internet-presidencia-ecuatoriana-sufrio-ataque-informatico.html?p=1354&m=638
Motivation:	Accusations of political corruption
Type of Attack:	DDoS
Any other groups claiming responsibility:	Possibly Anonymous.
Damage Caused	Presidential website out of commission for over 2 hours, elciudadano.com (government e-newspaper) down for an hour.
Additional Important Information:	Conflicting information on the group responsible. Some report that this "Latin Hack Team" is a part of Anonymous.

10. Anonymous - Operation #TMX

Target	Toronto stock exchange
Date:	7th[h] November 2011
Source:	Moretti, S 27/9/2011 http://www.torontosun.com/2011/10/27/video-warns-of-possible-cyber-attack-on-tsx , Errett, J, 7/11/11 http://www.nowtoronto.com/news/webjam.cfm?content=183319
Motivation:	Part of Occupy Movement - destabilising economy, poverty, class oppression, etc.
Type of Attack:	None – Likely DDoS
Any other groups claiming responsibility:	no
Damage Caused	None
Additional Important Information:	No reports of whether any attack has occurred.

11. Chaos Computer Club (Germany)

Target	German government
Date:	Oct 26, 2011
Source:	Wikipedia, CCC website: http://ccc.de/en/updates/2011/staatstrojaner , Leyden, J, 2011 the register: http://www.theregister.co.uk/2011/10/12/bundestrojaner/ , wikileaks: http://wikileaks.org/wiki/Skype_and_the_Bavarian_trojan_in_the_middle

Motivation:	Breach of rights by government and law enforcement, use of Trojan "Bundestrojaner"
Type of Attack:	Release of information, analysis of code. Short critique available at http://web17.webbpro.de/index.php?page=analysis-of-german-bundestrojaner
Any other groups claiming responsibility:	no
Damage Caused	Reputation of government, highlights issues of government-sanctioned malware use beyond the scope of what the courts and laws provide for.
Additional Important Information:	Data encryption is non-existent or ineffective, can be accessed by almost anyone with an internet connection which presents significant privacy issues outside of direct government involvement.

12. Chaos Computer Club

Target	Hamberg bank, Bildschirmtext network
Date:	1985
Source:	**Harrington, J 8/9/11, "Hacktivism: What is the Chaos Computer Club?", Suite101: http://joharrington.suite101.com/hacktivism-what-is-the-chaos-computer-club-a387917 , Wikipedia 2011, "Chaos Computer Club" : http://en.wikipedia.org/wiki/Chaos_Computer_Club**
Motivation:	Protest use of biometric data for personal documents.
Type of Attack:	Unauthorised access, modification of data, theft.
Any other groups claiming responsibility:	no
Damage Caused	134000 DM Donated to their club "from" the bank
Additional Important Information:	• Returned money the next day apparently. • Conflicting information on date of the hack. Some say 1984, others say 1985. Possibly closer to new years 1984 though unconfirmed.

13. Chaos Computer Club

Target	Quicken database
Date:	1996
Source:	Von Leitner, F http://tbtf.com/resource/felix.html , Wikipedia 2011, "Chaos Computer Club" : http://en.wikipedia.org/wiki/Chaos_Computer_Club
Motivation:	Highlight system flaws
Type of Attack:	Data modification, unauthorized access, fraud (kind of. Not for any personal gain as far as I'm aware).
Any other groups claiming responsibility:	No.
Damage Caused	Changed personal data, cloned SIM, wrote ActiveX control which, once executed, turns of internet security.
Additional	Apparently demonstrated this capability on TV.

Important Information:	

14. Chaos Computer Club

Target	German government, Minister of the Interior Wolfgang Schäuble
Date:	2008
Source:	**Ragan, S 1/8/2008, "CCC is at it again – hands out copies of German Interior Minister's fingerprint", The Tech Herald:** http://www.thetechherald.com/article.php/200814/581/CCC-is-at-it-again---hands-out-copies-of-German-Interior-Minister-s-fingerprint
Motivation:	Protest use of biometric data for personal document authentication
Type of Attack:	Not specified whether fingerprint was obtained physically or off a database. Probable unauthorised access involved.
Any other groups claiming responsibility:	no
Damage Caused	Cloned minister of interior's fingerprint and made it widely available. Was able to fool biometric scanners.
Additional Important Information:	Though biometric data is unique to people, databases on which these records are kept are open to compromise.

15. Hacker Union

Target	U.S. Military, and Government servers and sites
Date:	April 2001
Source:	Nazario, J, "Politically Motivated Denial of Service Attacks", *The Virtual Battlefield: Perspectives on Cyber Warefare*, Arbor Networks: http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf , Thomas, TL 2001, 'The Internet in China: Civilian and Military Uses', *Information & Security: An International Journal,* vol. 7, pp. 159-173. Available at: http://fmso.leavenworth.army.mil/documents/china-internet.htm
Motivation:	Retaliation for mid-air collision of a Chinese fighter jet and U.S. spy plane which killed the Chinese pilot
Type of Attack:	DDOS, unauthorised access, modification of data, website defaced, defacement of websites.
Any other groups claiming responsibility:	Not claiming responsibility, but certainly taking part, Hacker Union of China, China Eagle Union.
Damage Caused	• Defaced or crashed 100> websites. Majority were .gov and .com domains. Defacements of U.S. sites included posting pictures of the dead Chinese pilot and anti-U.S. messages. • Similar acts perpetrated by pro-United States hackers on approximately 300 Chinese web sites.

Additional Important Information:	• Some pro-Chinese hackers wiped a number of compromised servers. • Generally considered bad form to do so.

16. Decocidio

Target	European Climate Exchange
Date:	23rd July 2010
Source:	Leyden, J 26/7/2010, "EU climate exchange website hit by green-hat hacker", The Register: http://www.theregister.co.uk/2010/07/26/climate_exchange_website_hack/ , Takver 25/7/2010, "European Climate Exchange website hacked", Independent Media Centre Australia: http://indymedia.org.au/2010/07/24/european-climate-exchange-website-hacked ,
Motivation:	Political protest against carbon credits
Type of Attack:	Unauthorised access, modification of data, website defaced.
Any other groups claiming responsibility:	no
Damage Caused	Site was defaced for a weekend. Highlighted the group's opposition to carbon trading as a means of tackling climate change.
Additional Important Information:	• Superficial solution when it may still be more profitable for a corporation to pay fines for environmental damage than to effectively minimise such damage. • Cited links to Climategate scandal in 2009, sketchy information available. Leaked communications pertaining to manipulation of climate change data by researchers. This was never found to be the work of hackers.

17. German stock exchange

Target	German Stock exchange (or may have actually targeted French rugby team fansite)
Date:	October 2011
Source:	Leyden, J 4/11/11, "Hackers mistake French rugby site for German stock exchange", The Register: http://www.theregister.co.uk/2011/11/04/french_rugby_site_hacktivist_maul/ , Liebowitz, M 4/11/11, "Hackers Target Stock Index, Hit Rugby Team Instead", Security News Daily: http://www.securitynewsdaily.com/hackers-stock-index-rugby-team-1309/
Motivation:	"…appeared to be trying to make an Anti-Wall Street style protest against the German DAX website"
Type of Attack:	DDoS
Any other groups claiming responsibility:	unknown

Damage Caused	Accidently took down French rugby team fan site allezdax.com for 2 weeks.
Additional Important Information:	• Not known who was responsible for the attack. Since no one has come forward, fairly safe assumption that the team website was not the intended target, though not conclusive. • Seemed to have been reported after the website was back up and running. Time of attack could possibly be mid October.

18. CabinCr3w

Target	Citigroup CEO, Vikram Pandit
Date:	October 18th 2011
Source:	Couts A 18/8/2011, "Hackers leak Citigroup CEO's personal data after Occupy Wall Street arrests", Digital Trends: http://www.digitaltrends.com/computing/hackers-leak-citigroup-ceos-personal-data-after-occupy-wall-street-arrests/ ,
Motivation:	Apparently to protest arrests of protesters in a Citibank bank
Type of Attack:	Unauthorised access, release of personal information.
Any other groups claiming responsibility:	No.
Damage Caused	Mobile and office phone numbers, an email address, two home addresses, legal and financial information and information about Pandit's family posted online.
Additional Important Information:	

19. DonR4ul

Target	Brazilian presidency blog
Date:	13th October 2011
Source:	Xinhua 14/10/2011, "Brazilian presidency's blog hacked in protest of corruption", ChainDaily: http://www.chinadaily.com.cn/xinhua/2011-10-14/content_4060557.html
Motivation:	Corruption in government departments; high fuel prices.
Type of Attack:	Unauthorised access, modification of data, website defaced.
Any other groups claiming responsibility:	No groups. Alleged to be the work of one hacker – "@DonR4UL".
Damage Caused	Defaced blog website for a number of hours.
Additional Important Information:	

20. TurkguvenLigi

Target	NetNames (DNS Registrar)
Date:	4th September 2009
Source:	**Kirk, J 5/9/2011, "Turkish Hackers Strike Websites with DNS Hack", PCWorld: http://www.pcworld.com/article/239501/turkish_hackers_strike_websites_with_dns_hack.ht , http://www.zone-h.org/**
Motivation:	Unknown
Type of Attack:	SQL injection, unauthorised access, modification of data, website defaced.
Any other groups claiming responsibility:	No.
Damage Caused	Affected many websites including ups.com, vodafone.com, theregister.co.uk, acer.com, betfair.com, nationalgeographic.com and telegraph.co.uk. Damage presumably lasted for different periods of time, depending on the site.
Additional Important Information:	• Unclear whether this was perpetrated with devious intent; to highlight system flaws; or just for laughs. • A message on the redirect page read: "4 Sept. We Turkguvenligi declare this day as World Hackers Day - Have fun ;) h4ck y0u."

21. Anonymous

Target	Israel government, security services websites
Date:	5/11/11
Source:	**Pfeffer, A, Yaron, O 6/11/11, "Israel government, security services websites down in suspected cyber-attack", Haarettz.com: http://www.haaretz.com/news/diplomacy-defense/israel-government-security-services-websites-down-in-suspected-cyber-attack-1.394042**
Motivation:	Retaliation for intercepted Gaza flotilla
Type of Attack:	DDoS.
Any other groups claiming responsibility:	No.
Damage Caused	Websites offline for an unspecified amount of time including that of the Israel Defence Force (IDF), Mossad and the Shin Bet security services, in addition to a number of government portals and ministries.
Additional Important Information:	

22. Unknown

Target	Hong Kong Stock Exchange: hkexnews.hk
Date:	10th August 2011
Source:	**Wisniewski, C 10/8/11, "Hong Kong stock exchange (HKEx) website**

	hacked, impacts trades", Naked Security: http://nakedsecurity.sophos.com/2011/08/10/hong-kong-stock-exchange-hkex-website-hacked-impacts-trades/ , Wisniewski, C 12/8/11, "Hong Kong stock exchange attacked for second day in a row", Naked Security: http://nakedsecurity.sophos.com/2011/08/12/hong-kong-stock-exchange-attacked-for-second-day-in-a-row/
Motivation:	Possibly to accompany occupy movements
Type of Attack:	DDoS
Any other groups claiming responsibility:	unknown
Damage Caused	Unspecified
Additional Important Information:	Scattered information available. Possibly perpetrated by Anonymous though since

23. TeaMp0isoN

Target	Foreign Governments; includes armynet.mod.uk and aph.gov.au
Date:	7th November 2011
Source:	7/11/2011, International Foreign Government E-Mails Hacked by TeaMp0isoN", The Hacker News: http://thehackernews.com/2011/11/international-foreign-government-e.html
Motivation:	Generic dislike of government
Type of Attack:	Unauthorised access, release of data
Any other groups claiming responsibility:	no
Damage Caused	Relased personal information/email username/passwords of over 200 government officials
Additional Important Information:	

24. Iranian Cyber Army

Target	Twitter
Date:	17th December 2009
Source:	"Who are the 'Iranian Cyber Army'", The Green Voice of Freedom: http://en.irangreenvoice.com/article/2010/feb/19/1236
Motivation:	Appears to be retaliation for Iranian embargo.
Type of Attack:	Unauthorised access, modification of data, re-directing communications, website defacement.

Any other groups claiming responsibility:	
Damage Caused	• Twitter and many sub-domains inaccessible for an unspecified period of time. • DNS redirection means that the site itself may not have been defaced, just that users were being sent to the wrong page
Additional Important Information:	

25. Iranian Cyber Army

Target	Baidu
Date:	11th January 2010
Source:	**12/1/2010, "Baidu hacked by 'Iranian cyber army'", BBC News: http://news.bbc.co.uk/2/hi/8453718.stm , "Who are the 'Iranian Cyber Army'", The Green Voice of Freedom: http://en.irangreenvoice.com/article/2010/feb/19/1236**
Motivation:	Protesting Democracy
Type of Attack:	DNS cache poisoning, unauthorised access, modification of data, re-directing communications, website defacement.
Any other groups claiming responsibility:	
Damage Caused	Site inaccessible for approximately 4 hours.
Additional Important Information:	Unknown whether DNS records or the site itself was compromised.

26. Iranian Cyber Army

Target	Voice of America and related sites
Date:	22/2/2011
Source:	**Ragan S, 22/2/2011, "Iranian Cyber Army defaces Voice of America and 93 other domains (Update)", The Tech Herald: http://www.thetechherald.com/article.php/201108/6849/Iranian-Cyber-Army-defaces-Voice-of-America-and-93-other-domains**
Motivation:	Protest American interference with Islamic countries
Type of Attack:	DNS cache poisoning, unauthorised access, modification of data, re-directing communications, website defacement.
Any other groups claiming responsibility:	
Damage Caused	Re-directed Voice of America home site to one with a protest message. Claim

	to have hit 90> others with the same attack (most of them VOA-related). Sites inaccessible for an unspecified period of time
Additional Important Information:	

27. Iranian Cyber Army

Target	Tech Crunch
Date:	**26/1/2010**
Source:	**"TechCrunch Hacked? (yes,Techcrunch got hacked)** " TechnoFriends 26/1/2010http://technofriends.in/2010/01/26/did-techcrunch-got-hacked/ Kirk, J 25/8/2010, "Iranian Cyber Army Moves Into Botnets", PCWorld: http://www.pcworld.com/businesscenter/article/208670/iranian_cyber_army_moves_into_botnets.html
Motivation:	Unknown/unspecified
Type of Attack:	DNS cache poisoning? Social engineering? DoS?
Any other groups claiming responsibility:	
Damage Caused	"…installed a page on TechCrunch's site that redirected visitors to a server that bombarded their PCs with exploits in an attempt to install malicious software." – PCWorld
Additional Important Information:	

28. N33

Target	Hugo Chavez opponents
Date:	1st September 2011
Source:	**Sanchex, F 27/9/2011, "Hackers hijack Twitter accounts of Chavez critics", MSNBC: http://www.msnbc.msn.com/id/44689342/ns/technology_and_science-security/t/hackers-hijack-twitter-accounts-chavez-critics/**
Motivation:	Political opposition, "improper use of twitter"
Type of Attack:	Phishing, unauthorised access, modification of data.
Any other groups claiming responsibility:	no
Damage Caused	Hacked the twitter accounts of a number of political opponents, reputational damage, release of personal information/communications/photos.
Additional	

Important Information:	

29. Anonymous

Target	Mastercard
Date:	28th June 2011
Source:	**Bergen, J 28/6/2011, "Anonymous hacktivists take down MasterCard.com again in support of WikiLeaks", Geek: http://www.geek.com/articles/news/anonymous-hacktivists-take-down-mastercard-com-again-in-support-of-wikileaks-20110628/ , "Second WikiLeaks payback vs. MasterCard: LulzSec or Anonymous?", International Business Times: http://au.ibtimes.com/articles/170985/20110629/mastercard-citibank-LulzSec-anonymous-wikileaks-hack-hactivism.htm**
Motivation:	Blocking donations to WikiLeaks
Type of Attack:	DDoS
Any other groups claiming responsibility:	LulzSec – alluded to in reports, not formally claimed.
Damage Caused	Reported that the site was down for 2 hours.
Additional Important Information:	

30. Anonymous

Target	PayPal
Date:	6-9th December 2010
Source:	Leyden, J 6/12/2010, 20/7/2011, "Anonymous attacks PayPal in 'Operation Avenge Assange'", The Register: http://www.theregister.co.uk/2010/12/06/anonymous_launches_pro_wikileaks_campaign/ "FBI Cracks Down on 'Anonymous' Over PayPal Hacking, Arrests 14", International Business Times: **http://www.ibtimes.com/articles/183495/20110720/federal-bureau-of-investigation-fbi-paypal-online-security-anonymous-hacking-cyber-attack-wikileaks.htm**
Motivation:	Operation Avenge Assange – Retaliation for blocking WikiLeaks donations
Type of Attack:	DDoS
Any other groups claiming responsibility:	no
Damage Caused	Reported that the attack lasted about 8 hours and resulted in numerous disruptions. There was no substantial clarification in what these disruptions entailed.

Additional Important Information:	14 alleged members of anonymous charged for intentional damage to protected computers, which carries a maximum penalty of 10 years (5 for conspiracy) imprisonment and a $250000 fine.

31. Anonymous

Target	Sony
Date:	4th April 2011
Source:	Mick, J 4/4/2011, "Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit", Daily Tech: http://www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm 20/7/2011, "FBI Cracks Down on 'Anonymous' Over PayPal Hacking, Arrests 14", International Business Times: **http://www.ibtimes.com/articles/183495/20110720/federal-bureau-of-investigation-fbi-paypal-online-security-anonymous-hacking-cyber-attack-wikileaks.htm**
Motivation:	Retaliation for Sony taking legal action against George Hotz, a coder who wrote a tool that "allows *homebrew* software to run on the PlayStation 3 (PS3)." The tool allows for the use of 3rd party software on the consoles.
Type of Attack:	DDoS, data theft, unauthorised access.
Any other groups claiming responsibility:	LulzSec
Damage Caused	PS3 online capabilities were disrupted for almost a month.
Additional Important Information:	Compromised personal data of 77 million users worldwide and considered the largest breach of its kind to date.

32. LulzSec

Target	Sony BMG - Greece
Date:	22nd May 2011
Source:	Wisniewski, C 22/5/2011, "Sony BMG Greece the latest hacked Sony site", Naked Security: http://nakedsecurity.sophos.com/2011/05/22/sony-bmg-greece-the-latest-hacked-sony-site/ **Mills, E 6/6/2011, "Hackers taunt Sony with more data leaks, hacks", CNET: http://news.cnet.com/8301-27080_3-20069443-245/hackers-taunt-sony-with-more-data-leaks-hacks/**
Motivation:	
Type of Attack:	SQL injection, unauthorised access, data leak
Any other groups claiming responsibility:	
Damage Caused	Release of "usernames, real names and email addresses of users registered on SonyMusic.gr." Release of internal network map
Additional Important Information:	Large quantity of information reported to be incorrect.

33. Anonymous

Target	Mastercard, Visa, Swedish prosecutor's office, Sara Palin website
Date:	8-9th December 2010
Source:	9/12/2010, "'Anonymous' hackers hit Visa, Mastercard and Sarah Palin in WikiLeaks revenge", The Australian: http://www.theaustralian.com.au/in-depth/wikileaks/anonymous-hackers-hit-visa-mastercard-in-wikileaks-revenge/story-fn775xjq-1225968083650
Motivation:	Retaliation for blocking funding to WikiLeaks – Operation Payback; also for open opposition to Julian Assange.
Type of Attack:	DDoS
Any other groups claiming responsibility:	no
Damage Caused	• Mastercard's main site was down for 7 hours on the 8th. • Visa's site was down for 2> hours on the 9th. • Sara Palin's site was down for 6 minutes; additionally, her and her husband's bank accounts were disrupted. • Swedish prosecutor's office website was taken offline for an unspecified period of time.
Additional Important	"Icelandic firm DataCell said it would sue Visa for blocking payments to WikiLeaks and accused the credit card giant of bowing to political pressure."

Information:	

34. LulzSec

Target	Infragard (Atlanta) – FBI affiliate
Date:	3rd June 2011
Source:	**Beschizza, R 3/6/2011, "LulzSec claims FBI affiliate hacked, users and botnet are exposed", Boing Boing: http://boingboing.net/2011/06/03/LulzSec-claims-fbi-a.html**
Motivation:	
Type of Attack:	Unauthorised access, data leak, modification of data, defacement.
Any other groups claiming responsibility:	No
Damage Caused	Released personal information on the user database of 180 users, defaced http://infragardatlanta.org/, reputational damage – who do you believe?
Additional Important Information:	

35. LulzSec

Target	PBS
Date:	29-30th May 2011
Source:	**Wisniewski, C 30/5/2011, "PBS.org hacked... LulzSec targets Sesame Street?", Naked Security: http://nakedsecurity.sophos.com/2011/05/30/pbs-org-hacked-LulzSec-targets-sesame-street/** Ragan, S 30/5/2011, "PBS: LulzSec attack an attempt to chill journalism", The Tech Herald: http://www.thetechherald.com/article.php/201122/7215/PBS-LulzSec-attack-an-attempt-to-chill-journalism
Motivation:	"took offense to the portrayal of Bradley Manning in a segment on PBS's Frontline news magazine program"; Anti-WikiLeaks protests
Type of Attack:	"They claim they used a zero day exploit in Movable Type 4 and were able to compromise Linux servers running outdated kernels."
Any other groups claiming responsibility:	no
Damage Caused	Released login credentials of database administrators/users as well as those of affiliates; defaced/injected their own website
Additional Important Information:	

36. LulzSec

Target	CIA www.cia.gov
Date:	15th June 2011
Source:	15/6/2011, "LulzSec's CIA hack just one of many high-profile hackings", International Business Times: http://www.ibtimes.com/articles/163678/20110615/google-LulzSec-s-cia-hack-just-one-of-many-high-profile-hackings.htm **Schroeder, S 16/6/2011, "LulzSec Hackers Take Down CIA Website", Mashable: http://mashable.com/2011/06/16/LulzSec-hackers-cia/**
Motivation:	Unspecified
Type of Attack:	DDoS
Any other groups claiming responsibility:	no
Damage Caused	CIA website was inaccessible for an unspecified period of time, though reported as "several hours".
Additional Important Information:	

37. LulzSec

Target	Lockheed Martin
Date:	May 2011
Source:	**http://www.prnewswire.com/news-releases/LulzSec-and-anonymous-blur-lines-between-hacktivism-and-criminality-according-to-pandalabs-q2-report-125068654.html** **http://news.sky.com/home/technology/article/16099978**
Motivation:	Unknown
Type of Attack:	Unauthorised access,
Any other groups claiming responsibility:	
Damage Caused	Claims that no crucial data had been taken, though that "internal systems took a few days to fully recover"
Additional Important Information:	"Shortly after the breach, the UK government announced the formation of the National Cyber Security Programme, a special unit of the Ministry of Defence tasked with reducing the UK's vulnerability to cyber crime and attacks."

38. Unknown, but reported to be either LulzSec or Anonymous

Target	CitiBank
Date:	9th June 2011
Source:	**Cout, A 9/6/2011, "Citibank hacked, more than 200,000 bank customers**

	at risk", Digital Trends: http://www.digitaltrends.com/computing/citibank-hacked-more-than-200000-bank-customers-at-risk/
Motivation:	Unknown
Type of Attack:	Unauthorised access, data theft, data leak
Any other groups claiming responsibility:	
Damage Caused	Compromised information on names, account numbers and contact info of approximately 21 million accounts.
Additional Important Information:	

39. Unknown

Target	Sony Pictures Russia
Date:	6th June 2011
Source:	**Mills, E 6/6/2011, "Hackers taunt Sony with more data leaks, hacks", CNET: http://news.cnet.com/8301-27080_3-20069443-245/hackers-taunt-sony-with-more-data-leaks-hacks/**
Motivation:	Unknown
Type of Attack:	SQL injection
Any other groups claiming responsibility:	No
Damage Caused	Site inaccessible for an unspecified amount of time
Additional Important Information:	

40. The UnderTakers

Target	Sony Music Brazil - sonymusic.com.br
Date:	
Source:	**http://thehackernews.com/2011/06/sony-music-brazil-gets-defaced.html**
Motivation:	Unknown
Type of Attack:	SQL injection, unauthorised access, defacement
Any other groups claiming responsibility:	
Damage Caused	Website down for over 12 hours
Additional Important Information:	

41. Anonymous

Target	Neo-Nazi websites
Date:	8th August 2011
Source:	**11/7/2011, "Anonymous Hackers hack neo-Nazis websites & leak personal info of 16,000 Finns", The Hacker News: http://thehackernews.com/2011/11/anonymous-hackers-hack-neo-nazis.html**
Motivation:	"…apparent desire to shame the Finnish government into improving data security."
Type of Attack:	Unauthorised access, defacement, data leak
Any other groups claiming responsibility:	
Damage Caused	Released user info on 16000 members
Additional Important Information:	

42. 3xp1r3 Cyber Army

Target	Bangladesh Supreme Court official website
Date:	10th November 2011
Source:	**11/11/2011, "Bangladesh Supreme Court website hacked", The Hacker News: http://thehackernews.com/2011/11/bangladesh-supreme-court-website-hacked.html**
Motivation:	Apparently letting admins know that the site was insecure
Type of Attack:	Unauthorised access, defacement
Any other groups claiming responsibility:	
Damage Caused	Website defaced for unspecified period of time. No data leaked or deleted.
Additional Important Information:	

43. Anonymous – Operation Brotherhood Shutdown

Target	Muslim Brotherhood websites
Date:	11th November 2011
Source:	**http://thehackernews.com/2011/11/operation-brotherhood-shutdown-by.html**

Motivation:	
Type of Attack:	
Any other groups claiming responsibility:	
Damage Caused	
Additional Important Information:	

44. Unknown

Website "Kommersant" under prolonged hacker intrusion. As a result of DNS poisoning users visiting the online news website http://www.kommersant.ru/ were redirected to a page. The page consisted of a political cartoon and rhetoric calling for public gathering in St. Petersburg and Moscow to protest the "falsified <corrupt> elections". The CEO of the publishing company Kommersant commented that the company contacted the law enforcement agency.

[redacted]	[redacted]
Case Name:	
Citation:	Sergey Smirnov, 'Website "Kommersant" under prolonged hacker intrusion.' (December 1, 2011) Vedomosti <http://www.vedomosti.ru/tech/news/1440499/kommersant_podvergsya_hakerskomu_dejstviyu_s_vidimostyu > at 2 December 2011.
Jurisdiction:	
Main URL:	http://www.vedomosti.ru/tech/news/1440499/kommersant_podvergsya_hakerskomu_dejstviyu_s_vidimostyu
Charged With:	
Legislative Provisions:	
Typology:	
Main Target:	Attack on the news website of a publishing company "Kommersant". DNS poisoning redirecting users to a webpage calling for public gathering against "falsified elections" - upcoming legislative elections. The company contacted law enforcement agency.
Motivation:	Political
Convicted of:	
Sentence:	
Additional Important Information:	

45. The Man From Leningrad

The official website of the soccer club "Zenit" hacked by foul-mouthed hackers.

A Person calling himself "a man from Leningrad" gained access to the official website of "Zenit" soccer club and posted insults towards the governor of St. Petersburg Valentina Matvienko and the speaker of the Legislative Assembly Vadim Tulipov. The text of the page suggested citizens take their ballots home to "prevent them from stealing your … choice" (appears to be for local city elections). Management of the soccer club contacted Russian law enforcement knows as "Division K". (http://kguvd.ru/ essentially the subdivision of Russia's criminal police branch dealing with cyber crime).

Case Name:	
Citation:	'The official website of the soccer club "Zenit" hacked by foul-mouthed hackers.' (April 6, 2011) Newsru (http://www.newsru.com) <http://www.newsru.com/sport/06apr2011/zenit.html > at 4 December 2011.
Jurisdiction:	
Main URL:	http://www.newsru.com/sport/06apr2011/zenit.html
Charged With:	
Legislative Provisions:	
Typology:	
Main Target:	Website of the soccer club "Zenit" was hacked. An unknown person posted insults towards the governor and the speaker of the legislative assembly and suggested voting party other than United Russia or taking their ballots home.
Motivation:	
Convicted of:	
Sentence:	
Additional Important Information:	

46. Unknown

DDoS attack before the elections. A popular blogging platform LiveJournal was under DDoS attacks a week before Russian legislative elections. LiveJournal is a popular platform for political discussions and the attack did not surprise political scientists in Russia. This was not the first time LiveJournal is under attack, although unlike previous attack against the most popular bloggers, current DDoS attack was against the whole platform. During the spring attack of 2011 the journal of a Russian president Medvedev was offline. Medvedev called these attacks "outrageous and illegal" as they annoy the users, who see government behind such attacks. While political scientist are convinced that this attack was politically motivated to deny any last minute campaign outreach before the December legislative elections, IT specialists are more skeptical.

Case Name:	
Citation:	Anastasiya Matveeva 'DDoS attack before the elections' (November 28, 2011) Gazeta.ru (http://gazeta.ru) <http://www.gazeta.ru/news/lastnews/2011/11/28/n_2113590.shtml> at 4 December 2011.
Jurisdiction:	
Main URL:	http://www.gazeta.ru/news/lastnews/2011/11/28/n_2113590.shtml
Charged With:	
Legislative Provisions:	
Typology:	
Main Target:	Popular blogging platform LiveJournal was under a DDoS attack before the legislative elections in Russia. Political scientists are convinced that the motivation behind the attack is political in nature, while IT experts state that there might be different reasons.
Motivation:	political
Convicted of:	
Sentence:	
Additional Important Information:	

47. Chinese Hacktivism

Target	Mengnui
Date:	December 28, 2011
Source:	"Hacktivism Spreads to China? Mengnui Hacked in Protest of 2nd Milk Scandal" http://web2asia.blognhanh.com/2011/12/hacktivism-spreads-to-china-mengniu.html
Motivation:	Apparently letting admins know that the site was insecure
Type of Attack:	Unauthorised access, defacement
Any other groups claiming responsibility:	None
Damage Caused	Website defaced with statements ""Do you have a conscience?" and "this is our national shame."
Additional Important Information:	Mengnui had a second milk scandal where their milk contained high levels of carcinogens.

15. Appendix C – Questionnaire

Question 1: Has there been an erosion of a common hacker ethos or has the ethos merely evolved into many different sets of ethics?

Question 2: In your experience with hackers, does the law offer a deterrent?

Question 3: Based on your experience interviewing hackers, what are their perceptions of the illegality of their activity?

Question 4: What types of hacking activity would you consider "ethical"?

Question 5: Should ethical hacking be exempt from cybercrime provisions, and if so what kinds of ethical hacking?

Question 6: Do you equate some forms of ethical hacking as the electronic equivalent of civil disobedience (sit-ins, protests) and if so, should the current civil disobedience framework apply to the online setting?

Question 7: Is there a need for security research exemption in cybercrime provisions (unauthorised access)?

Question 8: Is there a need for a public interest exemption in cybercrime provisions (unauthorised access)?

Question 9: Is there any advice in general that you wish to impart to those engaged in ethical hacking?

Question 10: Is there any advice in general that you wish to impart to governments and organisations in dealing with ethical hacking?

16. References

Legislation and Treaties

Convention to the *International Covenant on Civil and Political Rights*, 999 UNTS 302 (1967).

Council of Europe Convention on Cybercrime, 22296 UNTS 167 (2001).

Criminal Code 1995 (Cth).

Model Criminal Code (January 2001).

Caselaw

Bank Julius Baer & Co. Ltd. v. WikiLeaks (2008) U.S. Dist. LEXIS 14758 United States District Court for the Northern District of California

e360 INSIGHT and David Linhardt v. The Spamhaus Project, United States Court of Appeals for the Seventh Circuit, 500 F. 3d 594; 2007 U.S. App. LEXIS 20725.

E360 Insight, LLC et al v. The Spamhaus Project, US District Court, Northern District of Illinois, 13 September 2006 (Case no. 06 C 3958). Access to default judgment at http://www.spamhaus.org/archive/legal/Kocoras_order_to_Spamhaus.pdf..

Glaria (Gator) v Internet Advertising Bureau.

In re § 2703(d) Order, 2011 U.S. Dist. LEXIS 25322.

McAuliffe v The Queen [1995] 183 CLR 108.

McCabe v British American Tobacco Services Limited [2002] VSC 73.

Microsoft Corporation v. John Does 1027 (Feb. 22, 2010) United States District Court for the State of Victoria, Civil Action 1:10 cv 156 (LMB/JFA).

Microsoft Corporation v Newport Interenet Marketing Corporation Does 2-20 King County Superior Court Seattle, Washington (2005) No. 03-2-12648-9 SEA. A copy of these court records may be found at http://4431647708582819520-a-1802744773732722657-s-sites.googlegroups.com/site/sjwest01/court.html?attachauth=ANoY7cr1KKGuLVCCDxAl6bNx-v95BNUiKBf2bIcFSmkkVrd-AaSbI221syEjJVdydf8eJc2TGS1VS08Y5HgucrxNIXJ-plhp65AsGtlaDrCOKfE_SLPwADmGmrJnDpt28IIOgiEVoNi0tUoo-wDWpetUHTYvZvnsIJQxRqQcRB0wUisYBRS0pUcJw07tH2zQgxbdntG3qy3a&attredirects=1 (last accessed October 26, 2010).

Paracha v. Obama (2011) U.S. Dist. LEXIS 46104 United States District Court for the District of Columbia

Regan Gerard Gilmour v Director of Public Prosecutions (Commonwealth) [1996] NSWSC 55.

R v. Caffrey (2006).

R v Stevens [1999] NSWCCA 69.

R. *v. Walker*, HC HAM CRI2008-0750711 [2008] NZHC 1114.

Salter v DPP [2008] NSWSC 1325.

Sierra Corporate Design Inc. v. David Ritz, (2007) District Court, County of Cass, State of North Dakota, File No. op-05-C-01660 *See* www.spamsuite.com.com/node/351.

Specht v. Netscape Communications Corp., 306 F. 3d 17 - Court of Appeals, 2nd Circuit 2002.

State of Israel vs Anat Kam (2011) (Israel – Tel Aviv District Court).

United States Army v. Bradley Manning

United States v Gorshkov (2001) WL 1024026 (Western District Washington).

United States v. Jarrett (2003) 338 F. 3d 339 (Court of Appeals 4th Circuit).

United States v Kevin George Poe (2011) CR 11 01166 (US District Court for the Central District of California)

United States v. Steiger (2003) 318 F. 3d 1039 (Court of Appeals 11th Circuit).

Zitierung: BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (

Books

The Oxford Pocket Dictionary of Current English (2009).

AITCHISON, R., "DNS Records" in *Pro DNS and BIND* (Apress Publishers, 2003).

ANDERSON, R., *Security Engineering: A Guide to Building Dependable Distributed Systems* 2nd ed (Indianapolis: Wiley Publishing, 2008).

ATHANASOPOULOS, E., ANAGNOSTAKIS, K., and MARKATOS, E., "Misusing Unstructured P2P Systems to Perform DoS attacks: The Network that Never Forgets" (2006) Lecture Notes in Computer Science for *Applied Cryptography and Network Security* (Springer Berlin) available at http://www.springerlink.com/content/xk82663475474857/.

ATKIN, T.. et al., *Information Security Management Handbook* (CRC Press, 2006).

BARLOW, J.P. "Crime and Puzzlement" Appendix 1 in LUDLOW, P. (ed) *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (MIT Press, 1996).

BARTON, P. And YEGNESWARAN, V., "An Inside Look at Botnets" in SOMESH, J., MAUGHAN, D., SONG, D., and WANG, C. (eds) *Malware Detection* (New York: Springer, 2007).

BENTHAM, J. *Panopticon, i*n Miran Bozovic (ed.), *The Panopticon Writings* (London: Verso, 1995), 29-95.

BLOUNT, S. *Electronic Contracts: Principles for the Common Law* (Australia: Reed International Books, 2009).

BOWREY, K., *Law & Internet Cultures* (Cambridge University Press, 2005).

CHAN, J., GOGGIN, G., and BRUCE, J., "Internet Technologies and Criminal Justice" in Jewkes, Y. and Yar, M., *Handbook of Internet Crime* (Willan Publishing 2010).

CHIESA, R., DUCCI, S., CIAPPI, S., Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking (UNICRI and CRC Press, 2009).

CLAYTON, R. "Failures in a Hybrid Content Blocking System in DANEZIS, G. And MARTIN, D. (eds) *Privacy Enhancing Technologies* (June 30 2005) volume 3856 of LNCS (Springer).

COHEN, F., *A Short Course on Computer Viruses* 2nd ed (Wiley, 1994).

CORONES, S and CLARKE, P. *Consumer Protection and Product Liability Law 3rded* (Thomson Lawbook, 2008).

CURCEREAU, D. *Aspects of Regulating Freedom of Expression on the Internet* (Intersentia, 2006)

DREYFUSS, S. and ASSANGE, J. Underground (Random House Australia, 2011)

DUNHAM, K. and MELNICK, J. *Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet* (CRC Press, 2009) page 132.

FITZGERALD, B., FITZGERALD, A., MIDDLETON, G., LIM, Y. and BEALE, T., *Internet and E-Commerce Law: Technology, Law and Policy* (Thomson 2007).

FLEMING, J., *The Law of Torts 8th ed* (The Law Book Company 1992).

GARFINKEL, S. and SPAFFORD, G. *Practical UNIX & Internet Security*, 2nd Ed (California: O'Reilly, 1996).

GODWIN, M. "Some 'Property' Problems in a Computer Crime Prosecution" in LUDLOW, P. (ed) *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (MIT Press, 1996).

GRABOSKY, P., *Electronic Crime* (Prentice Hall, 2007).

HARRIS, S., HARPER, A., EAGLE, C. and NESS, J. *Grey Hat Hacking: The Ethical Hacker's Handbook* (McGraw Hill 2008).

HIMANEN, P. *The Hacker Ethic: and the Spirit of the Information Age* (Random House, 2001).

KERR, I., and GILBERT, D., "The Role of ISPs in the Investigation of Cybercrime" in MENDINA, T., and BRITZ, J. (eds) *Information Ethics in an Electronic Age: Current Issues in Africa and the World* (McFarland Press, 2004).

LEVY, S. *Hackers: Heroes of the Computer Revolution* (New York: Doubleday, 1984).

LEVY, A. *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (Viking, 2001).

LIBICKI, M. *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge 2007).

LI, Z., LIAO, Q., and STRIEGEL, A., *Botnet Economics: Uncertainty Matters* (Springer 2009).

LUDWIG, M., *The Giant Black Book of Computer Viruses* 2nd ed. (American Eale, 1998).

LYNCH, A., and WILLIAMS, G., *What Price Security?* (UNSW Press, 2006).

MALCOM, J. *Multi-Stakeholder Governance andthe Internet Governance Forum* (Terminum Press 2008).

MAURUSHAT, A. 2011. "Australia" in *Freedom on the Internet: A Global Assessment of Internet and Digital Media*, Cook S. (ed) (New York: Freedom House, 2011).

MATSWSHYN, A.(ed) *Harboring Data: Information Security, Law, and the Corporation* (Stanford University Press, 2009).

MUELLER, M. *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Massachusetts Institute of Technology, 2002).

ORAM, A. (Ed) *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (O'Reily & Associates: Sebastopol, 2001).

PFLEEGER, C. and PFLEEGER, S. *Security in Computing* 4th Ed. (Prentice Hall, 2006).

PHAIR, N. *Cybercrime: The Reality of the Threat* (self-published 2007).

POULSEN, K., *Kingpin: The True Story of Max Butler, the Master Hacker who Ran a Billion Dollar Cyber Crime Network* (Hachett, 2011).

PROVOS, N. and HOLZ, T., *Virtual Honeypots: From Botnet Tracking to Intrusion Detection* (Safari 2008).

RAYMOND, E. *The Cathedral & the Bizaar: Musings on Linux and Open Source By an Accidental Revolutionary* (O'Reily, 2001).

REYES, A. O'SHEA, K., STEELE, J., HANSEN, J., JEAN, B. and RALPH, T., *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors* (Syngress 2007).

RICE, D., *Geekonomics: The Real Cost of Insecure Software* (Addison-Wesley, 2008).

ROSS, S., *UNIX System Security Tools* (McGraw-Hill, 1999).

SALTZER, J., REED, D. and CLARK, D., "End-to-End Arguments in System Design", in PARTRIDGE, C., ed, *Innovations in Internetworking* (Artech House, 1988).

SAMUELS, A. *Hacktivism and the Future of Political Participation* (PhD Thesis, Harvard, 2004).

SCHILLER, C., BINKLEY, J., HARLEY, D., EVRON, G., BRADLEY, T., WILLEMS, C., and CROSS, M., *Botnets: The Killer Web App* (Syngress 2007).

SCHNEIER, B., *Secrets and Lies* (Robert Ipsen 2000).

SCHILLER, C., BINKLEY, J., HARLEY, D., EVRON, G., BRADLEY, T., WILLEMS, C., and CROSS, M., *Botnets: The Killer Web App* (Syngress 2007).

SINGH, S. The *Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptopgraphy* (Doubleday, 1999).

SMITH, R., GRABOSKY, P., and URBAS, G. *Cyber Criminals on Trial* (Cambridge University Press, 2004).

TAYLOR, P., " Hacktivism: In Search of Lost Ethics?" in *Crime and the Internet* (London & New York: Routledge).

THOREAU, H.D. *Resistance to Civil Government* (original title 1849) but now known as Civil *Disobedience: On the Duty of Civil Disobedience* available at http://www.transcendentalists.com/civil_disobedience.htm

TIEN, L., "Architectural Regulation and the Evolution of Social Norms" in BALKIN, J., GRIMMELMANN, J., KATZ, E., KOZLOVSKI, N., WAGMAN, S., and ZARSKY, T. (eds) *Cybercrime: Digital Cops and Laws in a Networked Environment* (New York University Press, 2006).

WALDEN, I. "Computer Forensics and the Presentation of Evidence in Criminal Cases" in JEWKES, Y. and YAR, M. *Handbook of Internet Crime* (Willan Publishing, 2010).

WALL, D., *Cybercrime: Crime and Society Series* (Polity Press, 2007).

YAR, M., "The Private Policing of Internet Crime" in JEWKES, Y. and YAR, M. (eds) *Handbook of Internet Crime* (Willan Publishing, 2010).

YAR, M., "Public Perception and Public Opinion about Internet Crime" in JEWKES, Y. and YAR, M., *Handbook of Internet Crime* (Willan Publishing 2010), pages 104-120.

YEGNESWARAN, V. And BARFORD, P., "An Inside Look at Botnets" in CHRISTODORESCU, M., JHA, S., MAUGHAN, D., SONG, D. And WANG, C. Eds. *Advances in Information Security: Malware Detection* (2007).

Journal Articles

ANDERSON, K. "Hacktivism and Politically Motivated Computer Crime" (Ensurve 2008) available at http://politicalhacking.blogspot.com.

BAMBAUER, D. and DAY, O., "The Hacker Aegis" (2011) 60 Emory Law Journal.

BRENNER, S. W., CARRIER, B. and HENNINGER, J. "The Trojan Horse Defense in Cybercrime Cases" (2004) 21 *Santa Clara Computer and High Technology Law Journal.*

BRENNER, S.W., *Law in an Era of "Smart" Technology* (2007) 173.

BROADHURST, R., 'Developments in the Global Law Enforcement of Cyber-Crime' (2006) 29(3) *Policing: An International Journal of Police Strategies and Management* 408, page 418.

CHANDLER, J. "Liability for Botnet Attacks" (2006) *Canadian Journal of Law and Technology*

CHANDLER, J. "Security in Cyberspace: Combating Distributed Denial of Service Attacks" (2003-2004) 1 *University of Ottawa Law & Technology Journal* 231.

CHANDLER, J., "Technological Self-Help and Equality in Cyberspace" (2010) 55 *McGill Law Journal.*

CLARKE, R. "Information Technology and Dataveillance" (1988) *Communications of the ACM*, Vol. 31(5), p. 499.

CLARKE, R. and MAURUSHAT, A., "The Feasibility of Consumer Device Security" (2009) *UNSW Law Review Series* 5.

CLARKE, R. and MAURUSHAT, A., "Who Will Bear the Cost of Insecure Devices" (2007) 18 *Journal of Law, Information and Science* 8.

CLAYTON, R. "Complexities in Criminalising Denial of Service Attacks" written for the *Legal Subgroup of the Internet Crime Forum* (Feb. 2006) available at www.cl.ram.ac.uk/~rncl/complexity.pdf (last accessed April 27, 2010).

COHEN, F., "Computer Viruses: Theory and Experiments" (1987) *Computers & Security*, 6(1).

COLANGELO, A. and MAURUSHAT, A., "Exploring the Limits of Computer Code as a Protected Form of Expression: A Suggested Approach to Encryption, Computer Viruses and Technological Protection Measures" (2006) 1 *McGill Law Journal* 51.

DAVIS, N., "Presumed Assent: The Judicial Acceptance of Clickwrap" (2007) 22 *Berkeley Technology Law Journal* 577.

DENNING, D., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" (2001) available at http://www.nautilus.org/infor-policy/workshop/papers/denning.html.

DE VILLIERS, "Distributed Denial of Service: Law, Technology & Policy" (2006) *World Jurist Law/Technology Journal* v. 39 n. 3

DE VILLIERS, "Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare" (2005) 4 *Northwestern Journal of Technology and Intellectual Property* 1

DE VILLIERS, "Reasonable Foreseeability in Information Security Law: A Forensic Analysis" (2008) 30 *Hastings Communications And Entertainment Law Journal.*

DE VILLIERS, M. "Virus Ex Machine Res Ipsa Loquitor" (2003) S*tanford Technology Law Review* 1

EDWARDS, L. "Dawn of the death of Distributed Denial of Service: How to Kill Zombies" (2006) 24 *Cardozo Journal of Arts and Entertainment Law* 23.

EPSTEIN, R., "The Theory and Practice of Self-Help" (2005)1(1) Journal of Law, Economics and Policy 1.

EVRON, G., "Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War," (2008) *Georgetown Journal of International Affairs*, Volume IX, Number 1.

FITRI, N., "Democracy Discourses Through the Internet Communication: Understanding the Hacktivism for the Global Changing" (2011)1 Online Journal of Communication and Media Technologies 2.

GEIST, M., "Is There a There There: Toward Greater Certain for Internet Jurisdiction" (Fall 2001) Berkely Technology Law Journal.

GILBERT, D. And KERR, I. "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" Vol. 51(4) *Criminal Law Quarterly*.

GUZMAN, L., "Unleashing a Cure for the Botnet Zombie Plague" (2010) 59 *Catholic University Law Review* 527.

HAFELE, D., "Three Different Shades of Ethical Hacking: Black, White and Grey" (Feb. 23, 2004) available at http://www.sans.org/reading_room/whitepapers/hackers/shades-ethical-hacking-black-white-grey_1390.

HANCOCK-WHITE, K,. "Ethical Hacking" 2008 available at *casper182.atspace.com/HancockWhite_ethics_paper.doc*

HARDY, K., "Operation Titstorm: Hacktivism or Terrorist Act?" (2010) *University of New South Wales Law Journal* 16:1.

HIMMA, K., "Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?" (2005) ETHICOMP Conference, Linkoping, Sweden.

HUTCHINSON, W. And WARREN, M., "Attitudes of Australian Information System Managers Against Online Attackers" (2001) 9(3) *Information Management & Computer Security* 106.

Imperva, "Hacker Intelligence Initiative" (October 2011) Monthly Trend Report #5.

JOHNSTON, L., "What is Vigilantism?" (1996) *British Journal of Criminology*, vol. 26, No. 2.

JORDAN, T., "Mapping Hacktivism" (2001) 4 Computer Fraud and Security.

KASPERSKY, E., "Cruncher – the First Beneficial Virus?" (1993) *Virus Bulletin*.

KATYAL, N. "Criminal Law in Cyberspace" (2001) 149 *University of Pennsylvania Law Review* 1004.

KERR, O. "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes" (2003) *New York University Law Review*, Vol. 78, No. 53.

KERR, O., "Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability" (2005) 1 *Journal of Law, Economics and Policy* 197.

LESSIG, L., "Reading the Constitution in Cyberspace" (1997) 45 *Emory Law Journal* 1.

LESSIG, L. and RESNICK, P.,"`The Architectures of Mandated Access Controls" available at http://cyber.law.harvard.edu/works/lessig/Tprc98_d.pdf.

LESSIG, L., "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 *Harvard Law Review* 501.

LIN, P., "Anatomy of the Mega-D Takedown" (December, 2009) 12 *Network Security*, pages 4-7.

LUTHER KING, Jr., M., "Letters From a Birmingham Jail" (April 16, 1963) available at The Martin Luther King, Jr. Research and Education Institute http://mlk-kpp01.stanford.edu/index.php/resources/article/annotated_letter_from_birmingham

MAURUSHAT, A. "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in the Era of Obfuscation Crime Tools" (2010) *University of New South Wales Law Journal* 16:1.

MAURUSHAT, A., "Data Breach Notification Law Across the World from California to Australia" (April, 2009) *Privacy Law and Business International.*

MAURUSHAT, A. "Hong Kong Anti-Terrorism Ordinance and the Surveillance Society: Privacy and Free Expression Implications" *Asia Pacific Media Educator*, Vol. 1, Iss. 12/3 (2002).

MAURUSHAT, A. and WATT, R., "Australia's Internet Filtering Proposal in the International Context" (2009) 12(2) *Internet Law Bulletin* 18.

OHM, P. "The Rise and Fall of Invasive ISP Surveillance" available at http://ssrn.com/abstract=1261344 (last accessed April 15, 2009).

OLESON, K. and DARLEY, J., "Community Perceptions of Allowable Counterforce in Self-Defense and Defense of Property"(1999) *Law and Human Behavior*, 23.

POSNER, R., "Killing or Wounding to Protect a Property Interest" (1971) 14 *Journal of Law and Economics* 201.

RYCHLICKI, T. "Legal Issues of Criminal Acts Committed Via Botnets." (2006) *Computer and Telecommunications Law Review* 12(5), p. 163.

ROSE, C., and GORDON, J., "Internet Security and the Tragedy of the Commons" (2003) 1 Journal of Business and Economics Research 11.

SALGADO, R., "The Legal Ramifications of Operating a Honeypot" (2005) *IEEE Magazine Security and Privacy*, vol. 1.

Security Spotlight, "Even Governments are not Immune to Hacktivism" (Feb. 8, 2010).

SHOCK, J. and HUPP, J., "The 'Worm' Programs – Early Experience with a Distributed Computation" (1982) *Communications of the ACM*, 25(3).

SMITH, B., "Hacking, Poaching and Counterattacking: Digital Counterstrikes and the Contours of Self-Help" (2005) 1(1)*Journal of Law, Economics and Policy* 185.

SMITH, H., "Self-help and the Nature of Property" 2005) 1(1)*Journal of Law, Economics and Policy* 69.

SOLOMON, A. and EVRON, G., "The World of Botnets" *Virus Bulletin* September 2008.

SOLOVE, D. "Privacy and Power: Computer Databases and Metaphors for Information Privacy", (2001)53 *Stanford Law Review* 1393.

STEEL, A., "The Meaning of Dishonesty in Theft" (2009) *Common Law World Review*, 38(2).

THOMAS, J., "Ethics of Hacktivism" (2001) SANS Institute InfoSec Reading Room.

US-Cert (United States Computer Emergency Readiness Team), *Quarterly Trends and Analysis Report* (2007) volume 2, Issue 4.

VAN EETEN, M., BAUER, J., ASGHARI, H., TABATABAIE, S., "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data" (2010) *OECD Science, Technology and Industry Working Papers*, 2010/5, OECD Publishing.doi: 10.1787/5km4k7m9n3vj-en

VAUGHN, Z., "Hacktivism: Civil Rights Activism in the Digital Age"

WALDEN, I. And FLANAGAN, A. "Honeypots: A Sticky Legal Landscape?" 29 *Rutgers Communications and Technology Law* 315 (2003).

WARREN, S. and BRANDEIS, L., "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.

WINN, J. "Are 'Better' Security Breach Notification Laws Possible?" (2009) *Berkeley Technology Law Journal* Volume 24:3.

WRAY, S., "Electronic Civil Disobedience and the World Wide Web of Hacktivism" A Mapping of Extraparliamentarian Direct Action Net Politics" (November, 1998) available at http://www.nyu.edu.projects/wray/wwwhack.html.

WU, T., "Application-Centered Internet Analysis" (1999) 85 *Vanderbuilt Law Review* 1163.

YOUNG, J. 'Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation' (2004) 9 *International Journal of Communications Law and Policy.*

YOUNG, J., "Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation – A Critical Anlaysis of the Council of Europe Convention on Cybercrime and the Canadian Lawful Access Proposal" (2004-2005) *Yale Journal of Law and Technology* 346.

ZENZ, K., "Cyber Crime Within the Russian Federation" presentation at *AusCERT 2008*.

Websites and Articles Published Online

"4Chan Hacks Anti Piracy Lawfirm, Leaks Porn Downloaders' Names", (approximately 23 November 2010) *BuzzFeed* available at http://www.buzzfeed.com/wecanchangetheworld/4chan-hacks-anti-piracy-lawfirm-leaks-porn-downlo-1q36 (last accessed 21 November 2011).

"'Anonymous' hackers hit Visa, Mastercard and Sarah Palin in WikiLeaks revenge", (9 December 2010) *The Australian* available at http://www.theaustralian.com.au/in-depth/wikileaks/anonymous-hackers-hit-visa-mastercard-in-wikileaks-revenge/story-fn775xjq-1225968083650 (last accessed 10 December 2010).

"Anonymous Attacks Anonymous for Being Trolls" (16 November 2011) *Softpedia* available at http://news.softpedia.com/news/Anonymous-Attacks-Anonymous-For-Being-Trolls-234949.shtml (last accessed 18 November 2011).

"Anonymous busts Internet pedophiles" (3 November 2011) *RT* available at http://rt.com/usa/news/anonymous-child-tor-porn-513/ (last accessed 15 November 2011).

"Anonymous Hackers hack neo-Nazis websites & leak personal info of 16,000 Finns", (11 July 2011) *The Hacker News* available at http://thehackernews.com/2011/11/anonymous-hackers-hack-neo-nazis.html

"Anti-Gay Website Hacked by Anonymous" (4 June 2011) *lezbelib.over-blog.com* available at http://lezbelib.over-blog.com/article-anti-gay-website-hacked-by-anonymous-75636306.html (last accessed 5 June 2011).

"Baidu hacked by 'Iranian cyber army'", (12 January 2010) *BBC News* available at http://news.bbc.co.uk/2/hi/8453718.stm (last accessed 13 January 2010).

"Bangladesh Supreme Court website hacked" (11 November 2011) *The Hacker News* available at http://thehackernews.com/2011/11/bangladesh-supreme-court-website-hacked.html (last accessed 12 November 2011).

"BART drafts new policy on disruption of cellphone service" (19 October 2011) *LA Times* available at http://latimesblogs.latimes.com/lanow/2011/10/bart-outlines-cell-phone-service-disruption-policy.html (last accessed 20 October 2011).

BENDRATH, R. "Frankfurt Appellate Court Says Online Demonstration is Not Coercion" (June 7, 2006) Digital Civil Rights in Europe http://www.edri.org/edrigram/number4.11/demonstration

"CCC is at it again – hands out copies of German Interior Minister's fingerprint" (1 April 2008) *The Tech Herald* available at http://www.thetechherald.com/article.php/200814/581/CCC-is-at-it-again-hands-out-copies-of-German-Interior-Minister-s-fingerprint (last accessed 15 July 2010).

"Customs Authority of Yemen Hacked for Protests against Government", (8 May 2011) The Hacker News available at http://thehackernews.com/2011/08/customs-authority-of-yemen-hacked-for.html (last accessed 9 May 2011).

"Cyber-Warfare: The New Global Battlefield" (31 October 2011) *news.sky.com* available at http://news.sky.com/home/technology/article/16099978 (last accessed 2 November 2011).

"FBI Cracks Down on 'Anonymous' Over PayPal Hacking, Arrests 14", (20 July 2011) *International Business Times* available at http://www.ibtimes.com/articles/183495/20110720/federal-bureau-of-investigation-fbi-paypal-online-security-anonymous-hacking-cyber-attack-wikileaks.htm (last accessed 21 July 2011).

"Hacker History & Culture" *H@cker's Handbook* available at http://www.telefonica.net/web2/vailankanni/HHB/HHB_CH03.htm (last accessed 5 January 2012).

"Hackers hit government Web sites after China embassy bombing", (9 May 1999) *CNN Tech* available at http://articles.cnn.com/1999-05-10/tech/9905_10_hack.attack.02_1_hackers-government-web-sites-interior-department-web?_s=PM:TECH (last accessed 10 November 2011).

"Is Serco Behind Stuxnet" (thread started September, 2010 and ongoing) *AboveTopSecret* available at http://www.abovetopsecret.com/forum/thread615788/pg1 (last accessed February 7, 2011).

"Japanese Web Sites Hacked", (25 January 2001) *ABC News* available at http://abcnews.go.com/Technology/story?id=99306&page=1 (last accessed 14 November 2011).

"Lulzsec and Anonymous Blur Lines Between 'Hacktivism' and Criminality, According to PandaLabs Q2 Report" (6 July 2011) *PR Newswire* available at http://www.prnewswire.com/news-releases/lulzsec-and-anonymous-blur-lines-between-hacktivism-and-criminality-according-to-pandalabs-q2-report-125068654.html (last accessed 8 July 2011).

"LulzSec's CIA hack just one of many high-profile hackings", (15 June 2011) *International Business Times* available at http://www.ibtimes.com/articles/163678/20110615/google-lulzsec-s-cia-hack-just-one-of-many-high-profile-hackings.htm (last accessed 20 June 2011).

"Nepal Telecommunications Authority Hacked by w3bd3f4c3r", (21 August 2011) *Hacking Beast* available at http://www.hackingbeast.in/2011/08/nepal-telecommunications-authority.html (last accessed 22 August 2011).

"Online activists hack into Syrian government websites" (26 September 2011) *The Jerusalem Post* available at http://www.jpost.com/MiddleEast/Article.aspx?id=239552 (last accessed 27 September 2011).

"Operation Brotherhood Shutdown: Multiple Sites taken down by Anonymous Hackers", (12 November 2011) *The Hacker News* available at http://thehackernews.com/2011/11/operation-brotherhood-shutdown-by.html (last accessed 13 November 2011).

"Operation Rainbow Dark" *AnonNews* available at http://anonnews.org/?p=press&a=item&i=1162 (last accessed 5 January 2012).

"Owning Kraken Zombies: A Detailed Dissection" (April, 2008) *DVLabs* available at http://dvlabs.tippingpoint.com/blog/2008/04/28/owning-kraken-zombies (last accessed November 11, 2010).

"Second WikiLeaks payback vs. MasterCard: LulzSec or Anonymous?", (29 June 2011) *International Business Times* available at http://au.ibtimes.com/articles/170985/20110629/mastercard-citibank-lulzsec-anonymous-wikileaks-hack-hactivism.htm (last accessed 30 June 2011).

"TechCrunch Hacked? (yes,Techcrunch got hacked)" (26 January 2010) *TechnoFriends* available at http://technofriends.in/2010/01/26/did-techcrunch-got-hacked/ (last accessed 15 November 2010).

"The Complete History of Hacking" *Scribd.com* available at http://www.scribd.com/doc/48245151/The-Complete-History-of-Hacking-1980-2010 (last accessed 5 January 2012).

"Waledac Questions Answered" *LavaSoft* available at http://www.lavasoft.com/mylavasoft/company/blog/waledac-questions-answered.

"War Hack Attacks Tit For Tat", (28 March 2003) *Wired* available at http://www.wired.com/politics/law/news/2003/03/58275 (last accessed 10 November 2011).

"Website of the Presidency of Ecuador suffered cyber attacks", (20 June 2011) *El Universo* available at http://www.eluniverso.com/2011/06/20/1/1355/pagina-internet-presidencia-ecuatoriana-sufrio-ataque-informatico.html?p=1354&m=638 (last accessed 21 June 2011).

"Who are the 'Iranian Cyber Army'", (15 December 2010) *The Green Voice of Freedom* available at http://en.irangreenvoice.com/article/2010/feb/19/1236 (last accessed 16 December 2010).

ANDERSON, N. "Vint Cerf: one quarter of all computers part of a botnet" (January 25, 2007) *Ars Technica* available at http://www.arstechnica.com/news.ars/post/20070125-8707.html. (last accessed May 31, 2011).

BARLOW, J.P., "A Declaration of Independence in Cyberspace" *Humanist* 1996 available at http://editions-hache.com/essais/pdf/barlow1.pdf (last accessed 10 December 2011).

BARROSO, D. of the European Network and Information Security Agency, *Botnets – The Silent Threat* (2007) p. 6 available at http://www.enisa.europa.eu/act/res/other-areas/botnets/botnets-2013-the-silent-threat (last accessed January 29, 2010).

BERGEN, J 28 June 2011, "Anonymous hacktivists take down MasterCard.com again in support of WikiLeaks", *Geek* available at http://www.geek.com/articles/news/anonymous-hacktivists-take-down-mastercard-com-again-in-support-of-wikileaks-20110628/ (last accessed 29 June 2011).

BERNERS-LEE, T. "Net Neutrality: This is Serious" Blog (2006) available at www.dig.csail.mit.edu/breadcrumbs/node/144 (last accessed March 3, 2010).

BESCHIZZA, R. (3 June 2011), "LulzSec claims FBI affiliate hacked, users and botnet are exposed", Boing Boing available at http://boingboing.net/2011/06/03/lulzsec-claims-fbi-a.html

BOYDON, C. "Building a Botnet Empire in Two Days" (June 30, 2006) available at http://images.google.com.au/imgres?imgurl=http://blog.spywareguide.com/upload/2006/05/ISTAdwareThroughWMVFile/ActiveX-thumb.GIF&imgrefurl=http://blog.spywareguide.com/2006/06/&usg=__aA8hJy8hCGm0aUesHouq5e9kMzM=&h=97&w=128&sz=10&hl=en&start=13&tbnid=sxNZtB3wnM9qmM:&tbnh=69&tbnw=91&prev=/images%3Fq%3Ddollarrevenue%2Bpopup%2Bactive%2BX%26gbv%3D2%26hl%3Den

Brandeis http://www.brandeis.edu/legacyfund/bio.html (accessed March 17, 2011).

BRENNER, S. "Hackback as Self-Defense, CYB3RCRIM3: Observations on Technology, Law and Lawnessness" available at http://cyb3rcrim3.blogspot.com/2007/03/hackback-as-self-defense.html. (last accessed April 16, 2010).

CAMBER, R., COLLINS, L., & FERNANDEZ, C., "British teenager charged over cyber attack on CIA as pirate group takes revenge on 'snitches who framed him'" *dailymail.co.uk* (22 June 2011) available at http://www.dailymail.co.uk/sciencetech/article-2006118/Ryan-Cleary-charged-cyber-attack-CIA-LulzSec-takes-revenge.html (last accessed November 10, 2011).

CATE, F. "Information Security Breaches: Looking Back & Thinking Ahead" *The Centre for Information Policy Leadership* (2008) available at www.informationpolicycentre.com/ (last accessed October 22, 2009).

CHIARAMONTE, P. & WINTER, J., "Hacker Group Anonymous Threatens to Attack Stock Exchange" (4 October 2011) *Fox News* available at http://www.foxnews.com/scitech/2011/10/04/hacker-group-anonymous-threatens-to-attack-stock-exchange/ last accessed 4 October 2011.

CLARKE, R., "Categories of Malware" (September 2009) available at http://www.rogerclarke.com/II/MalCat-0909.html (last accessed February 7, 2011).

CLARKE, R., "Peer-to-Peer (P2P) – An Overview" (2004) available at http://rogerclarke.com/EC/P2POview.html (last accessed February 6, 2011).

CLAYTON, R., "Missing the Wood for the Trees" comments on ICANN fast-flux-report (Feb. 2009) available at http://forum.icann.org/lists/fast-flux-initial-report/msg00022.html (last accessed February 7, 2011).

COMLAY, E., "Hackers target mexico government websites" (15 September 2011) *Reuters* available at http://www.reuters.com/article/2011/09/15/us-mexico-hackers-idUSTRE78E7AC20110915 (last accessed 18 September 2011).

CONSTANTIN, L 1 August 2011, "AntiSec Hackers Hit 77 Law Enforcement Websites", Anonymous available at http://news.softpedia.com/news/AntiSec-Hackers-Hit-77-Law-Enforcement-Websites-214555.shtml

CONSTANTIN, L 6 June 2011, Sony Pictures Russian Website Compromised, Softpedia available at http://news.softpedia.com/news/Sony-Pictures-Russian-Website-Compromised-204563.shtml

COUTS, A 9 June 2011, "Citibank hacked, more than 200,000 bank customers at risk", Digital Trends available at http://www.digitaltrends.com/computing/citibank-hacked-more-than-200000-bank-customers-at-risk/

COUTS A 18 August 2011, "Hackers leak Citigroup CEO's personal data after Occupy Wall Street arrests", Digital Trends available at http://www.digitaltrends.com/computing/hackers-leak-citigroup-ceos-personal-data-after-occupy-wall-street-arrests/ ,

DEMETRIOU, C. AND SILKE, A., "A Criminological Internet 'sting': Experimental Evidence of Illegal and Deviant Visits to a Website Trap" (2003) 43 British Journal of Criminology 213

DERIENZO, P., "Eating its Own: Hack Attack" available at http://pdr.autono.net/message2c.html (last accessed 5 January 2012).

DUNN, J. E., "Alleged LulzSec Hacker 'Kayla' Arrested By UK Police" *csoonline.com* (2 September 2011) available at <http://www.csoonline.com/article/689060/alleged-lulzsec-hacker-kayla-arrested-by-uk-police> at 10 November 2011.

ERRETT, J, "Expecting Anonymous at #TMX" (7 November 2011) *NowToronto.com* available at http://www.nowtoronto.com/news/webjam.cfm?content=183319 (last accessed 8 November 2011).

FALLIERE, N., "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems" (August 6, 2010) *Symantec* available at http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (last accessed February 7, 2011).

FARLEY, M 1 February 2001, "Dissidents Hack Holes in China's New Wall"/ "Magazine Is Sent to 250,000 in China", Los Angeles Times available at http://www.gis.net/~cht/dissidents.html

FLETCHER, O., "China Hackers Seek to Rally Peers Against Cybertheft" (3 September 2011) *WSJ.com* available at http://online.wsj.com/article/SB10001424053111903895904576546430870651962.html (last accessed 5 September 2011.

FOGARTY, K 28 October 2011, "Hackers come out of shadows to attack police, support Occupy protests", IT world available at http://www.itworld.com/security/217561/hackers-come-out-shadows-attack-police-support-occupy-protests

GALLAGHER, S., "Anonymous takes down darknet child porn site on Tor network" (24 October 2011) *arstechnica.com* available at http://arstechnica.com/business/news/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network.ars (last accessed 31 October 2011).

GRANT, D., "NYSE Hacked! Is The Anonymous Infrastructure Crumbling?", (10 October 2011), *New York Observer* available at http://www.observer.com/2011/10/nyse-remains-unhacked-is-the-anonymous-infrastructure-crumbling-video/ (last accessed 10 October 2011).

GUTMAN, P. "The Commercial Malware Industry" available at www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf *(last accessed February 4, 2011).*

HARRINGTON, J 8 September 11, "Hacktivism: What is the Chaos Computer Club?", Suite101 available at http://joharrington.suite101.com/hacktivism-what-is-the-chaos-computer-club-a387917 , Wikipedia 2011, "Chaos Computer Club" available at http://en.wikipedia.org/wiki/Chaos_Computer_Club

Honeynet Organisation at http://www.honeynet.org/node/132 (last accessed February 6, 2011).

Honeynet Project at http://old.honeynet.org/misc/project.html (last accessed November 12, 2010).

International Foreign Government E-Mails Hacked by TeaMp0isoN", (7 November 2011) The Hacker News available at http://thehackernews.com/2011/11/international-foreign-government-e.html

JARDIN, X 14 August 2011, "Anonymous hacks BART after wireless shutdown; protests planned for Monday", BoingBoing available at http://boingboing.net/2011/08/14/anonymous-hacks-bart-after-wireless-shutdown-protests-planned-for-monday.html

JIDENMA, N 28 September 2011, "Naija Cyber Hactivists Hack EFCC website to protest proposed internet censor in Nigeria", The Next Web available at http://thenextweb.com/africa/2011/05/26/nigerian-government-agency-website-hacked-by-cyberhacktivists/

KIRK, J 25 August 2010, "Iranian Cyber Army Moves Into Botnets", PCWorld available at http://www.pcworld.com/businesscenter/article/208670/iranian_cyber_army_moves_into_botnets.html

KIRK, J 5 September 2011, "Turkish Hackers Strike Websites with DNS Hack", PCWorld available at http://www.pcworld.com/article/239501/turkish_hackers_strike_websites_with_dns_hack.html , http://www.zone-h.org/

KOVACS, E 15 November 2011, "Anonymous Turns Green and Goes After Polluters", Softpedia available at http://news.softpedia.com/news/Anonymous-Turns-Green-and-Goes-After-Polluters-234681.shtml

KOVACS, E 16 November 2011, "French Nuke Company Fined After Hacking Greenpeace", Softpedia available at http://news.softpedia.com/news/French-Nuke-Company-Fined-After-Hacking-Greenpeace-234900.shtml

KOVACS, E 17 November 2011, "Anonymous Threatens Congress Over SOPA", Softpedia available at http://news.softpedia.com/news/Anonymous-Threatens-Congress-Over-SOPA-235201.shtml

KUMAR, M., "Operation OpIndependencia: Anonymous hit Mexican government official websites", *The Hacker News* available at http://thehackernews.com/2011/09/operation-opindependencia-anonymous-hit.html last accessed 30 September 2011.

KUMAR, M., "Sony Music Brazil Gets Defaced!" (5 June 2011) *thehackernews.com* available at http://thehackernews.com/2011/06/sony-music-brazil-gets-defaced.html (last accessed 6 June 2011).

LAWSON, L., "You say crackers; I say hacker: A hacking Lexicon" (April 13, 2001 available at http://articles.techrepublic.com.com/5100-10878_11-1041788.html (last accessed July 28, 2009).

LEYDEN, J 26 July 2010, "EU climate exchange website hit by green-hat hacker", The Register available at http://www.theregister.co.uk/2010/07/26/climate_exchange_website_hack/ (last accessed 27 July 2010).

LEYDEN, J 4 November 11, "Hackers mistake French rugby site for German stock exchange", The Register available at http://www.theregister.co.uk/2011/11/04/french_rugby_site_hacktivist_maul/ ,

LEYDEN, J 6 December 2010, 20 July 2011, "Anonymous attacks PayPal in 'Operation Avenge Assange'", *The Register* available at http://www.theregister.co.uk/2010/12/06/anonymous_launches_pro_wikileaks_campaign/

LEYDEN, J, 2011 *The Register* available at http://www.theregister.co.uk/2011/10/12/bundestrojaner/ ,

LEYDEN, J., "Anonymous hackers hacked by Young Turks" (22 July 2011) *The Register* available at http://www.theregister.co.uk/2011/07/22/anonplus_hacked/ (last accessed 23 July 2011).

LIEBOWITZ, M 4 November 11, "Hackers Target Stock Index, Hit Rugby Team Instead", Security News Daily available at http://www.securitynewsdaily.com/hackers-stock-index-rugby-team-1309/

LIEBOWITZ, M., "Anonymous releases IP addresses of alleged child porn viewers", (3 November 2011) *MSN Today* available at http://today.msnbc.msn.com/id/45147364/ns/today-today_tech/t/anonymous-releases-ip-addresses-alleged-child-porn-viewers/ (last accessed 4 November 2011).

LIMER, E 15 August 2011, "Anonymous follows through on BART hack, organises protest", Geekosystems available at http://www.geekosystem.com/anon-hacks-bart/ ,

MANDELL, N., "Anonymous hacker group threatens Mexican drug cartel Zetas in online video", (31 October 2011) *New York Daily News* available at http://www.nydailynews.com/news/world/anonymous-hacker-group-threatens-mexican-drug-cartel-zetas-online-video-article-1.969859#ixzz1d4sAfvE6 (last accessed 1 November 2011).

MARTIN, P 10 February 2010, "Australian Government Website Hacked In Protest", Technorati:

MARTIN, P., "Australian Government Website Hacked in Protest" (10 February 2010) *Technorati* available at http://technorati.com/politics/article/australian-government-website-hacked-in-protest/ (last accessed 11 February 2010).

MICK, J 4 April 2011, "Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit", Daily Tech available at http://www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm

MILLMAN, R 29 November 2004, "SCO hit by hacker protest", SC Magazine available at http://www.scmagazineus.com/sco-hit-by-hacker-protest/article/31510/

MILLS, E 6 June 2011, "Hackers taunt Sony with more data leaks, hacks", CNET available at http://news.cnet.com/8301-27080_3-20069443-245/hackers-taunt-sony-with-more-data-leaks-hacks/

MORETTI, S 27 September 2011 http://www.torontosun.com/2011/10/27/video-warns-of-possible-cyber-attack-on-tsx ,

MOSES, A., "Super bad: First State set police on man who showed them how 770,000 accounts could be ripped off" (18 October 2011) *smh.com.au* available at http://www.smh.com.au/it-pro/security-it/super-bad-first-state-set-police-on-man-who-showed-them-how--770000-accounts-could-be-ripped-off-20111018-1lvx1.html (last accessed 18 October 2011).

MOSES, A., "Super sloppy: First State customers kept in the dark" (19 October 2011) *smh.com.au* available at http://www.smh.com.au/it-pro/security-it/super-sloppy-first-state-customers-kept-in-the-dark-20111019-1m7g6.html (last accessed 20 October 2011).

National Cyber-Forensics Training Alliance website available at http://www.ncfta.net/ncfta-initiatives/malware-botnet (last accessed March 2, 2011).

NAZARIO, J, "Politically Motivated Denial of Service Attacks", The Virtual Battlefield: Perspectives on Cyber Warefare, Arbor Networks available at http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf , Thomas, TL 2001, 'The Internet in China: Civilian and Military Uses', Information & Security: An International Journal, vol. 7, pp. 159-173. Available at:

NEAL, D 9 August 2011,"Team Poison hacks Blackberry after riots", The Inquirer available at http://www.theinquirer.net/inquirer/news/2100557/team-poison-hacks-blackberry-riots

NUTTALL, C 19 August 1998, "Chinese protesters attack Indonesia through Net", BBC News available at http://news.bbc.co.uk/2/hi/science/nature/154079.stm

Op free condor http://knightcenter.utexas.edu/blog/hackers-attack-news-website-ecuador

Pagerghost, blog entry commenting on "How to Build a Botnet Empire in Two Days" *Security Lab blog. SpywareGuide* available at http://blog.spywareguide.com/2006/06/building_a_botnet_empire_in_tw_1.html (last accessed May 31, 2010).

PENENBERG, A., "Hacking Bhabha" (16 November 1998) *Forbes* available at http://www.forbes.com/1998/11/16/feat.html (last accessed 11 November 2011).

PFEFFER, A, YARON, O., "Israel government, security services websites down in suspected cyber-attack", (6 November 2011) *Haaretz.com* available at http://www.haaretz.com/news/diplomacy-defense/israel-government-security-services-websites-down-in-suspected-cyber-attack-1.394042 (last accessed 7 November 2011).

POSPISILLI, J., "Cyber Criminals Turn to P2P for DoS Attacks" (July 20, 2007) available at http://tech.blorge.com/Structure:%20/2007/07/20/cyber-criminals-turn-to-p2p-for-dos-attacks? (last accessed July 1, 2010).

QMI AGENCY, "Hacktivist group shuts down child porn sites" (24 October 2011) *Canoe Technology* available at http://technology.canoe.ca/2011/10/24/18871656.html (last accessed 25 October 2011).

RAGAN S, 22 February 2011, "Iranian Cyber Army defaces Voice of America and 93 other domains (Update)", The Tech Herald available at http://www.thetechherald.com/article.php/201108/6849/Iranian-Cyber-Army-defaces-Voice-of-America-and-93-other-domains

RAGAN, S 1 August 2008, "CCC is at it again – hands out copies of German Interior Minister's fingerprint", The Tech Herald:

RAGAN, S 30 May 2011, "PBS: LulzSec attack an attempt to chill journalism", The Tech Herald available at http://www.thetechherald.com/article.php/201122/7215/PBS-LulzSec-attack-an-attempt-to-chill-journalism

ROGERS, M., "Psychological Theories of Crime and Hacking" (Dec. 15, 2006) Telmatic Journal of Clinical Criminology

ROMANO, M., ROSIGNOLI, S., and GIANNINI, E. "Robot Wars – How Botnets Work" (2005) available at http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html (last accessed June 17, 2010).

SANCHEZ, F 27 September 2011, "Hackers hijack Twitter accounts of Chavez critics", MSNBC: http://www.msnbc.msn.com/id/44689342/ns/technology_and_science-security/t/hackers-hijack-twitter-accounts-chavez-critics/

SAWYER, J. "Tech Insight: The Enterprise Hacks Back!" *Dark Reading* available at http://darkreading.com/security/attacks/showArticle.jhtml?articleID=223100750.

SCHNEIER, B. "Stuxnet" (October 7, 2010) available at http://www.schneier.com/blog/archives/2010/10/stuxnet.html (last accessed November 12, 2010).

SCHNEIER, B., Benevolent Worms, Crypto-Gram Newsletter, 2003, available at http://www.schneier.com/cryptogram-0309.html (last accessed November 12, 2010).

SCHROEDER, S 16 June 2011, "LulzSec Hackers Take Down CIA Website", Mashable available at http://mashable.com/2011/06/16/lulzsec-hackers-cia/

Security Beyond Borders, "Salami technique" available at http://securitybeyondborders.org/global-security-glossary/global-security-glossary-s/ (last accessed Marc 18, 2011).

SELTZER, S 22 August 2011, "For-Profit Company Oversaw Davis's Execution, Had Prompted Complaint for Illegal Purchase of Lethal Injection Drugs", Alternet available at http://www.alternet.org/newsandviews/article/670237/for-profit_company_oversaw_davis%27s_execution,_had_prompted_complaint_for_illegal_purchase_of_lethal_injection_drugs/ ,

SYPNOWICH, C. (2001) Law and Ideology, Stanford Encyclopedia of Philosophy, available at http://www.plato.stanford.edu./entries/law-ideology

TAKVER, "European Climate Exchange website hacked", (25 July 2010) *Independent Media Centre Australia* available at http://indymedia.org.au/2010/07/24/european-climate-exchange-website-hacked (last accessed 29 July 2010).

TAYLOR, R., CAETI, T., LOPER, K., FRITSCH, E., AND LIEDERBACH, *Digital Crime and Digital Terrorism* (UK: Pearson, 2005).
The Gospel According to Tux republished from newsgroup posting to various websites such as The New Hacker's Dictionary available at http://www.fullbooks.com/The-New-Hacker-s-Dictionary-version-4-219.html.

The Wrong Guy 10 November 2011, "Activists hack French ruling party's phone numbers", WhyWeProtest available at http://forums.whyweprotest.net/threads/activists-hack-french-ruling-partys-phone-numbers.96206/

THOMAS, T. .L., "The Internet in China: Civilian and Military Uses" (2001) available at http://fmso.leavenworth.army.mil/documents/china-internet.htm (last accessed 5 January, 2012).

TICEHURST, J 20 September 2000, "HSBC internet sites hacked", V3 available at http://www.v3.co.uk/v3-uk/news/2007500/hsbc-internet-sites-hacked

TippingPoint, "Kraken Botnet Infiltration" (April 2008) available at http://www.dvlabs.tippingpoint.com/blog/2008/04/28/kraken-botnet-infiltration (last accessed Nov. 12, 2010).

Tor Project: Anonymity Online available at https://www.torproject.org (last accessed March 17 2011).

Trend MICRO, "Zeus: A Persistent Criminal Enterprise" (March , 2010) available at http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/zeusapersistentcriminalenterprise.pdf (last accessed December, 2010).

TYSON, J., "How Virtual Private Networks Work" available at https://www.computer.howstuffworks.com/vpn.com (last accessed June 30).

VON LEITNER, F http://tbtf.com/resource/felix.html , Wikipedia 2011, "Chaos Computer Club" available at http://en.wikipedia.org/wiki/Chaos_Computer_Club

WHOIS Task Force, available at http://www.gnso.icann.org/issues/whois-privacy/whois-tfl-preliminary.html#GTLDRegistriesconstituency (last accessed April 30, 2010).

WHYTE, S., "Meet the hacktivist who tried to take down the government" (March 14, 2011) *smh.com.au* available at <http://www.smh.com.au/technology/security/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html> (last accessed 7 November 2011).

Wikileaks available at http://wikileaks.org/wiki/Skype_and_the_Bavarian_trojan_in_the_middle

Wikipedia, CCC website available at http://ccc.de/en/updates/2011/staatstrojaner ,

WILLIAMS, Jeff, 'Dismantling Waledac' on *Microsoft Malware Protection Centre – Threat Research & Response Blog* (25 February 2010)
<http://blogs.technet.com/b/mmpc/archive/2010/02/25/dismantling-waledac.aspx>.

WISNIEWSKI, C 10 August 11, "Hong Kong stock exchange (HKEx) website hacked, impacts trades", Naked Security available at http://nakedsecurity.sophos.com/2011/08/10/hong-kong-stock-exchange-hkex-website-hacked-impacts-trades/ ,

WISNIEWSKI, C 12 August 11, "Hong Kong stock exchange attacked for second day in a row", Naked Security available at http://nakedsecurity.sophos.com/2011/08/12/hong-kong-stock-exchange-attacked-for-second-day-in-a-row/

WISNIEWSKI, C 22 May 2011, "Sony BMG Greece the latest hacked Sony site", Naked Security available at http://nakedsecurity.sophos.com/2011/05/22/sony-bmg-greece-the-latest-hacked-sony-site/

WISNIEWSKI, C 30 May 2011, "PBS.org hacked... LulzSec targets Sesame Street?", Naked Security:

WISNIEWSKI, C., "PBS.org hacked... LulzSec targets Sesame Street?" *Sophos* available at http://nakedsecurity.sophos.com/2011/05/30/pbs-org-hacked-lulzsec-targets-sesame-street/ (last accessed 31 May 2011).

WYSS, J 1 November 2011, "Political hackers are one of Latin America's newest headaches", Bellingham Herald available at http://www.bellinghamherald.com/2011/11/01/2252902/political-hackers-are-one-of-latin.html

Xinhua 14 October 2011, "Brazilian presidency's blog hacked in protest of corruption", ChainDaily available at http://www.chinadaily.com.cn/xinhua/2011-10-14/content_4060557.html

ZAKALWE, C 7 July 2011, "Turkish Government Websites Hacked in Protest at Internet Censorship", BlogSpot available at http://stopturkey.blogspot.com/2011/07/turkish-government-websites-hacked-in.html

Zeroday Emergency Response Team (ZERT), available at http://www.isotf.org/zert/.

ZORZ, Z., "Anonymous shuts down child porn sites, leaks usernames" (24 October 2011) *Help Net Security* available at http://www.net-security.org/secworld.php?id=11831&utm_source=twitterfeed&utm_medium=twitter&utm_campaign=s3cb0t (last accessed 31 October 2011).

Chatham House Rules Conference Presentations

Chatham House Organisation available at http://www.chathamhouse.org.uk/about/chathamhouserule/ (last accessed February 7, 2011).

Chatham House Rules. Internet Filtering and Censorship Proposal Forum" (Nov. 2008) Cyberspace law and Policy Centre, the University of New South Wales, Sydney, Australia.

Closed panel on Cybercrime at AusCERT 2008 with Chatham House Rules. Law enforcement agents from the AFP, NSW, Germany and the FBI were present.

Direct question posed to Australian Federal Police at the 2010 High Tech Crime Conference, Sydney. Chatham House Rules.

ISOI 5, Estonia, 2008, Chathom House Rules.

Technical/industry/academic reports

AYCOCK, J. and MAURUSHAT, A., 'Good' Worms and Human Rights. Technical Report 2006-846-39. Department of Computer Science, University of Calgary, 2006.

BALATAZAR, J., COSTOYA, J. And FLORES, R., "Infiltrating WALEDAC Botnet's Covert Operations", (2009) TREND MICRO.

OWENS, W., DAM, K. and LIN, H. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and use of Cyberattack Capabilities(* 2009) Committee on Offensive Information Warfare, National Research Council, Computer Science and Telecommunications Board (CSTB).

PERRIOT, F. And KNOWLES, D., "W32.Welchia.Worm" (July 28, 2004) *Symantec Security Response.*

Quarterly Report PandaLabs (January-March 2010) available at http://www.pandasecurity.om/img/enc/Quarterly_Report_Pandalabs_Q1_2010.pdf (last accessed June 24, 2010).

Symantec, Report on the Underground Economy (2008) available at http://www.symantec.com/content/en/us/about/media/pdfs/underground_Econ_Report.pdf (last accessed June 28, 2010).

TrustDefender, "In-Depth Analysis of Mebroot/Torpig Trojan Available" available at http://www.trustdefender.com/trustdefender-labs-blog-in-depth-analysis-of-mebroot-torpig-trojan-available.html (last accessed January 31, 2011).

WHEELER, D. and LARSEN, G. "Techniques for Cyber Attack Attribution" *Institute for Defense Analysis* (2003) http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf.

United States National Cyber-Forensics and Training Alliance, report on Stuxnet available at http://www.ncfta.net/ncfta-news/ncfta-cyber-alerts/stuxnet (last accessed February 7, 2011).

Briefing papers/working papers/white papers/theses/research projects

BRUNEA, G., "DNS Sinkhole" *SANS Institute InforSec Reading Room* (Aug. 7, 2010), page 2 available at http://www.sans.org/reading_room/whitepapers/dns/dns-sinkhole_33523 (last accessed Feb. 20, 2011).

CLAYTON, R., "Missing the Wood for the Trees" comments on *ICANN fast-flux-report* (Feb. 2009) available at http://forum.icann.org/lists/fast-flux-initial-report/msg00022.html (last accessed February 7, 2011).

CONNELLY, C., MAURUSHAT, A., VAILE, D., and VAN DIJK, P., *Cyber-Security Education Research Project* (2010)..

"Know Your Enemy" series of whitepapers available at http://old.honeynet.org/papers/index.html (last accessed November 12, 2010).

KROGOTH, "Botnet Construction, Control and Concealment: Looking into the Current Technology and Analysing Tendencies and Future Trends" (2008), available at http://www.shadowserver.org/wiki/uploads/Information/thesis_botnet_krogoth_2008_final.pdf (last accessed July 5, 2010)..

LUMBY, C, GREEN, L., and HARTLEY, J., "Untangling the Net: The Scope of Content Captured by Mandatory Internet Filtering" (December 2009) Report Written for Google Australia, available at http://www.saferinternetgroup.org/pdfs/lumby.pdf (last accessed January 3, 2011).

MAURUSHAT, A. "Freedom House Report on Internet Freedom: Australia" (2011).

Media Releases

CONROY, Stephen (Senator), *Budget provides policing for Internet safety*, media release, 13 May 2008, at <http://www.minister.dbcde.gov.au/media/media_releases/2008/033>

FBI Press Release: 'Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems' (Sep 22, 2011) available at http://www.fbi.gov/losangeles/press-

releases/2011/member-of-hacking-group-lulzsec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems (last accessed 20 October 2011).

FBI Press Release: Office of Public Affairs, 'Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks' (19 July 2011) available at http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks (last accessed 10 November 2011).

FBI Press Release: Public Affairs Specialist Laura Eimiller, 'Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems' (22 September 2011) available at http://www.fbi.gov/losangeles/press-releases/2011/member-of-hacking-group-lulzsec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems (last accessed 11 November, 2011).

FBI Press Release: 'Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks' (July 19, 2011) available at http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks (last accessed 20 October, 2011).

FBI Press Release: U.S. Attorney's Office, 'Two Men Charged in New Jersey with Hacking AT&T's Servers' (18 January 2011) available at http://www.fbi.gov/newark/press-releases/2011/nk011811.htm (last accessed 11 November, 2011).

U.S. Department of Justice Press Release: California Man Pleads Guilty in "Botnet" Attack That Impacted Seattle Hospital and Defense Department (May 4, 2000) available at http://www.usdoj.gov./criminal/cybercrime/maxwellPlea.htm (last accessed December, 2010).

Magazine and newspaper articles

BARLOW, J.P., "Is there a there in Cyberspace?" *Utne Reader* 1995 available at http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/3966/3537 (last accessed November 10, 2010), also at http://www.utne.com/archives/IsThereaThereinCyberspace.aspx (last accessed March 18, 2011).

BBC News, "Questions Cloud Cyber Crime Cases" October 11, 2003 available at http://www.bbc.co.uk/2/hi/technology/3202116.stm (last accessed April 27, 2010).

BBC News, "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers" (September 26, 2010) available at http://www.bbc.co.uk/news/world-middle-east-11414483 (last accessed November 12, 2010).

BERINATO, S. "Attack of the Bots" *Wired Magazine* Issue 14.11 (November 2006).

BROAD, W., MARKOFF, J. and SANDER, D., "Israeli Test Worm Called Crucial in Iran Nuclear Delay" (Janaury 15 2011) *The New York Times* available at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (last accessed February 7, 2011).

MADRIGAL, A., "Ahmadinejad Publicly Acknowledges Stuxnet Disrupted Iranian Centrifuges" (November 29, 2010) available at http://www.theatlantic.com/technology/archive/2010/11/ahmadinejad-publicly-acknowledges-stuxnet-disrupted-iranian-centrifuges/67155/# (last accessed February 7, 2011).

MOSES, A. "Super bad: First State set police on man who showed them how 770 000 accounts could be ripped off" (October 18, 2011) available at http://www.smh.com.au/it-pro/security-it/super-bad-first-state-set-police-on-man-who-showed-them-how--770000-accounts-could-be-ripped-off-20111018-1lvx1.html.

PILGER, J. "The War on Wikileaks: A John Pilger Investigation and Interview with Julian Assange" (January 13, 2011).http://johnpilger.com/articles/the-war-on-wikileaks-a-john-pilger-investigation-and-interview-with-julian-assange

RASH, M. "Mother, May I" available at http://www.securityfocus.com/print/columnists/463 (last accessed January 29, 2008).

RAYWOOD, D., "Is the Mariposa Botnet Still Functioning?" (June 24, 2010) available at http://www.securecomputing.net.au/News/217678,is_the_mariposa_botnet_still_functioning.aspx (last accessed June 26, 2010).

RISING, G., "Cody Kretsinger Arizona College Student Charged in Sony Hacking Case" The Huffington Post (January 12, 2010) at http://www.huffingtonpost.com/2011/09/23/cody-kretsinger-arizona-c_n_977490.html

SOPHO, "Sopho Assists Computer Crime Unit in Bringing Botnet Master to Justice" June 12, 1008 available at assistshttp://www.sophos.com/pressoffice/news/articles/2008/06/bentley-imprisoned.html.

The Age, "The Cyberspace Wars" (June 22, 2003) available at http://www.theage.com.au/articles/2003/06/21/1056119529509.html (last accessed December 2010).

WHYTE, S. "Meet the Hacktivist Who Tried to Take Down the Government" (March 14, 2011) Sydney Morning Herald.

ZORZ, Z., "French Hacker and Alleged Anonymous Member Arrested After Bragging on TV" (April 13, 2011) at http://www.net-security.org/secworld.php?id=10895

Online videos and podcasts

"Anonymous to Australia" available at http://www.youtube.com/watch?v=eEc80U46hIQ (last accessed January 13, 2011).

INSIGHT, "Hacktivism" (September 27, 2011) available at http://www.sbs.com.au/insight/episode/index/id/431.

KEMMER, R. "How to Steal a Botnet and What Can Happen When You Do" *Google Tech Talk* (Sept. 2010) available at http://www.youtube.com/watch?v=2GdqoQJa6r4 (last accessed June 26, 2010).

LANGILL, J., "Stuxnet Worm Detailed Examination by SANS" available on a hacker website http://www.garage4hackers.com/showthread.php?604-Stuxnet-Worm-Detailed-Examination-by-SANS (last accessed February 7, 2011).

GREY, P., Risky.biz Podcast, "RB2: AusCERT Podcast: Interview with Moscow-Based Cybercrime Analyst Kimberly Zenz" (May 20, 2009).

GREY, P. Risky.biz Podncast, "Interview on Risky Business with Michael Dwyer, Chief Executive of First State Superannuation" (October 14, 2011) http://risky.biz/minter

The Agenda, "Attack of the Hacktivists" TVO October 25, 2011

Wikipedia

Wikipedia, "Anonymous P2P" available at http://en.wikipedia.org/wiki/Anonymous_P2P (last accessed November 12, 2010).

Wikipedia, "Bennett Arron" available at http://en.wikipedia.org/wiki/Bennett_Arron (last accessed May 31, 2010).

Wikipedia, "Click Fraud", available at http://en.wikipedia.org/wiki/Click_fraud (last accessed June 30, 2010).

Wikipedia, "Denial of Service Attack (distributed)", available at http://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack (last accessed June 30, 2010).

Wikipedia, "Denial-of-service (unintentional)", available at http://www.en.wikipedia.org/wiki/Denial-of-service_attack#Unintentional_denial_of _service (last accessed June 30, 2010).

Wikipedia, "Peer-to-peer" available at http://en.wikipedia.org/wiki/Peer-to-peer (last accessed December 2011).

Wikipedia, "SPAM", available at http://en.wikipedia.org/wiki/E-mail_spam (last accessed June 30, 2010).

Wikipedia, "Virtual Private Network" available at http://www.en.wikipedia.org/wiki/Virtual_private_network (last accessed June 30, 2010).

Pilon, Claude

From: Covo, Pierre
Sent: Tuesday, October 16, 2012 11:00 AM
To: Clow, Patrick
Cc: Pilon, Claude
Subject: RE: Study

Great, thanks.

From: Clow, Patrick
Sent: October-15-12 4:00 PM
To: Covo, Pierre
Cc: Pilon, Claude
Subject: Study

Hi Pierre,

Please find attached a copy of the Ethical Hacking article discussed last week.

Thank you

Pilon, Claude

From: Covo, Pierre
Sent: Tuesday, October 16, 2012 10:41 AM
To: * Legal Serv. / Ser. Juridiques
Subject: FYI: Study commissioned by PS on ethical hacking
Attachments: Report PS-SP Ethical HackingFINAL.DOC

Courtesy of the CCIRC client. Here is a media link about the report. (link here)

Ethical Hacking

A Report for the National Cyber Security Division of
Public Safety Canada

2012

Alana Maurushat

Contents

1. Executive Summary

1.1 What is ethical hacking?

In its traditional form, hackers were people who used clever technical solutions to solve problems. Ethical hacking then is the non-violent use of a technology in pursuit of a cause, political or otherwise which is often legally and morally ambiguous. [1] Ethical hacking is also referred to as electronic civil disobedience, hacktivism, grey hat hacking, intrusion and penetration testing, counter-attacks, and politically motivated hacking/computer crime.

This report discusses ethical and legal issues with four types of ethical hacking: hacktivism, online civil disobedience, penetration/intrusion testing & security activism, and counter-attack.

1.2 Methodology

This report examines different types of ethical hacking. It includes a multi-disciplinary literature review, interviews from hacker researchers, caselaw charted over the last ten years in Canada, the United States, the United Kingdom, Australia, New Zealand, Hong Kong, France, Germany and Russia, and a recent time-line of important ethical hacking incidents. A more detailed description of the methodology is found in section 3.

Abbreviated references are found in the footnotes. Full references are found in the Reference Section at the end of this Report.

1.3 Key Findings and Recommendations

Key findings are listed below:

- Online protests will increase and the type and size of such attacks will escalate in order to continue to capture the interest of the media.

- There is a growing movement in some online communities (hackers) to ensure that "backdoors" (ways to exploit a program) are inserted into computer programs and then kept quiet as a means of ensuring access to future information (especially government websites). These types of "attacks" are not done for instant media attention.

- Technologies such as LOIC will evolve to allow for encryption and anonymity. This will parallel similar developments that took place with peer to peer file-sharing networks.

- The most popular discussion threads in hacking forums are "beginner hacking" and "hacking tools and programs" indicating the likelihood of increased hacking, both ethical and for criminal purposes.

- Deterrent effect of laws and sentences only works with beginners and with younger hackers. These individuals will generally quit illegal hacking after first conviction (under 25).

---

[1] Samuel 2004.

- The law does not have a deterrent effect for highly skilled and often older hackers (over 25).

- Some individuals involved in hacking are considered be have an addiction in the same way that an individual may become addicted to gambling, video games, drugs or alcohol.

- A significant portion of corporations and organisations are engaged in some form of counter-attack.

- Many ethical hacking incidents are closely tied with the objective of protecting human rights and promoting an open, transparent democracy.

- Many ethical hackers view their work as acts of civil disobedience and align their actions with traditional civil disobedience as espoused by Ghandi, Martin Luther King Jr. And Henry David Thoreau.

- Other hackers identify with an ethos of hacking that developed in the 1980s forward and look to technical gurus and the writings of "Hacktivismo Declaration" by the Cult of the Dead Cow, "The Hacker Manifesto", "The Anonymous-Anonops", The Electrohippies "Client-Side Distributed Denial-of-Service" and the "Gospel According to Tux".

- Other groups are less ideal in their philosophy citing motivation as "for the laughs". However, further probing of such hackers reveals that their hacking is done out of "a streak of sense of wrongdoing" without always being able to clearly articulate what that wrongdoing is.

- Denial of Service Attacks by movements such as Anonymous require critical mass in order for an operation to be successful.

- There is often a correlation between the number of participants in a denial of service attack, and the worthiness/morality of the cause.

- Which causes will acquire critical mass is unpredictable.

- It would be incorrect for governments or organisations to assume that members of ethical hacking groups come from one type of community, race, or age.

- Many ethical hackers are not aware that their activities are illegal, especially those participating in politically motivated denial of service attacks.

- Elite hackers tend to work alone due to the higher risk of "getting caught" when groups are involved. This may support the proposition that a technically sophisticated attack may in fact be the work of only one individual, or few individuals.

- While many instances of ethical hacking may be illegal, it is interesting to note that some methods used by law enforcement and by security firms contracted to perform criminal intelligence gathering may also be illegal, or at best highly controversial.

The report concludes by making a number of recommendations. These are:

- Develop and publicise guidelines for online civil disobedience and hacktivism.
- Run an education campaign once these guidelines are finalised.
- Allow and encourage a legitimate "space" for virtual protests.
- Investigate the licensing of security experts.
- Implement a security research exemption for computer offences.
- The idea of a public interest exemption for hacking offenses should be given further consideration. This could be done in a multi-party working group on both security research and public interest exemptions.
- Develop a code of conduct for counter-attack and have a legislative review of how principles of self-defence might apply to a counter-attack situation.
- Any governmental engagement with ethical hacking should be legal and transparent. These activities should not be contracted out to security firms unless they are closely scrutinised and held accountable in some form of safeguard or compliance mechanism.
- Ensure that data owned or generated by Canadians is protected and that such data, if collected and stored, is deleted after a reasonable period when using foreign services such as Google, Facebook and Twitter (United States based). Currently, any person who uses Google, Facebook, Twitter and similar services is subject to US Internet monitoring by governments and law enforcement, and potentially is exposed to subpoenas to release personal information, even in the *absence* of a transparent criminal investigation.

1.4 Research Acknowledgements

This research would not have been possible without the research assistance of Lauren Loz, ,Taylor Hall, Bodil Diederichsen, Nazar Sharunenko, Patrick Webster, and several individuals who have chosen to remain anonymous. Additional thanks to Suelette Dreyfus and Alexandra Samuel for agreeing to share their expertise in this area.

2. Introduction and Background

In its traditional form, hackers were people who used clever technical solutions to solve problems. Ethical hacking then is the non-violent use of a technology in pursuit of a cause, political or otherwise which is often legally and morally ambiguous. Ethical hacking is also referred to as electronic civil disobedience, hacktivism, grey hat hacking, intrusion and penetration testing, counter-attacks and politically motivated computer crime (discussed in detail in section 4). The current most popular term used by media to describe ethical hacking is hacktivism.

Civil activists in the 1960s and 1970s had sit-ins and protests for civil rights and anti-war. Many people equally thought that this civil disobedience could lead to change. Change would lead to rational and critical discussion of citizens with governments in a move towards more open and transparent democratic governance. In the late 1970s and early 1980s many governments enacted laws around freedom and access to information to better ensure open disclosure and government transparency. Prior to such enactment of freedom and access to information laws, it was difficult to obtain copies of government documents. These laws were devised in an attempt to move the disclosure of information default from private to public. In this sense, a government employee

would not ask when something should be made public, but rather, when something should be made private (in other words, transparency by default).

While freedom and access to information laws have shifted the line of transparency, they did not achieve transparency by default. Internal guidelines for when information should remain private or public were muddled with bureaucratic wording, and confusion. The end result was government employees began to self-censor. This took place in two main ways. The first, when classifying documents employees erred on the side of caution and thus over-classified documents as private/secret and under-classified documents as public/transparent. The second, when access to information requests were granted, often documents were so blacked out that it was difficult to ascertain with any certainty what decision or policy was adopted or why. The "black pen" effect began.

The first part of the 21st Century will likely go down in history as the era when ethical hackers opened governments. The line of transparency is moving by force. The twitter page for Wikileaks demonstrates this ethos through its motto "we open governments" and its location to be "everywhere". Hacktivism is a form of civil rights activism in the digital age. In principle hacktivists believe in two general but spirited principles: respect of human rights and fundamental freedoms including freedom of expression and personal privacy, and the responsibility of government to be open, transparent and fully accountable to the public. In practice, however, hacktivists are as diverse in their backgrounds as they are in their agendas.

Ethical hacking is not new. In the late 1980s Australian hacktivists penetrated the NASA computer system releasing a worm known as WANK – Worms Against Nuclear Killers.[2] The worm was written and released as a form of protest for the NASA launch of the rocket Galileo which was to navigate itself to Jupiter using nuclear energy. The infamous German hacker group "Chaos Club" was also busy in the late 1980s attacking German government systems to protest against collecting and storing of census information; the groups believed that the government should not collect or store the personal information of its citizens.[3]

Moving forward to the first decade of the 21st Century, ethical hacking, while not new, has fundamentally changed in one distinct manner – the ability to participate in attacks (denial of service attacks) is no longer limited to an elite group of people with excellent computer skills; the technology is available to the masses in an accessible format for those with limited technical skill. People follow tweet feeds of Anonymous and LulzSec where operations are suggested. If the person decides to participate in an operation, they simply click the download button for LOIC software, select the demonstration they wish to participate in by typing in the URL (Eg. www.alana.com), then click again. Fait accompli. The individual is now participating in a denial of service attack. It must be noted that denial of service attacks using LOIC require a critical mass to be effective. This means that many people must deliberately choose to participate in an event.

People around the globe are participating in denial of service attacks on many types of websites for a variety of causes. Websites that have been attacked to date include the Australian Parliament's website, Paypal, Mastercard, Mexican government website, paedophilia websites, the New York Stock Exchange, the Toronto Stock Exchange, News of the World, Oakland City Police, Ecuadorian government, Peruvian government and the list goes on and on (see **Appendix B**).

One of the most well-known hacktivism "groups" is Anonymous. The word group here is arguably used incorrectly as Anonymous is more like an umbrella name or a movement for a plethora of

---

[2] Dreyfus and Assange 1997.
[3] Dreyfus and Assange 1997.

smaller groups and operations. In addition to performing denial of service attacks, members of some of the smaller groups participate in more sophisticated forms of hacktivism that require a higher range of computer skills. Instances of these more sophisticated attacks include the release of names and details of the Mexican drug cartel, Los Zetas, the names and details of individuals who use child pornography sites, and the capturing of secret documents held by governments around the world – some of these documents are then given and released by Wikileaks.

Hacktivism isn't limited to attacking information systems and retrieving documents. It also extends to finding technical solutions to mobilise people. At the height of the Egyptian e-revolution the major Internet service providers and mobile phone companies shut down the Internet (the kill switch) preventing people from using the Internet and mobile phones. This, in turn, affected the people's ability to mobilise. Anonymous worked around the clock to ensure that images from the revolution were still being sent to the international press. Hacktivists also work to penetrate the Iranian government's firewall to tunnel passages allowing Iranian citizens to view blocked sites. I myself have been involved with a similar firewall penetration when I organised some of the internal testing of the Chinese firewall for the Open Net Initiative – a collaborative research project between the Citizen Lab, at the University of Toronto, The Berkman Centre for Internet and Society at Harvard, and the University of Cambridge. There are similar initiatives for Saudi Arabia and other parts of the world with strong censorship. Keeping secrets and preventing citizens from accessing information may no longer be an achievable goal. The question becomes, should governments adopt heavy-handed policies and law to investigate and prosecute ethical hackers to deter such activity and keep the status quo? Or should governments enact an appropriate legislative response that reflects the reality of this new era – the forced line of transparency?

Other forms of ethical hacking are rooted in ensuring the security of networks. This has taken shape in four main ways. The first is through intrusion or penetration testing where experts are invited to expose any security vulnerabilities of an organisation's network. The second is somewhat more controversial as it involves hackers who, without authorisation, illegally access a network, software or hardware to expose security vulnerabilities. Sometimes these hackers will go so far as to fix the vulnerability or to report it to the system's owner. Third, there is a growing concern that many organisations including corporations and governments are engaging in counter-attack efforts to deter attacks to their systems. Last, many security experts are forming self-organised security communities to actively engage in intelligence gathering, and counter-attacks – this will be called security activism.

This report discusses moral and legal issues of ethical hacking. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. There are no exceptions to the cybercrime/computer crime provisions for security research or public interest in most jurisdictions around the globe. Equally difficult will be how civil rights will apply to hacktivism. This question is shrouded with uncertainty. How will governments and courts manoeuvre in this new era of activism meets computer within the boundaries of protected civil liberties?

3. Methodology

This report examines four types of ethical hacking:

- Hacktivism,
- Online civil disobedience,
- Penetration/intrusion testing, & Security activism, and

- Counter-attack

Each category will be defined and a series of related aspects will be examined. These include:

- Selected Case Studies
- Motivation
- Main Targets
- Relation Between Targets and Motivations
- Fundamental Principles of "Hacker-Ethics"
- Perceptions of the Illegality of Activity
- Deterrence Effects of Case Law and Convictions
- Relevant Case Law Convictions
- Observations

An ethical hacking case law summary for the last 10 years will be provided looking at cases in Canada, the United States, the United Kingdom, Australia, New Zealand, Hong Kong, Singapore, France, Germany and Russia. The summary is found in **Appendix A**.

Recent ethical hacking incidents for the last two months of 2011 is provided in **Appendix B**.

Technical and legal challenges to the investigation and prosecution of hackers will additionally be analysed. This portion of the study borrows heavily from my own PhD in cybercrime entitled, "Botnet Badinage: Regulatory Approaches to Combating Botnets" (PhD Thesis, The University of New South Wales, 2011) where I interviewed people involved in the cyber security industry (including law enforcement), some cybercriminals and attended conferences around the world including Eastern Europe, the United Kingdom, Canada, Australia, Hong Kong and the United States. The technical and legal challenges are the same for hacking activities in general. Any specific technical or legal challenges specific to ethical hacking will also be analysed.

As there have been few interviews or empirical studies on ethical hacking (though there are several studies now underway which have not yet been published), studies that have looked at hacking in general will be utilised. Three of the most significant studies of hackers to date have been:

1) Dr. Suelette Dreyfus and Julian Assange in their book, *Underground* (William Heinemann, first published in 1997, with a reprint and update in 2011).

2) Raoul Chiesa, Stefania Ducci and Silvio Ciappi in their UNICRI study, *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* (CRC Press, 2009).

3) Dr. Alexandra Samuel, *Hacktivism and the Future of Political Participation* (PhD Thesis, Harvard, 2004).

Suelette and Alexandra have agreed to be interviewed for their views on the topic. The interview questions are included in **Appendix C**. Some of their responses are incorporated into the main body of the report. Raoul was not able to be interviewed but I have gratefully borrowed some statistics and other information from his profiling of hackers study.

An extensive multi-disciplinary literature review (information systems, psychology, fiction, risk management, computer science, law, political science) was conducted and is included in the reference section.

4. Typology

The terminology around ethical hacking is confusing as terms mean different things according to their disciplines and often these terms are used interchangeably. For instance, the technical world distinguishes between a hacker and a cracker whereas the mainstream media lump both terms under the umbrella of "hacker". Expressed differently, the distinction is sometimes made by referencing black hat, grey hat and white hat hackers. For clarity these terms are defined below:

Hacker: "A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term.[4]"

Cracker: "A cracker is an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system.[5]"

Black Hat Hacker: (also referred to as a cracker), is "someone who uses his computer knowledge in criminal activities in order to obtain personal benefits. A typical example is a person who exploits the weaknesses of the systems of a financial institution for making some money.[6]"

White Hat Hacker: "Although white hat hacking can be considered similar to a black hacker, there is an important difference. A white hacker does it with no criminal intention in mind. Companies around the world, who want to test their systems, contract white hackers." [7]" They will test the security of a system, and are often hired to make recommendations to improve such systems.

Grey Hat Hacker: "A grey hat hacker is someone who is in between these two concepts. He may use his skills for legal or illegal acts, but not for personal gains. Grey hackers use their skills in order to prove themselves that they can accomplish a determined feat, but never do it in order to make money out of it. The moment they cross that boundary, they become black hat hackers."[8]

People who participate in ethical hacking are predominantly grey hat hackers. The differentiation, however, between hackers, crackers, and colours of hats plays little importance when looking at these concepts from a legal perspective. Any form of unauthorised access, modification or impairment of data, a network or computer is a crime. There are no exemptions in most jurisdictions; hackers and crackers alike rely on the discretion of law enforcement as to whether to prosecute or turn a blind eye. Another fallacy in classifying hackers is that an individual falls solely into one definition. Each single attack must be characterised, not the person behind the attack. For example, you might have a hacker who predominantly breaks into systems to learn, sometimes she might even fix a security flaw in a system. The same hacker might also break into a system to collect data on individuals who are actively engaged in viewing and downloading child pornography, and then make this data publicly

---

[4] RFC 1392 Internet Users Glossary.
[5] RFC 1392 Internet Users Glossary.
[6] Hacking Alert, "White Hat and Grey Hat Hacking: What is the Real Difference?" http://www.hackingalert.com/hacking-articles/grey-hat-hackers.php. *See also* Hafele 2004.
[7] Hacking Alert, "White Hat and Grey Hat Hacking: What is the Real Difference?" http://www.hackingalert.com/hacking-articles/grey-hat-hackers.php
[8] Hacking Alert, "White Hat and Grey Hat Hacking: What is the Real Difference?" http://www.hackingalert.com/hacking-articles/grey-hat-hackers.php

available to law enforcement and the public at large. Yet this same hacker might also accept a fee to break into a corporation's (who they view as unethical) database and steal a trade secret that is handed over to a competitor. Each of these examples involves unauthorised access. The difference with each attack goes to intent, motive, and involves the individual's subjective notion of what is ethical or moral. Ethical hacking is, therefore, difficult to define.

Ethical hacking is also a term that is used interchangeably with hacktivism in the media, but which has a distinct meaning in the computer science discipline. For example, in the computer science field "ethical hacking" is used to describe what is known as penetration or intrusion testing (white hat hacking). Similarly, someone who merely participates in a denial of service attack for political reason would not be considered a hacker within the computer science community. This type of action would be more akin to online civil disobedience.

For this report, "ethical hacking" will be used in its broadest sense to include the following activities:

Hacktivism: is the clever use of technology which involves unauthorised access to data or a computer system in pursuit of a cause or political ends. [9]

Online Civil Disobedience: is the use of any technology that connects to the Internet in pursuit of a political ends.

Penetration/Intrusion Testing: is a type of information systems security testing on behalf of the system's owners. This is known in the computer security world as "ethical hacking". There is some argument, however, as to whether penetration testing must be done with permission from a system's owners or whether a benevolent intention would suffice in the absence of permission. Whether permission is obtained or not obtained, however, does not change the common cause, that of improving security.

Security Activism: is similar to penetration/intrusion testing in that the cause is to improve security. Security activism goes beyond mere testing of security, however, to gather intelligence on crackers, and to launch active attacks to disrupt criminal online enterprises. One example is the taking down of a botnet (see section 7).

Counter-Attack: is also referred to as hackback or strikeback. Counter-attack is when an individual or organisation who is subject to an attack on their data, network or computer takes similar measures to attack back at the "hacker/cracker". For example, when an individual or organisation is subject to a denial of service attack, that organisation might initiate their own denial of service attack on the responsible party's website.

<u>Ethical Hacking:</u> Ethical hacking then is the non-violent use of a technology in pursuit of a cause, political or otherwise which is often legally and morally ambiguous.[10]

The use of a technology which resulted in acts of violent or physical harm would fall outside of the scope of ethical hacking, and may even be considered as cyber-terrorism (attack to critical infrastructure). The ambiguous legal and moral nature of ethical hacking will be explained in sections 5 through 8.

---

[9] Samuel 2004.
[10] Samuel 2004.

5. Online Civil Disobedience

5.1 Description

Online Civil Disobedience is the use of any technology that connects to the Internet in pursuit of a political end. There are many forms of online civil disobedience. A person or groups of individuals may block access to a website, redirect web traffic to a spoof website, deface a website, or flash messages on someone's computer screen. The offline equivalents would be a sit-in blocking access to a building, a protest which prevents people from using a street such that they are redirected down another path, protesting with signs and images, handing out flyers or placing such flyers in mailboxes.

Online civil disobedience incorporates a variety of techniques to carry out activities. These technologies are described below:

SQL Injection
Defacing a website involves the insertion of images or text into a website. This is often done via a SQL injection (structured query language). A SQL injection is an attack in which computer code is inserted into strings that are later passed to a database.[11] A SQL injection can allow someone to target a database giving them access to the website. This allows the person to deface the website with whatever images or text they wish.

DNS Highjacking
DNS hijacking allows a person to redirect web traffic to a rogue domain name system server.[12] The rogue server runs a substitute IP address to a legitimate domain name. For example, www.alanna.com's true IP address could be 197.653.3.1 but the user would be directed to 845.843.4.1 when they look for www.alanna.com. This is another way of redirecting traffic to a political message or image.

Adware/Spyware
Adware refers to any software program in which advertising banners are displayed as a result of the software's operation. This may be in the form of a pop-up or as advertisements displayed on the side of a website such as Google or Facebook.

Distributed Denial of Service Attack (DDoS)
A DDoS is the most common form of online civil protest. A denial of service attack is distributed when multiple systems flood the channel's bandwidth and/or flood the host's capacity (e.g. overflowing the buffers) .[13] This technique renders a website inaccessible.

Distributed denial of service attacks are performed with a botnet with several of the compromised computers sending packets to the target computer simultaneously. A DDoS attack may also be distributed by use of peer-to-peer nodes.[14] The importance of botnets is explained below.

---

[11] Security Spotlight 2010.
[12] Security Spotlight 2010.
[13] Denial of Service Attack is well defined on http://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack
[14] Athanasopoulos et al. 2006. E., Anagnostakis, K., and Markatos, E., "Misusing Unstructured P2P Systems to Perform DoS attacks: The Network that Never Forgets".

Botnet: A botnet is a collection of compromised computers that are remotely controlled by a bot master.[15]

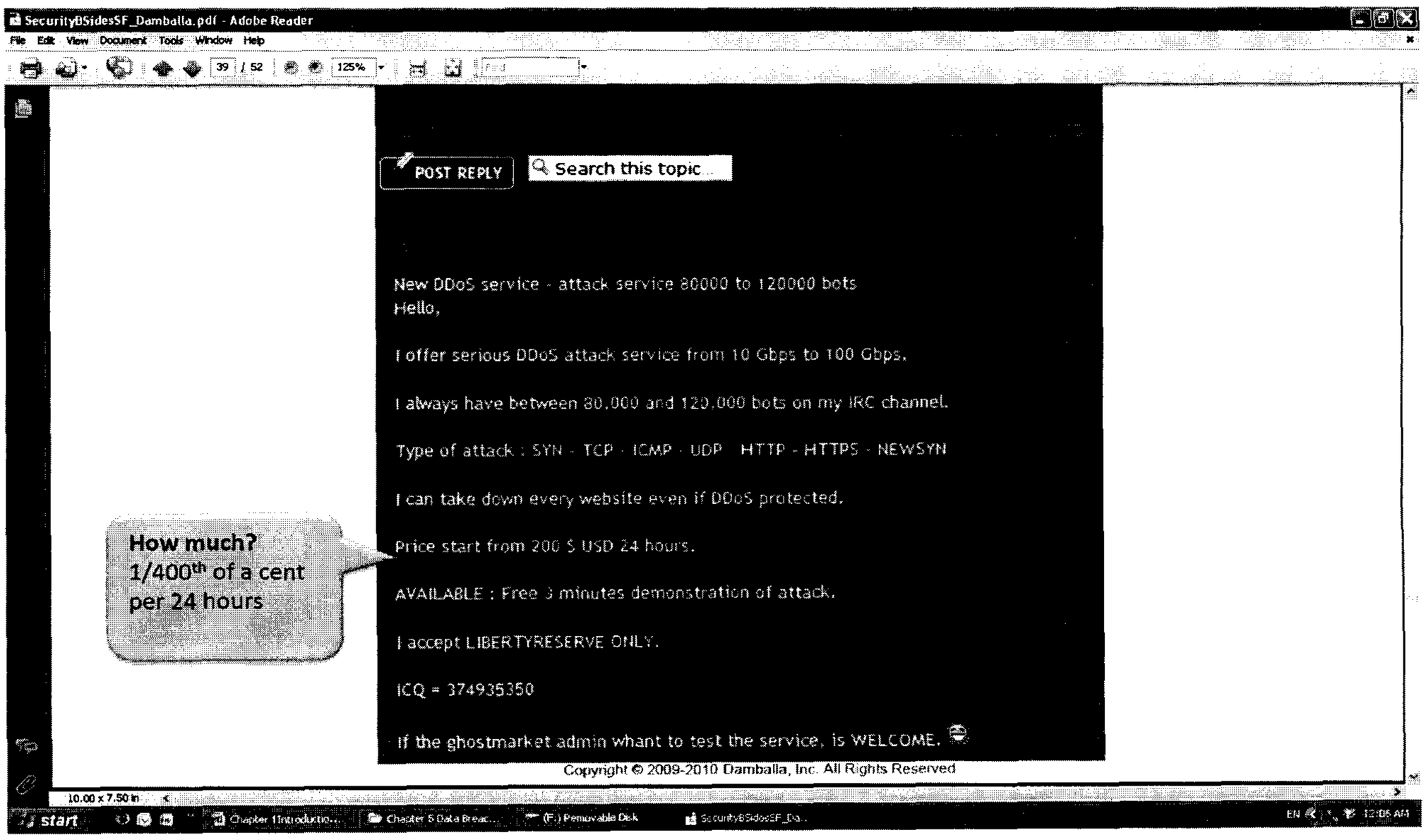
There are three ways of using a botnet to perform a denial of service attack:

Make the Botnet: In the first, a person would have to physically make a botnet through painstaking hours of labour as it would involve compromising several hundred if not thousands of computers. This type of botnet would require the botnet master to have a high level of computer skills.

Hire/Rent a Botnet: T he second type is whereby the person merely hires someone to execute a denial of service attack. This requires no computer skills but for the ability to use Google. Bot agent design and bot delivery have become a commoditized service industry.[16] A small botnet is sufficient to launch an effective denial of service attack causing much damage and costs as little as $200 USD for a 24 hour attack.[17] A person does not require any special computer skills to use a botnet to commit a crime. **Figure 1** on the following page is a sample of the commercialisation of denial of service attacks with a botnet. The customer would merely specify the targeted website to attack, pay a nominal fee of $200 USD, and a denial of service attack (DOS attack) would be launched for 24 hours against the website.

[15] Maurushat 2011.
[16] Ollmann 2010.
[17] Ollmann 2010.

Figure 1 Denial of Service Attack as Commercial Service[18]

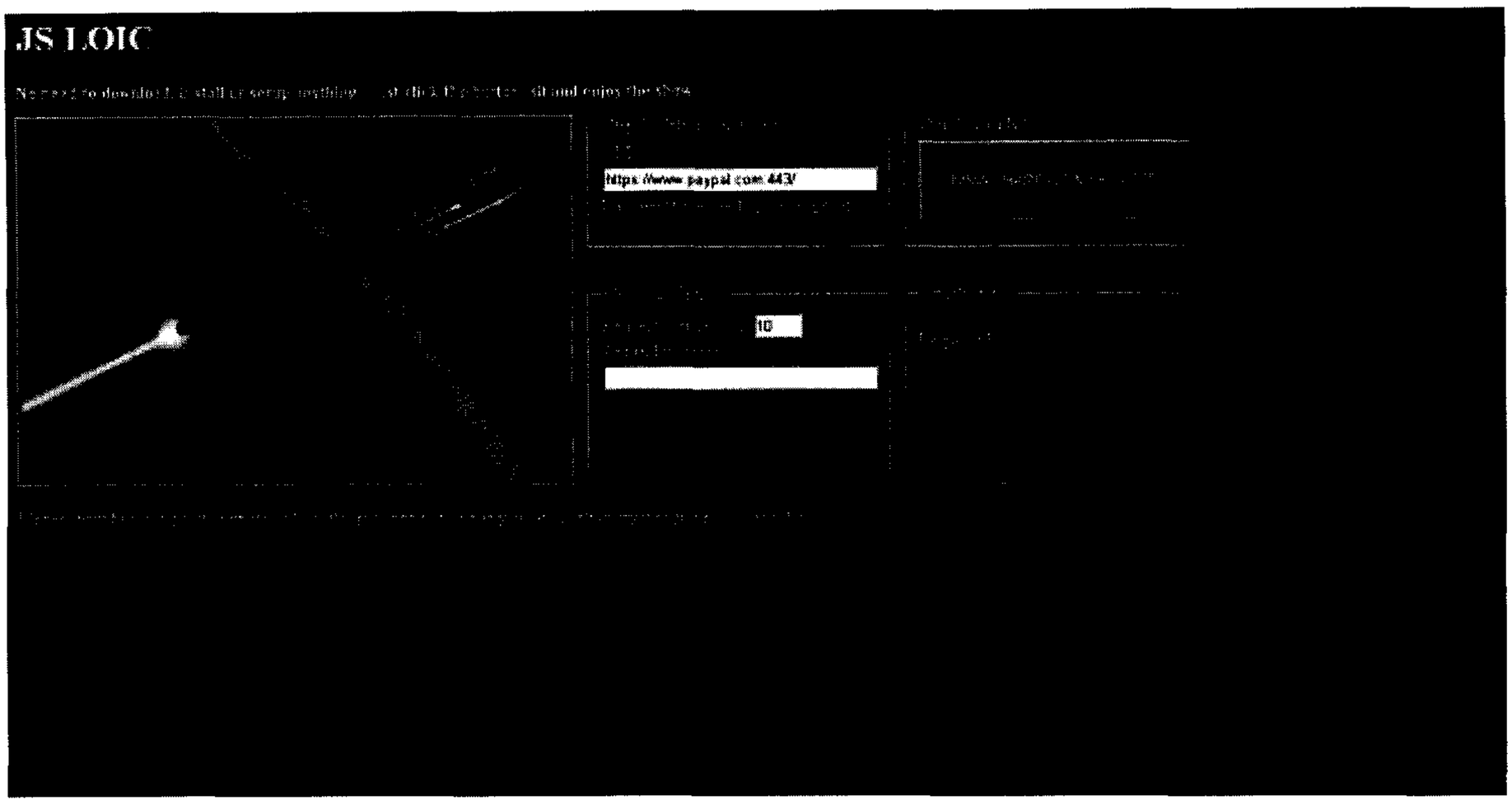


Commercialisation is also occurring within another context known as crime kits. In this instance a person is able to purchase a copy of the botnet code in the form of a crime kit. The kit comes with a licence to use the botnet, and instructions. ZeuS, for example, is a popular crimeware kit that may be purchased for $700 USD.[19] Expert computer skills are not required for botnet usage. A criminal may elect to purchase a crimeware kit with simple instructions on how to execute an attack.

LOIC or Similar Software: The last botnet involves a free software program known as LOIC (Low Orbit Ion Canon). LOIC is used for most of the denial of service attacks performed by members of Anonymous. **Figure 2** on the following page captures an image of LOIC executing a denial of service attack against Paypal. Use of LOIC requires minimal computer skills. One googles LOIC, downloads the software with a click, types in the URL (Eg. www.paypal.com), and presses start. The denial of service attack then commences and people join in from all over the world using LOIC.

[18] Image from Ollmann 2010.
[19] *See* Trend MICRO 2010.

Figure 2 LOIC DDoS Attack Against Paypal[20]



Differentiating between these three types of botnets has legal implications. In the instance of making a botnet, the botnet master would have had to acquire control over user's computer without their authorisation thereby attracting cybecrime provisions for unauthorised access, modification or impairment to data. Hiring or renting a botnet also attracts similar criminal sanction. Using LOIC, however, would not necessarily attract criminal sanction for unauthorised access. This is because the computers connected to LOIC are doing so voluntarily. The issue of whether the actual attack involves unauthorised access as opposed to a form of legitimate civil disobedience is contentious (see below for caselaw).

5.2 Case Studies

Wikileaks Operation Payback

Wikileaks founder Julian Assange was arrested in London on charges of sexual crime under Swedish law. Many viewed this as a false arrest and indirect way of incarcerating Assange for the release of secret US cables to Wikileaks. A legal defence fund was quickly established where people could make donations via Mastercard or Paypal to help the cause. Mastercard and Paypal disallowed any payments to be made to the Assange legal defence fund causing an international uproar, and in particular, within hacktivism communities. Members of LulzSec launched a denial of service attack against Mastercard and Paypal which took down their capabilities in December 2010 and then again in June 2011. As will later be seen in section 8, there was a denial and counter-denial of service attack showdown which might best be seen as gunfire between warring factions, with evidence that the US government contracted security firms to perform attacks against Wikileaks and other journalists.

---

[20] Image from http://www.wired.com/threatlevel/2010/12/web20-attack-anonymous/

Anonymous Operation Titstorm

In 2010 the Australian government sought to introduce a mandatory internet filter. This was unofficially referred to as 'Clean Feed'. Internet filtering in this context would mean requiring Internet Service Providers (ISPs) such as Optus, Telstra and iiNet to implement technical means to filter out a set list of illegal websites, most notably websites with images of child abuse and child pornography. Internet filtering techniques are commonly used in authoritarian regimes such as China and Iran, as well as in Western democracies such as Canada, the United Kingdom, France and Sweden. Although Australia will not be the first country, authoritarian or democratic, to implement internet filtering, the proposed filtering system has many unique features, separating it from other regimes.

Australia would have been the first western democracy to mandate internet filtering through formal legislation. ISPs would have been required legally to block illegal material. In countries such as France, Belgium, and Germany, courts have mandated ISPs to block hate speech and the illegal peer-to-peer filesharing of copyright protected materials.[i] In countries such as Canada and the United Kingdom informal government pressure led to voluntary internet filtering frameworks by the countries' major ISPs.

There is no Australian legislation yet on internet filtering, therefore, important details of the scheme are unknown. As Australia's filtering system has yet to be implemented, it stands to reason that its details, configuration and scope may change.

The criteria for evaluation of websites to be blocked remain equally uncertain and ambiguous. As it stands, the Clean Feed proposal had two tiers.

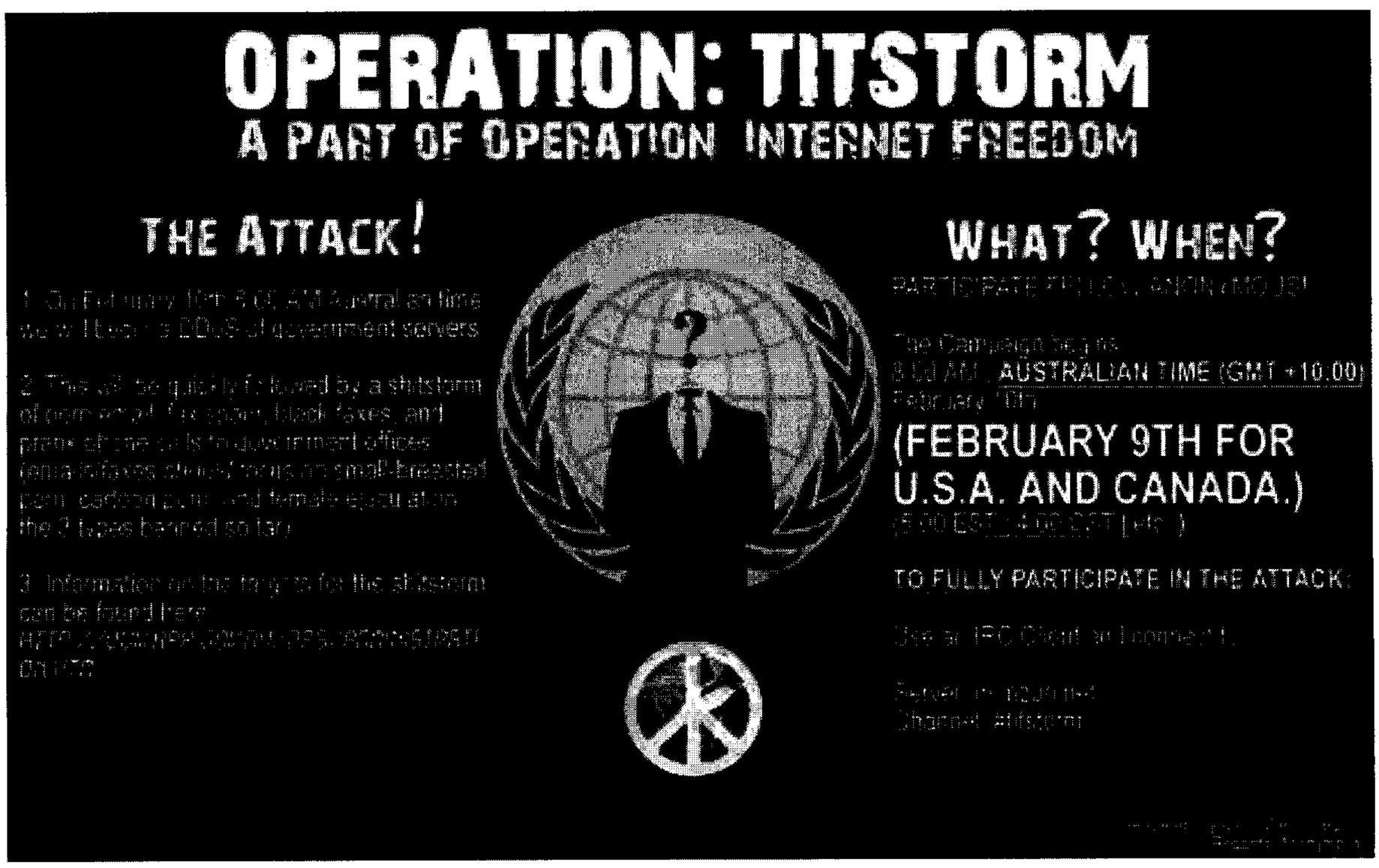
1) **Blacklist Filtering:** The first tier is an ACMA issued blacklist of 'child pornography' websites and 'other prohibited' materials to be blocked by Internet Service Providers at the URL level. The scope of 'other prohibited' materials in unknown. This will be mandatory for all Australians with no ability to opt-out of the scheme. Circumvention of the blacklist will be illegal. The blacklist will only block those URLs found on the ACMA Blacklist. It will **not** block websites with 'child pornography' and 'other prohibited content' found on:
   - Peer-to-peer systems (Eg. bit torrent, Winnie),
   - Encrypted channels,
   - Chatrooms,
   - MSN Instant Messaging;
   - Mobile phones, and
   - Unknown whether a blocked URL will block every website operating on a domain name or merely the specific offending material (Eg. www.youtube.com versus a specific video on www.youtube.com).

2) **Content Filtering:** The second tier will block types of materials which are legal but potentially unwanted. The scope of such material has not been delineated but examples would likely include adult pornography and other 'R' rated material – material inappropriate for children but clearly legal for adults. It remains unknown what types of filtering techniques would be used. Potentially these could include URL blacklists, deep packet inspection, peer-to-peer content inspection, and URL and http content inspection. Users will be able to opt-out as well as legally circumvent this type of filtering.

In response to the Australian government's decision to introduce a mandatory filter there were a number of offline marches and online acts of protest. One of these protests was the online defacement and DDoS attack of the Australian Parliamentary Website in 2010.

The Anonymous operation was dubbed Operation Titstorm (see **Figure 3** below). The operation saw the Parliamentary website taken down and images of penises and breasts were portrayed on the Parliamentary website's screen. Australians have a long history of both censorship and opposition to censorship. Unlike Canada, the United States and many parts of Europe, human rights are not protected in a Charter of Human Rights, Bill of Rights or within the Constitution.[21] The courts in Australia have less ground to strike down legislation that infringes civil liberties.

Figure 3 Operation Titstorm



As evidenced in the above figure, participation was clearly not limited to Australians. The campaign sought participation from Americans and Canadians as well.

[21] Cook et al 2011.

5.3 Motivations

Online civil disobedience participants are motivated by the same reasons as participants in traditional offline acts of civil disobedience. For example, consider the following offline and online acts of civil disobedience:

Sit-ins	Virtual Sit-ins
Barricades	Denial of Service Attacks & Website Redirection
Political Graffiti	Website Defacements
Wildcat Strikes	Denial of Service Attacks & Website Redirection
Underground Presses	Site Parodies, Blogs, Facebook Protest
Petitions	Web-Petitions (Eg. Facebook Likes)

The motivation is derived from a strong desire to protest that which is seen to be immoral, corrupt, undemocratic and above all, to send a strong message to ensure transparent governance. There is a strong link between the protection of civil liberties and online civil disobedience activity.

5.4 Main Targets

The main targets are the websites and databases of governments and organisations linked to government (Eg. Stratfor), including departments of defence, intelligence agencies and law enforcement. The other main target is organisations that are viewed as corrupt.

5.5 Relation Between Targets and Motivations

The main relation between motivation and targets is perception of the target behaving immorally. In many instances "immoral" means infringing civil liberties, whether this be freedom of the press, freedom of expression, or privacy. Police brutality is another common link between target and motivation. There are many videos of police brutality that are shown in Anonymous, LulzSec and CabinCr3w tweet feeds. For instance, there is a video on a Tweet Feed from January 3, 2012 showing the beating of a 15 year old by Harris, Texas police after the accused turned himself in.[22] It remains to be seen if the incident will gain popular consensus amongst Anonymous members to provoke protest.

In other instances, "immoral" is a combination of violation of civil liberties as well as more severe instances where tyrant governments stand in the way of democracy.

Not every possible event that could be received as "immoral" however qualifies for hacktivism action. This is a crucial point in that hacktivism movements require critical mass. Generally speaking, the stronger the cause, the more likely the action to be perceived as "ethical".

It must further be stated that there are many attacks which are being categorised as performed by Anonymous which don't appear to be linked to civil liberties or other types of political cause. One such example is the French hacker known as "Carl" who was arrested after he appeared in the French television program "Complément d'enquête" where he demonstrated that he had gained access to the French Army and Thales (security corporation that provides information systems to

[22] See http://twitter.com/#!/search?q=%23CabinCr3w

defence departments).[23] He has also stolen and used credit cards and bank account numbers to purchase personal possessions. Carl claims to be part of the Anonymous group. However, shortly after Carl's arrest, Anonymous issued a statement claiming that Anonymous does not associate with cybercriminals who use credit cards to benefit themselves.

5.6 Fundamental Principles of "Hacker-Ethics"

In hacktivism blogs and tweet feeds there are repeated references to pirates, Robin Hood, Billy the Kid, Ned Kelly, and famous civil disobedience activists such as Martin Luther King.[24] Members of groups such as LulzSec and other Anonymous affiliates, unlike earlier hacktivism groups in the late 1990s such as the Hong Kong Blondes (provided Internet access to ensure free flow of information in China) and the Cult of the Dead Cow, don't publish ethical hacking manifestos or similar documents. Ethical statements appear to be more limited such as "opening governments", "fighters for internet freedom", "exposing corruption", and so forth.

One interesting aspect, however is that Anonymous quickly issued a public statement after the French TV "Carl" incident disassociating itself with credit card and bank account theft for personal use. The post-Christmas operation to donate money to charity was orchestrated by members of Anonymous. The difference here is not one of whether or not personal information, and credit cards are copied, but how they are used. Under Anonymous culture, there cannot be a connection to self-benefit such as seen in the "Carl" incident. This is similar to the Sony incident where personal information and credit card numbers were copied, but this information was not used to purchase products or for blackmail purposes. There is a strong sense of Robin Hood tradition. What is equally interesting is that cybercriminals in Eastern Europe have also described their activities along the Robin Hood line where they will only steal money from rich Western countries, and then, only money from people who have more than a $1000 in their account.[25]

5.7 Perceptions of the Illegality of Activity

Unlike participants in hacktivism as will be seen in section 6, many participants in online civil disobedience believe their activity to be legal. They assume that a virtual sit-in or denial of service attack is a legitimate form of protest similar to regular picketing, barricading, protesting and sit-ins. Meanwhile, many users of the LOIC software are unaware that the software provides no anonymity even though they are participating in an act under the umbrella movement Anonymous. Many of the arrests of members of Anonymous were LOIC users. As will be seen in section 6, hacktivism as defined in this report, requires good computer skills and involves more than the ability to use LOIC.

5.8 Deterrence Effects of Case Law and Convictions

Online civil disobedience became popular in 2009. Since then there have only been a handful of arrests internationally. Whether pressure from law enforcement has a deterrent effect has not been the study of any criminological research yet – we may have to wait a few more years. Anecdotal evidence does yield some interesting observations.

With the case of Operation Titstorm, the arrested and convicted Matthew George has publicly stated that it was his first and last experience with online protests.

---

[23] Zorz 2011.
[24] *See for example* http://anonops.blogspot.com .
[25] Zenz 2008.

Arrests of LulzSec members in the US and the UK has had the opposite effect. Other members of the group as will be seen in section 8, have met the arrests with counter-attacks of law enforcement databases, and any organisation who they see as having aided in the arrest of these individuals. It is important to note that some companies such as Twitter have fought court orders to reveal account details and other information about their clients. The Twitter case against Wikileaks members is likely to be taken to the Supreme Court of the United States. Further, academics from around the United States will appear in a Senate hearing in the latter part of January 2012 to give evidence of the acute lack of transparency in the American regulation of Internet matters and they will express their concerns of a growing surveillance state.

In conducting interviews for this report, neither Samuel nor Dreyfus thought that hacktivism should be met with a heavy handed response. Samuel noted that the actions of Anonymous and similar hacktivists "were problematic when people with technical skills highjack the political process". Samuel herself has participated in a quasi/form of disobedience when she established a website which aggregated tweet feeds from around Canada displaying election results. Samuel, however, is quick to note that there needs to be legitimate room in politics to allow for virtual participation and virtual protests. Samuel, Dreyfus and I unanimously believe that governments should actively establish, publish and promote some form of guidelines for virtual protesting. Guidelines or a Code of Conduct is a priority recommendation.

5.9 Relevant Case Law and Convictions

Germany

In 2001 two civil rights activist groups, Libertad and "Kein Minch ist illegal" had called for protests against Lufthansa for their policy of helping to identify and deport asylum-seekers. There was an offline protest at the Lufthansa shareholders meeting. This was met with an online protest. The online protest consisted of a DDoS attack where over 13,000 people participated in the online attack temporarily shutting down Lufthansa's server for two hours (this is pre LOIC).[26]

One of the protest organisers, Andreas-Thomas Vogel, was convicted of coercion by a regional German court. On Appeal, the higher court found that there was no coercion under §240 of the German criminal law. They reasoned that there was no violence or threatening behavior. Further, the court reasoned there needs to be a permanent and substantial modification of data to be found guilty of incitement of alteration of data. The Court viewed the DDoS attack as a modern form of non-violent blockade fully within the right to freedom of expression. In Australia, a similar attack attracted comments from the court as falling within terrorist activity. There was no mention of freedom of expression or freedom of assembly.

Australian

Matthew George was an Australian member of Anonymous who participated in "Operation Titstorm". He was charged and convicted of incitement. The Magistrate stated that George had incited others to attack government websites and went so far as to liken his activities to cyber-terrorism – a claim that is truly outrageous given the context of the protest. George was given a $550 fine. George was not a ring-leader but merely a participant using LOIC software. Taken from statements made by George to the Sydney Morning Herald, he states:

> "We hoped to achieve a bit of media attention to why internet censorship was wrong ...
>
> I didn't think that I would ever get caught. I was actually downloading connections from other computers in America, so I didn't think the Australian government would be able to track me down."
>
> "I had no idea that what I was doing was illegal. I had no idea that there was incitement and it was illegal to instruct others to commit a legal [sic] act."[27]

There is an underlying theme here whereby many DDoS users do not realise that they are participating in an illegal activity.

5.10 Observations

The issues with online civil disobedience are in many ways the same issues as with offline civil disobedience. One commenter asks, "If a building is blockaded by protestors, is it civil disobedience or infringement on freedom of assembly? Is a book burning activism or censorship? Are causes

---

[26] Vendrath 2006.
[27] Whyte March 14, 2011.

more important than rights?"[28] There have been a paucity of cases addressing the issue; therefore, the issues are very much open for debate.

Critical mass is important as to which causes get taken up.

Which causes are taken up by a critical mass remain unpredictable.

6. Hacktivism

6.1 Description

Hacktivism was defined as the clever use of technology which involves unauthorised access to data or a computer system in pursuit of a cause or political ends. Hacktivism is more than the online equivalent of sit-ins and protesting which might be considered acts of online civil disobedience. Hacktivism still involves hacking for a cause, often political. Hacktivism, however, is taking that one step further from an online protest such as the collection and disclosure of personal emails, extortion or blackmail for a political cause.

Common forms of hacktivism include information theft (Eg. copy emails, account information, government documents, credit card information, viewing habits of Internet users – child pornography), virtual sabotage (SQL injection whereby content on the website is replaced with new content of the attacker), insertion of backdoor, and software development. The latter two require further elaboration.

It is often assumed that incidents of hacktivism and online civil disobedience are done in order to attract media attention to a cause. While that is true in many incidents, there is also a growing movement of silent activists who view the current political landscape as a long-term information war.[29] When security vulnerabilities are found in government and corporate databases, this information is kept secret. They are not looking for media attention, but wish to ensure that there continue to be backdoors available for accessing information. In some instances software or hardware is purposefully developed with a backdoor included in its coding for this purpose. In this instance, the software company and contractor are not aware of the default when the product is shipped out and received (Eg. surveillance software used by governments and corporations). This type of insertion of a deliberate vulnerability is performed by security experts working in the field. Their active participation in hacktivism is not publicized. They do not seek media attention and there are no media stories on their activities. Their goal is to fly under the radar. They possess the highest level of computer skills. This type of hacktivism has a particular focus on information related to democracy – censorship, government surveillance, and war efforts.

Software development is another critical form of hacktivism. The technologies used in Wikileaks for example ensure the integrity of the document, and the anonymity of the informant. Additionally Wikileaks has developed technology that allows people in non-democratic jurisdictions such as China a way to access their otherwise filtered content. Other hacktivism technologies include anonymisers such as the Tor proxy, and Track-Me-Not which allow people to view online content anonymously.

---

[28] Thomas 2001.
[29] Interviews with Wikileaks members. For example, Pilger 2012.

6.2 Case Studies

There are many instances of online civil disobedience spilling beyond into hacktivism. Two of the most interesting examples, however, are the Christmas charity donation drive by Anonymous, and the exposure of key officials linked to the neo-Nazi movement in Europe.

Anonymous Post-Christmas Charity Donations

The 2011 post-Christmas Anonymous attack targeted credit card information of the clients of U.S. based security think tank, Stratfor. In this instance, members of Anonymous were able to access and steal credit cards of Statfor's clients. Clients included members of intelligence agencies, law enforcement and Fox news journalists. The credit card numbers were later used to give away money as Christmas donations to charities such as the Red Cross, Care and Save the Children.[30]

According to Anonymous postings, the personal information, credit card details and emails of Statfor were not encrypted. This echoes a reoccurring theme of poor and sub-par security practices of large corporations, governments and even security think tanks entrusted with sensitive data.

Neo-Nazi Website

Anonymous claimed responsibility for an attack of a neo-Nazi website in Finland, and stole the information of the websites members then released it to the public. The list of members included a Parliamentary aide who later resigned from her post. It was later reported that Anonymous had issued a statement claiming:

> "We have no tolerance for any group based on racial, sexual and religion discrimination as well as for all the people belonging to them and sharing their ideologies, which is the reason why we decided to carry out last Monday's attack."

Similar types of attacks have been launched to reveal membership of child paedophilia groups, and organised crime cartels.

6.3 Motivations

There is no singular motivation at the heart of hacktivism. The motivation of such players may often not be well articulated, if articulated at all. There are, however, some reoccurring themes amongst many hacktivism activities. At the heart of all hacktivism is a sense of some sort of moral wrongdoing that either needs to be exposed and/or needs to be punished, and a wider sense of public loss of confidence in their institutions.[31] Many hacktivism activities expose corruption and/or humiliate the establishment.

Some hacktivists are motivated to expose insecure practices of corporations and governments handling personal information as seen in the Sony and Statfor attacks (see Section 7 and Appendix B).

---

[30] AnonOps Communications December 2011.
[31] Interview with Dreyfus and Samuel. *See also* Chiesa et al. 2009.

Most hacktivism, however, is related to a political cause. For example, many hacktivists are motivated by exposing censorship and surveillance of individuals by governments and corporations. Wikileaks, for example, has posted documents outlining the surveillance activities of governments around the world. Secret filtering blacklists of websites blocked by internet service providers on behalf of governments frequently find their way to the Internet. Other hacktivists target oppressive governments and enable the free flow of information in and out of areas where media coverage and access to local and foreign press is restricted. These include areas in Iran, China, Egypt, Syria, Libya, and include more local venues in the recent Occupy movements that are occurring globally. Other hacktivism efforts target underworld child paedophile websites and both the Internet Service Providers that host such repugnant content and the customers of this material. Religions such as Scientology have also been targeted with claims that such groups disseminate misinformation and have a corrupt hand in lobbying efforts of US governments.

Hacktivism and online civil disobedience are linked to empowerment and the strongest desire to find an effective public voice. This also applies equally to social media movements including online petitions. The motivation of much hacktivism is closely linked to whistleblowing. Generally, critical mass is important in determining which causes get taken up. In this sense it is very democratic. Hacktivism is not anarchy nor does it have a top down leadership which steers its course. Critical mass is required and generally speaking, the stronger the cause, the more likely any hacktivism activity will be seen as ethical. Equally important, however, is predictability. Dr. Suelette Dreyfus, expert researcher in both hacking, hacktivism and whistleblowing, indicates hacktivism targets are not predictable. Which causes are taken up by a critical mass remain unpredictable.

6.4 Main Targets

The main targets are the websites and databases of governments and organisations linked to government (Eg. Stratfor), including departments of defence, intelligence agencies and law enforcement. The other main target is organisations that are viewed as corrupt.

6.5 Relation Between Targets and Motivations

The main relation between motivation and targets is similar to online civil activism perception of the target behaving immorally. In many instances "immoral" means infringing civil liberties, whether this be freedom of the press, freedom of expression, privacy. Surveillance, intelligence gathering and contracting security firms to discredit hacktivist groups is currently a strong motive. In other instances, "immoral" is a combination of violation of civil liberties as well as more severe instances where tyrant governments stand in the way of democracy.

Many operations by LulzSec, however, are difficult to qualify as ethical hacking when the release of innocent third party personal information is disclosed on the Internet, and no motive other than "just for the laughs" is apparent in many of LulzSec attacks.

6.6 Fundamental Principles of "Hacker-Ethics"

Principles in hacktivism parallel those in online civil disobedience. When Anonymous member Barrett Brown (former journalist, and now Founder of the Project PM) was asked to comment on television whether the activities of Anonymous were ethical, he encouraged the public to make a comparison chart. Chart what is good versus what is bad about each Anonymous Operation then compare it with the issue that Anonymous sought to bring attention to. In other words, compare it with the actions of the traditional institution. For example, the actions of hacktivists must be

compared with Arab states' governments trying to 'turn off' the internet and to control social media; the treatment of WikiLeaks after publishing controversial information and continuing to assert its right of free speech; the heavy handed crackdown on the non-violent worldwide Occupy Movement by various regional and federal governments; and the lack of law around the shutting off of critical payment services as in the case of Mastercard and Paypal. Conversely, many hacktivism activities run the risk of being perceived as immoral, especially when personal information of innocent parties is released to the Internet.

Transgressive forms of hacking may be viewed as illegal yet ethical. It remains to be seen whether in 10 years time these same forms of transgressive hacking will become a legal part of the civil disobedience landscape.

6.7 Perceptions of the Illegality of Activity

Unlike many people who participate in online civil disobedience, participants in hacktivism are well aware that their actions are legal, and take precautions to ensure their anonymity online. As will be seen with online civil disobedience groups, many participants are unaware that using software such as LOIC to take part in a denial of service attack is illegal; they assume that it is a lawful protest. When hacktivists hack, copy, view and disclose the personal information of others they are clearly aware of that their actions are illegal and they have taken a calculated risk in spite of the threat of criminal sanction.

6.8 Deterrence Effects of Case Law and Convictions

Historical evidence shows that some hackers who are caught and later convicted of conspiracy or unauthorised use, will either give up such activities or use their talents in a legitimate matter such as working as a security expert or in some form of technology field. This is well documented in Suelette Dreyfus and Julian Assange's interviews with hackers in *Underground.* Raol Chiesa's work in *Profiling Hackers* also notes that the law offers deterrence to younger hackers (script kiddies) but not other levels of hacking. Both studies, however, reveal that the law offers no deterrence to future generations of hackers; the deterrence value is only individualised and is limited to the person who has been charged with a crime. Criminal prosecutions and convictions fuel the underworld of hackers and have the sole effect of driving the hacking world further underground, and have led to the development of many obfuscation technologies that make traceback to the source of an attack difficult (see section 9). As Dreyfus and Assange note, prosecutions and convictions have not had the message "don't hack" but, rather, have had the message of "don't get caught."

The studies that have been done to date, however, have been about hacking in general and not about ethical hacking. It is unknown whether the prosecution and conviction of ethical hackers will act as a deterrent sending the message, "ethical hacking is wrong" or whether such prosecutions will act as a catalyst to even more ethical hacking as a sign of protest. When members of Anonymous were arrested in the United States this past year, there were a series of attacks of law enforcement, news channels (FOX) and university websites as a form of public protest. Similar attacks were performed on security firms who contract with governments and corporations to attack Anonymous, LulzSec and Wikileaks. This is explored further in section 8.

6.9 Relevant Case Law and Convictions

Members of LulzSec and Anonymous have been arrested in the UK and the US, charges pending, and outcomes unknown at this time.

Nineteen year old Ryan Cleary was arrested in Essex in the United States and has been charged under the Computer Misuse Act for his hacking effort of the UK's Serious Organised Crime Agency. He is also alleged to have broken into many other law enforcement agencies both in the United Kingdom and the United States. Cleary is said to be a member of LulzSec. Cleary is said to suffer from agoraphobia and he has been diagnosed with aspergers and attention deficit disorder. Similar cases against hackers in the United Kingdom, Australia and New Zealand in the last ten years have involved people addicted to computers, those who suffer from agoraphobia and others who have autism spectrum disorder or attention deficit disorder. A hacker who went by the handle Wandii was acquitted on all counts of computer misuse in the United Kingdom due to a computer addiction.[32] A 19 year old New Zealand hacker, Owen Walker was brought up on several charges of computer misuse. The first charge was under s. 252(1) of the New Zealand *Crimes Act 1961* with accessing a computer system without authorization. The second charge related to interfering with a computer system under s. 250(2)(c) of the *Crimes Act 1961*. The third charge was the use of a computer system for dishonest purpose under s. 249(2)(a) of the *Crimes Act 1961*. Lastly, under s. 251(a) and (b) for possession of software for the purpose of committing a crime. Walker pleaded guilty to all charges. He could have been sentenced to up to 16 years of imprisonment under the four offences that he was charged with but was instead discharged without conviction, and was ordered to pay $9 526 NZD in reparation as well as to relinquish any assets acquired as a result of gains he achieved through use of his botnet.[33] The court noted that Walker committed the crimes over a two year period when he was aged 16 to 18. The court heard evidence of Walker's difficulty in socializing due to having Asperger's syndrome. Walker now works in Melbourne, Australia for Telstra (the largest telephone and Internet Service Provider in Australia). There has been no study that has looked at the link, if any, between agoraphobia, aspergers or attention deficit disorder and hackers.

Arizona college student Cody Kretsinger, alleged member of LulzSec, was arrested and charged with multiple counts of conspiracy and unauthorised impairment of a protected computer in the United States for allegedly hacking Sony Pictures Entertainment. The hacking is said to be that of Sony's computer system, which was compromised in May and June in 2011. LulzSec, unlike Anonymous, performs hacks both for political reasons and "just for fun" or "just for laughs" (lulz is computer slang for laughs). LulzSec has not formally announced any political reason for the Sony hack. Interesting, however, are the many media comments and blog responses that sympathise with LulzSec and find the lapse security measures of such corporations to be the worst offender. As one blogger writes:

> "The main offender here is Sony. They were fully aware of the vulnerability of their current system. They were just too lazy to fix it. All it took was a Google search and some script kiddies entered in one SQL line and broke into the system. This wasn't a "zero day attack," it was a well known vulnerability to their system that was public. It's like having a stack of money just behind a gate with no lock. All it takes is one simple well known action and you are in. Why do you think class action lawsuits were charged against Sony if it wasn't their fault?"[34]

Other members of LulzSec have been arrested and detained in Italy, Switzerland, and the United States for computer offences for hacking a number of different websites. It is much more difficult to see any public benefit or ethical conduct in many of LulzSec's operations, other than the media coverage exposing the poor security habits of most corporations and governments. Security experts have been urging companies and governments to improve their outdated and insecure protection of

---

[32] Dreyfus and Assange 1997.
[33] *R. v. Walker*, HC HAM CRI2008-0750711 [2008] NZHC 1114.
[34] Herpderp1189, Huffington Post January 5, 2012

their systems for decades. During the last decade, however, many corporations still don't use basic encryption to protect personal information of their customers, nor do they adequately protect their own assets. The LulzSec attacks may act as a catalyst for corporate improvement to security.

6.10 Observations

At the heart of all hacktivism is a sense of some sort of moral wrongdoing that either needs to be exposed and/or needs to be punished, and a wider sense of public loss of confidence in their institutions – even if the actions of LulzSec are poorly articulated if at all (the membership of this group seems to be confined to young males unlike the membership of Anonymous with participants of all ages and walks of life).

Hacktivism and online civil disobedience are linked to empowerment and the strongest desire to find an effective public voice. This equally applies to social media movements such as online petitions.

The motivation of much hacktivism is closely linked to whistleblowing.

7. Penetration / Intrusion Testing and Security Activism

7.1 Description

Penetration/Intrusion Testing is a type of information systems security testing on behalf of the system's owners. This is known in the computer security world as "ethical hacking". There is some argument, however, as to whether penetration testing must be done with permission from a system's owner or whether a benevolent intention would suffice in the absence of permission. Whether permission is obtained or not does not change the common cause, that of improving security.

Most penetration or intrusion testing occurs when a security expert is hired to test the security of an organisation's network. In this sense, the security expert has permission to hack into the organisation's network such that the law will view this as authorised, thereby not attracting criminal sanction. The legal ambiguity arises when these same security experts stumble across security vulnerabilities, then actively investigate further without permission or authorisation from the system's owner. It is only this latter form of act which would be considered as legally and morally ambiguous thus qualifying as ethical hacking.

Security Activism is similar to penetration/intrusion testing in that the cause is to improve security. Security activism goes beyond mere testing of security, however, to gather intelligence on crackers, and to launch active attacks to disrupt criminal online enterprises. A good example of security activism involves botnet tracking and takedown.

These two types of ethical hacking are considered here together as they share similar if not identical attributes in motivation, cause, and techniques.

7.2 Case Studies

Australian White Hat Security Expert Patrick Webster

Australian security expert Patrick Webster was threatened with legal action and criminal charges for disclosing a serious security flaw in First State's Superannuation System.[35] When Webster went to log into the First State system to check on his superannuation he noticed that the URL contained his individual identity information linking to his superannuation account. He found this odd, and investigated further, Patrick ran a simple for loop script to check for other anomalies. The script started with the scan of one account number then continued to scan by incremented numbers. In the time that it took to initialise the script (computer program), make tea and come back to the computer, the script revealed hundreds of megabytes of account numbers. Upon seeing this, Patrick ascertained that potentially every account was exposed to the Internet. He quit running the program. In the scanning time, the script automatically saved the details of the first 500 accounts.[36]

Alarmed at this security flaw, Webster notified the information technology personnel at First State Superannuation. Some of the IT staff sent him emails thanking him.[37] However, the Chief Information Officer and others at First State Superannuation reacted differently alleging that by accessing not just his own account but the accounts of others he had committed a crime. Webster was served with legal papers and was told that the police might press charges against him. What is more alarming is the fact this security flaw should have been picked up through basic security compliance checks. It is further alarming that over 770 000 FSS accounts were vulnerable, as well as the details of another 1.2 million accounts from other companies who outsourced their data storage to Pillar Administration. The alarming rate of corporations having their data compromised has sparked Data Breach Notification laws around the globe yet corporations and organisations still have not implemented many basic security mechanisms. First State Superannuation is reviewing its data storage contract with Pillar as well as its own personal handling of personal information.

It has become standard industry practice to thank and often reward those individuals who alert companies to security flaws. Corporations such as Facebook and Google send their thanks and offer a small reward. Anti-virus and anti-spyware companies also pay money for zero day threats. In this instance, however, First State's reaction was to threaten Webster with civil and criminal proceedings if he didn't turn his computer over to the IT personnel at First State for them to verify that he had deleted the information from those 500 accounts.[38] The charges were later dropped. This incident has set off alarm bells for security researchers in Australia and perhaps even abroad.

In the words of Patrick Webster:

> "I am genuinely disappointed the government legislation will not provide safeguards for security researchers, though I am not the least bit surprised.
>
> I've encountered clients who are actively being attacked by a compromised legitimate website and considered counter attacking in self defence to protect my client and the comprised organisation... I haven't, but it would be nice if we could.

---

[35] Moses 2011.
[36] Email correspondence with Patrick Webster.
[37] Grey 2011.
[38] Grey 2011.

> My only hope is that my incident with First State Superannuation sets a precedent for future researchers. Obviously not in Australian law as the NSW Police stated that no laws were broken and I was providing a civil duty, and Minter Ellison halted proceedings, but with any luck the media attention will convince corporations that not everybody is acting with malicious intent. If it helps just one researcher in the future I'll be happy."[39]

The incident is a timely reminder of the lack of legitimate exemptions for security research.

Botnet Removal Communities

There exist a number of undocumented small independent research communities that were (or still are) actively involved with botnet harm mitigation, interdiction, counter-attack and take-down. This may include attempts by the command & control (C&C) source to program and re-program its bots, altering payloads of malicious applications delivered on botnets, and launching a denial of service attack on C&C servers.[40] Offense-in-Depth Initiative (OID) was launched in 2008 as a small group targeted approach to fighting cybercrime. OID is comprised of volunteers who work within smaller subset groups dedicated to botnet countermeasures. Each subgroup specialises in one particular botnet. So, for example, there was the OID-Kraken and OID-Torpig small working groups targeting the Kraken and Torpig botnets. The main goal of the OID teams is to erode the profit model of specific major cybercriminals, while obtaining intelligence for use by law enforcement.[41] Each specialist subgroup divides their roles into reverse-engineer operations specialist, coder, social-engineer linguist and information warrior. In some instances the same person could fulfil multiple roles, and in other instances the roles are somewhat superficial.

The group's aim was to form small working groups singling out one botnet or criminal operation with the purpose of long-term disruption *(Note: the group has disbanded and no longer performs botnet takedowns).* Other small independent research groups have performed counter-measures for a few weeks or a month, then the countermeasures stop, allowing the criminal operation a chance to regroup and get back to "business as usual."[42] OID's focus was on long-term countermeasures aimed at disrupting the profitability of the botnet operations. Whether a cybercriminal continues operating depends on many factors. OID has singled out three major factors: complexity of the operation, risk of getting caught, and reward/profit of the crime.[43] OID uses methods aimed to increase the complexity of the criminal's organisation, forcing them to spend more time, effort and money into maintaining their criminal operations. For instance, techniques include subverting the command and control or by either increasing or decreasing the size of the botnet. There has been some research done on optimal botnet size for certain types of activities.[44] Compromised machines can be remediated so that they are no longer part of a botnet. If you remediate enough machines, the size of the botnet becomes untenable for criminal operations. Likewise, if you grow a botnet from 100 000 to 10 000 000 it becomes very difficult to effectively manage the botnet without constantly writing new instructions for the command and control. The botnet master ends up spending extraordinary amounts of time and effort to control the bots. Just as one person may only successfully tend to a set amount of sheep or cattle within a set amount of land, an increase in the size of the herd requires more land, water, and labour. Similar to caring for livestock, taking care of botnets is often referred to as "herding" bots.

---

[39] Email correspondence with Patrick Webster.
[40] Smith 2005.
[41] Observations from email orrespondance with members of the OID Initiative.
[42] ISOI is one such group. Members complained of the unfocused, ad hoc short-term approach of ISOI.
[43] Observations from founder of OID in listserve correspondance.
[44] Li, et al. 2009.

When a botnet's operations are interrupted it may create the need for more complex operations in order to adapt to the new environment. In the case of botnets, if the complexity becomes too great for the criminal, more expertise may be needed in the form of hiring a programmer to develop new encryption methods or programs. It is believed that, in turn, this forces the cost of business to rise. It is hoped that if the disruption is continuous, and that costs of doing business rise so that profitability will be reduced, then this will correspond with a lower level of criminal activity. There is no evidence to suggest that this has worked to date. Botnet activity remains a growth industry. Nonetheless, this is the belief of groups such as OID. As stated in the OID mission, it is about long-term disruption. It may be too early to ascertain whether such countermeasures are effective.

OID tactics are decided by looking at effectiveness, stealth, ethics and ability to avoid collateral damage to third parties. Such an approach to tactics is not an official code but represents a rough understanding between members of the group.[45] Ultimately what tactics are used depends on the decisions of the specialist group. While the operations of the OID groups are not openly discussed, many of its operations have involved working with select individuals working for computer security companies. Such companies, unlike OID, often will make available to the public information on botnet infiltration and countermeasures taken against a botnet. This was the case with the Kraken botnet, which OID members infiltrated and took down in December of 2008. OID members have not publicly discussed how the botnet was taken down. Researchers with the security corporation, TippingPoint, however, have provided publicly available information about the Kraken botnet and infiltration process available from their security blog.[46]

Researchers at TippingPoint infiltrated Kraken by starting with a sample of the code provided by Offensive Computing. The various protocols of the botnet were noted. The command and control instructions were encrypted. Researchers had to reverse engineer the computer code which entailed decrypting the encryption routes. TippingPoint created a fake server (sinkhole) to redirect Kraken traffic. TippingPoint played a somewhat passive role in that they did not rewrite instructions and send alternative instructions via the command and control. In their words, "we are not talking back to any of the Kraken zombies that are phoning home to us. We are simply listening passively, decrypting the request and recording statistics."[47] As such they were able to then redirect traffic to their server (often referred to as a sinkhole). Researchers at TippingPoint recorded the list of all uniquely infected IP addresses and applied a reverse DNS lookup to ascertain what types of computers and locations of IP addresses were part of the botnet. The majority of the compromised computers were home broadband users with compromised machines predominantly based in the USA, Spain, United Kingdom, Colombia, Mexico, Peru and Chile.[48]

TippingPoint wrote an update code capable of cleaning up the compromised computers of Kraken. They have even provided a video demonstrating their capability of removing the Kraken botnet altogether. TippingPoint researchers have not cleaned up the botnet for ethical and legal reasons, chiefly that there is no security research exemption.

7.3 Motivations

Self-organised security communities recognise that there is great need for action to alleviate some of the non-functionality in an attempt to reduce cybercrime. When viewed in this light, the work of

---

[45] Observations from listserve correspondance.
[46] TippingPoint.
[47] TippingPoint.
[48] TippingPoint.

self-organised communities may be seen by those involved with these communities as an act of "doing justice" where justice has otherwise proven to be non-functioning.

The motto "to do justice"[49] is potentially applicable to both self-help security communities and botnet communities. There is, for example, mounting evidence that Eastern European communities have likened internet crime such as fraud to a legitimate activity – Robin Hood stealing from the rich Western countries to give to the poor developing nations. Many types of malware and botnets for hire are now distributed with end-user license agreements and some have even been registered for copyright protection. Conversely, anti-botnet communities have justified breaking the law where required to achieve justice. The motto "to do justice" parallels the actions of many self-organized security communities who are "fighting malware and botnets" under the motto of "doing justice" in the absence of effective regulatory response to the problems. In fact, regulation may never effectively deal with botnets. The point is, rather, that the perception of the absence of regulation or the presence of ineffective regulation motivates people to take matters into their own hands.

7.4 Main Targets

Main targets vary for security activists. In some instances the target might be simply to gather intelligence in a honeypot. In other instances, it may mean actively taking down a botnet, or removing malware from infected websites, or sending information to companies whose security has been compromised, to collecting information and handing it over to law enforcement.

7.5 Relation Between Targets and Motivations

Targets are either performing illegal criminal functions (running a botnet, stealing credit cards) or they are organisations whose security practices are poor (and often not fully compliant with security standards). The underlying link between target and motivation is inept security and the ability to exploit vulnerabilities.

7.6 Fundamental Principles of "Hacker-Ethics"

Security activists almost always have excellent computer skills. There is no one set of hacker ethos that applies to any group of hackers though anecdotal evidence and in the opinion of Dr. Suelette Dreyfus (interviewed), expert security activists share a common set of ethics that can best be described as responsible engagement.[50] This does not, however, imply that all actions are within the law. Security activism and research is a grey and murky area of the law.

7.7 Perceptions of the Illegality of Activity

It is difficult to qualify or quantify perceptions without empirical research. Nonetheless, my observations from my research and with interviews of cybersecurity experts is that they are highly skilled individuals who are acutely aware that what they are doing is illegal in many jurisdictions but view their activities are necessary and ethical. For example, university researchers investigating the Torpig botnet invaded the privacy of those individuals whose computers had been compromised in order to gain intelligence about the botnet propagation trends.[51] They did so without consent of the

---

[49] Tamanaha 2001.
[50] Chiesa et al. 2009.
[51] Torpig.

computer owner and in clear violation of the law. Law enforcement was notified of these violations and did not press charges. If anything, they condoned the actions.[52]

7.8 Deterrence Effects of Case Law and Convictions

As a general proposition, security activists are not deterred by the law; if anything the law turns a blind eye and encourages ethical hacking for these purposes. Security researchers are imperative in any initiative to combat cybercrime. For example, there has yet to be a single takedown of a botnet that didn't involve cooperation from a number of entities including security researchers from specialised security software companies and universities, Internet Service Providers, Domain Name Service Providers, and often law enforcement – often these parties are located in different parts of the world.

7.9 Relevant Case Law and Convictions

There have been few incidents where security activists have been the target of criminal investigations though there have been many security researchers who have been threatened with criminal sanction. There have, however, been several instances of civil law suits against security activists. Two of these civil (quasi-criminal) cases are discussed below.

Spamhaus Project

Spamhaus Project, an organisation of volunteers in the computer industry, composes blacklists of some of the worst spam propagators to aid ISPs and businesses to better filter spam. The company E360insight.com sued Spamhaus Project in the Northern District of Illinois Federal Court alleging it was a legally operating direct marketing company and should not be blacklisted as a spam provider. Spamhaus did not file a response and did not appear before the court. As such, the arguments presented before the court were unilateral such that the court issued a default judgment.[53] The court ordered Spamhaus to pay $11.7 million USD, to post a notice that E360 was not a spammer, and ordered that the Spamhaus Internet address be removed from the Internet Corporation for Assigned Names and Numbers (ICANN). Spamhaus ignored the ruling, did not pay the money, and did not post a notice on its website that E360 was not a spammer, nor did ICANN remove the Spamhaus website from its root server. In a similar situation, the anti-virus and anti-spyware company Symantec was taken to court in California by a company which it defines and reports in its services as spyware. Hotbar.com claims that the classification of its software as spyware is in violation of trade libel laws, and constitutes interference with contract. The suit was reported as settled with Symantec agreeing to classify Hotbar as 'low risk'.[54] A series of cases of a similar nature have been filed and heard between 2005 and 2009, with most settling.[55]

---

[52] Torpig.

[53] E360 Insight, LLC et al v. The Spamhaus Project US District Court, Norther District of Ilinois, 13 Deptember 2006 (Case no. 06 C 3958). Access to default judgment at http://www.spamhaus.org/archive/legal/Kocoras_order_to_Spamhaus.pdf.

[54] Messmer 2006.

[55] 1-800 Contacts v WhenU., 1-800 Solutions v. Zone Labs, Cassav (CasinoOnNet) v Sunbelt Software, Glaria (Gator) v Internet Advertising Bureau.

Sierra vs. Ritz

The US trial court decision of *Sierra v. Ritz*[56] involved unauthorised use of a domain name system zone transfer. Zone transfers are, generally speaking, open access public information. They provide data about all of the machines within a domain. Without zone transfer, you would literally have to type in an IP (internet protocol) address every time you went to a website – it is one factor contributing to the convenience of the Internet. The information may be retrieved by the use of 'host command' with the 'I' option. Zone transfers contain public information to varying degrees depending on the protocols used by an organization. Zone transfers may be disabled to the greater public with only trusted machines and senior administrators having access on a 'need to know' basis. This is a form of limited authorised public access. In Sierra's case, the zone transfer was more widely available in the sense that the system allowed zone transfers to everyone, thereby publicizing potentially private data into a public forum. There would be no way for a person accessing the zone transfer in the latter context to know whether Sierra was truly allowing shared access or whether it was merely a mis-configuration. From a technical perspective, this is a situation of authorised access to the information found in the zone transfer. From a legal perspective, the judge ruled that access was unauthorized with a large emphasis placed on the defendant's intention to obtain and divulge information found in the zone transfer.[57] David Ritz is a well-known anti-spammer. There has been debate as to whether Sierra has facilitated spam in the past. Neither of these two facts appeared to weigh into the decision. While *Sierra v. Ritz* is a civil suit, Ritz has been criminally charged with unauthorised access to a computer in North Dakota. Although the charges were later dropped, Ritz lost the civil suit and court reasoned that "Ritz's behaviour in conducting a zone transfer was unauthorized within the meaning of the North Dakota Computer Crime Law".

The case illustrates how the terms 'unauthorised' and 'access' do not produce a similar set of shared assumptions in the technical, legal or ethical fields. A technical researcher may falsely assume that they are operating within safe legal parameters only to discover that such parameters do not translate across fields. The technical researcher would likely assume that he/she is authorised to perform an act where technical protocols and programming convention allow for it. From a legal standpoint, authorisation and consent involve a number of factors including intention, damage, and the bargaining position of affected parties. One commentator on the decision noted that it is the equivalent of, "Mommy, *can* I have a cookie? Sure you can have a cookie, but you *may* not."[58] The case foregrounds a recurring theme: if a user interacts with a server in a way that the protocol does not prohibit but which is upsetting to the server's operator, should this be construed as "unauthorized access" as a matter of law?[59] The scope of unauthorized access in computer fraud statutes is an old question.[60] Whether or not this would constitute a "hack" is one question, and if it is a "hack" then surely the motives appear to be somewhat ethical.

7.10 Observations

Exemption from liability and criminal prosecution has been argued for application to security researchers, and for acts that threaten to cross technical and accepted protocols. A resounding

---

[56] The judgment is unreported. A copy of the decision is accessible from private list-serves as well as from the webpages of SpamSuite.com. *Sierra Corporate Design Inc. v. David Ritz*, (2007) District Court, County of Cass, State of North Dakota, File No. op-05-C-01660 *See* www.spamsuit.com.com/node/351.

[57] A detailed analysis of the case can be found on SpamSuite.com available at http://www.spamsuite.com/node/351.

[58] Rash 2008.

[59] Original idea expressed by Paul Ohm in the cyberprof list serve.

[60] Kerr 2003.

question underlies the debate: do the ends justify the means? Some examples might include the Recording Industry's proposal to hack into users' computers to find infringing material and cyber-activists placing Trojans on child pornography to track and record the contents of offenders hard-drives for evidential purposes. These examples go to the question of intent as well as whether or not an act may be justified as social utility for the good of the public similar to how public interest exemptions work for the admissibility or otherwise inadmissible evidence in court.

For example, if one argues that David Ritz has indeed accessed the zone transfer without authorization, inevitably one must question his motive, intent and whether such activities were performed in the public interest. Peering into the zone transfer to document illegal spamming activity may indeed be in the public interest. If one successfully concludes that no unauthorized access was performed due to the public nature of the zone transfer and DNS, it seems equally perverse to not consider motive and intent. By way of analogy, if I have equipment to make false passports along with a stack of 200 shell passports (no photos or false names inserted), the trajectory towards the commission of a crime is called into question. Accessing information in the zone transfer for illicit purposes should attract attention, if not a penalty. The implication, however, of criminalizing an act of accessing publicly available information without illicit intent, calls into question the utility of 'unauthorized access' provisions. The inconsistency of the courts' interpretation of 'unauthorised access' makes the use of the provision unpredictable as well as malleable to prosecutorial will. The scope of 'unauthorized access' is ripe for reconsideration and debate.

There is no public interest exemption for computer offences. A public interest exemption refers to unauthorised access, modification or impairment where it is in the public interest to break the law. Typically, this might relate to security research but there are other instances that go beyond mere research which may justify the law being broken. There are reasons to allow for a public interest exemption. However, in my opinion these reasons are not sufficiently compelling at this point in time as to open up the exemption beyond security research. The idea of a public interest exemption, however, should be given further consideration by governments.

8. Counter-Attack

8.1 Description

Counter-Attack is also referred to as hackback or strikeback. Counter-attack is when an individual or organisation who is subject to an attack of their data, network or computer takes similar measures to attack back at the "hacker/cracker".

Counter-attack also refers to a self-help measure used in response to a computer offence. In most instances computer offences refers to an act that is or has already occurred such as a cyber attack (Eg. deliberate actions to alter, disrupt, or destroy computer systems), or specific types of cyber attacks such as unauthorised access or modification to data or computer system (Eg. this may merely mean accessing a computer system), installing malware onto a computer system, or launching a denial of service attack.

Consider the example of a denial of service attack launched against a corporation's website. A botnet has been used to launch the DDoS. The corporation would have several options to pursue:

1. Implement passive measures to strengthen its defensive posture (Eg. upgrade security software, firewalls, and training to staff).
2. Report the cyber attack to law enforcement authorities, and leave it to the law enforcement authorities to take appropriate action. If the DOS attack has been done for blackmailing purposes, the corporation may elect to pay the sum.
3. Do nothing and wait for the attack to be over. Purchase insurance against cyber attack to mitigate against future attacks.
4. Contact a third party specialising in cyber attacks to assist in the matter (Eg. AusCERT, SANS Institute, National Cyber Forensics and Training Alliance).
5. Take self-help measures to gather information and investigate the source of the attack with the view of mitigation of damage and traceback to the source
6. Take actions to actively neutralize the incoming attack through forms of counterstrike such as a counter of denial of service attack

Often an organisation will use a combination of options in dealing with the matter. Mitigation of damages is the key priority of most corporations when under cyber attack.[61] The most important component in mitigating against damage is protecting assets not already compromised. This could mean protecting data that has not yet been stolen. This could mean stopping the denial of service attack as soon as possible through various means – technical measures, paying a bribe, or launching a counter denial of service attack. Damage control may also mean ensuring that there is no media attention to the matter in order to keep stock prices from falling. Corporations and organisations are taking self-help measures such as counter-attack.

8.2 Case Study

LulzSec, Mastercard & Paypal, and Barr

The Lulzsec DDoS attacks against Mastercard and Paypal were motivated by the treatment of Mastercard and Paypal's refusal to accept online donations for the Wikileaks situation. Someone (perhaps members of the Mastercard and Paypal team, or perhaps other security researchers upset with Wikileaks) launched a counter denial of service attack at the LulzSec website. One DDoS attack was met with a counter-attack.

Additionally, law enforcement were on the hunt for the members of LulzSec who had launched the attacks against Mastercard and Paypal. During this time, security researcher Aaron Barr, CEO of HBGary Federal, was privately investigating the matter and claimed that he had identified the members who had performed the attacks, and had proof of the matter. Aaron Barr's emails on the matter were leaked to the Internet and may be found on a number of websites.[62] According to the leaked emails, Barr used Internet Relay Chat (public channel) to obtain the handle names of those members involved in the attack. He then used social media such as Facebook and LinkedIn to allegedly look at friends and family of the hacker group. He then made inferences to the point where he claimed he had identified members who launched the attack. Members of LulzSec retaliated claiming he had put many innocent individuals in danger. If Barr had indeed used social media to retrieve this information, his methodology remains unclear. Most people are unable to view one's Facebook account unless they befriend them. There are, however, methods to hack into a Facebook account without authorisation.[63] It is likely that Barr had indeed accessed this information without

---

[61] Email correspondence with Ron Plescoe, Director of the National Cyber Forensics and Training Alliance (NCFTA). *See also* Purdy 2009.

[62] For example, the emails are provided on The Old Computer at http://www.theoldcomputer.com/blog/index.php?start=60

[63] AusCERT 2011 presentation.

authorisation. Members of LulzSec responded to Barr's claims by allegedly copying 40,000 emails and making it available on piratebay, launching a denial of service attack to his company's website, and posting the message, "now the Anonymous hand is bitch-slapping you in the face".

According to the UK newspaper The Guardian, the exposed emails from HBGary revealed that they, along with security firms Palantir and Berico, "were discovered to have conspired to hire out their information war capabilities to corporations which hoped to strike back at perceived enemies, including US activist groups, WikiLeaks and journalist Glenn Greenwald."[64] An interview with Dreyfus revealed a similar theme of corporations and governments engaging "cowboy security firms" to perform attacks either directly on hacktivism websites and other targets. Dreyfus also revealed that there were several recent attacks performed by cowboy security firms who have made it look as though such attacks came from Anonymous. The contracting out of intelligence services, "for hire cyber-attack services" by governments to security firms was also exposed in the Canadian television program The Agenda.[65] Identifying attack sources is a difficult proposition as will be seen in section 9."

8.3 Motivations

Counter-attacks are launched as a form of self-defence or as a means of retribution. The LulzSec and Paypal example certainly highlights the retribution motive. However, most organisations perform acts of counter-attack as a form of self-defence. In 2001, researchers surveyed 528 IT managers in Western Australia and Victoria to obtain their views on counter-attack. Those surveyed were asked a variety of questions including whether strike-back should be allowed if their organisation was subject to an attack (65% replied yes, 30% no, and 5% were undecided).[66] This question was then broken down into specific types of attacks such as attempt at network access and attempt to destroy or alter data where the yes response rates increased to ranges between 70% and 93%.

8.4 Main Targets

The main targets are the IP addresses (often websites or computer) that initialise the attack. Information may also be gathering and collected where possible of those individuals who perform the attack though this is often very difficult to trace as will be seen in section 9.

8.5 Relation Between Targets and Motivations

Again, the motivation is either to defend or retaliate against the origin of the attack. The target is normally a website, and does not typically involve the individual per se behind the attack (because identification is often difficult).

8.6 Fundamental Principles of "Hacker-Ethics"

There are a variety of ethical and moral issues at play with counter-attack. One principle could be seen as defending one's property against attack. The other main principle is retribution. There appears to be an additional principle of hacking to discredit an organisation, typically by deliberately launching an attack to make it look as though it has come from another organisation. There appears to be foul play by most parties involved with hacktivism counter-attack.

---

[64] Huffington Post October 2, 2011.
[65] The Agenda, October 25, 2011
[66] Hutchinson, et al. 2001.

8.7 Perceptions of the Illegality of Activity

There is no consensus as to whether corporations and organisations engaged in counter-attack are aware of the illegality of their activity. Some security software will automatically initialise a counter-attack whereby the organisation may or may not be aware. It may be the case that those individuals running the security of the organisation are aware of the illegality of the action, but that the Board of Directors is kept in the dark. There is also evidence that many organisations employ former black hat hackers under strict control and surveillance yet this type of arrangement is rarely publicised.[67]

8.8 Deterrence Effects of Case Law and Convictions

Unknown and untested. There are no cases against a corporation or organisation that has engaged in counter-attack.

8.9 Relevant Case Law and Convictions

None. In section 5 it was noted that there are ongoing investigations, and arrests had been made against two members of LulzSec for participation in the Mastercard and Paypal attacks. There has been no public investigation nor charges laid against those responsible for the DDoS attack against the LulzSec website. Furthermore, there has not been a public investigation made or charges laid in relation to how Aaron Barr obtained his supposed information of members of LulzSec through social media. There have not been any arrests made for those members of LulzSec/Anonymous responsible for releasing Aaron Barr's personal email, and for the DDoS attack of his website. It would appear that investigations and charges are highly, and perhaps unfairly, discretionary in this area of law.

8.10 Observations

Self defence may apply to some forms of counter-attack. There are no cases that deal with defending oneself against an online attack. There is likewise little literature on the topic. In this instance the Australian Model Criminal Code (MCC) provides guidance as to the scope of self-defence in such situations. The MC discussed at length the growing trend in the United States for corporations' use of computer software with counter-strike abilities. The MC stated that:

> "It is possible that the defence of self-defence in Chapter 2, s.10.4 of the Model Criminal Code might extend to some instances of computerised counterattack against cybernet intruders. Self-defence includes conduct which is undertaken "to protect property from unlawful appropriation, destruction, damage or interference". It is possible that a strikeback response to the hacker's attack could be characterised in this way.
> In practice, counterattack involves serious risk s since hackers are likely to adopt precautions which divert the counterattack to innocent third parties.
> It is apparent that principles of self defence of persons, which extend without undue strain to include protection of tangible property, are inadequate for the purpose of regulating computerised counterattack against hackers. The familiar concepts of necessity and reasonable response, which excuse or justify counterattack against physical threats, are next to useless as guides in this field."[68]

---

[67] For example, former botnet master Owen Walker is now employed by Telstra. *See* Maurushat 2011.
[68] MCC, note 5 above, page 108.

The MC committee concluded that "legislative intervention would be "premature". They further noted that corporations who resorted to self-help / hackback "would be left to the uncertain promise of a merciful exercise of prosecutorial discretion."[69] The concluding sentence provides even more ambiguity to the MC where it is stated:

> "The familiar criteria of necessity and proportionality which govern self defence in other applications have no obvious application here. Reliance on a test of what is or is not reasonable in the way of counterattack against hackers would place an inappropriate legislative burden on courts to determine issues of telecommunications policy."[70]

The conclusion seems to echo a recurring theme of "This is a tough one so let's wait and see." The MCC declared that legislation was premature and that courts should not be the ones to determine issues of telecommunications policy. So who should make these determinations? The reality is that individuals and corporations are making these determinations as a matter of internal policy. An anonymous survey on self-help/hackback measures was put to the attendees of the AusCERT 2009 conference. Over 20% of the audience indicated that their corporation or organisation used hackback. Another 25% stated that their corporations are currently considering the use of hackback[71]. In closed conference sessions with Chatham house rules, chief information officers from banks, internet service providers, Internet auction sites and Internet payment companies have all indicated that they employ blackhat hackers whose work is closely scrutinized. Counterstrike against a denial of service attack was a common hackback method – some hackback was performed with authorisation from the Board of Directors, but mostly circumstances are kept quiet and unreported to the Board of Directors.[72] However, the report came out in 2001 and the prevalence of self-help remedies may not have been the same as it is in 2012. There have been no Parliamentary statements since 2001 on hackback.

9. Technical and Legal Challenges in Investigation and Prosecution

There is often a false belief amongst law makers that if the right legislation is enacted and if enough resources are allocated to the task that law can rise up to the challenge and overcome a myriad of obstacles to combat cybercrime. Cybercrime investigations, whether it be for online identity theft, selling counterfeit products via spam, or hacking (unauthorised access, modification of impairment/interference with data or data systems), involve unique challenges. The challenges involve difficulty with harmonisation of laws, jurisdictional issues, resource implications, lack of training, ambiguity in terms of how a criminal provision will be interpreted alongside human rights protections, and, above all, a host of technical hurdles making tracing back to the "offender" difficult.

The following sections *assume* that investigation and prosecution of an ethical hacker is desirable; there are good arguments as previously discussed for exemptions to apply to ethical hacking, especially in situations where the online activity corresponds with legal

---

[69] MCC, note 5 above, page 109
[70] MCC, note 5 above, page 109
[71] Survey on file with the author.
[72] Contemporaneous notes by author filed with research materials from closed panel sessions at AusCERT 2008 Conference, AusCERT 2009 Conference, and Internet Security and Intelligence Operations 5 Workshop 2007, Estonia.

offline activity. This typically occurs at the intersection of the act with protection of human rights / civil liberties.

9.1 Obfuscation Technologies

Many different techniques exist to make traceback of an attack to the original source difficult. These technologies/techniques will be described as "obfuscation tools", as such tools allow people to evade technological controls and legal sanction.[73]

Commonplace obfuscation techniques include dynamic DNS, multihoming, FastFlux DNS, distributed command and control (superbotnet), encryption, proxy servers, virtual platforms, rootkits, and the use of peer-to-peer channels. These tactics allow people to hide behind a cloak of anonymity and low possibility of traceback of an attack to its source. These key terms are defined below:

Multihoming involves the configuration of a domain to have several IP addresses. If any one IP address is blocked or ceases to be available, the others essentially back it up. Blocking or removing a single IP address, therefore, is not an effective solution to removing the content. The content merely rotates to another IP address.

Dynamic DNS is a service that enables the domain name entry for the relevant domain-name to be updated very promptly, every time the IP address changes. A dynamic DNS provider enablers a customer to either update the IP address via the provider's web page or using a tool that automatically detects the change in IP address and amends the DNS entry. To work effectively, the Time to Live (TTL) for the DNS entry must be set very short, to prevent cached entries scattered around the Internet serving up outdated IP-addresses.

FastFlux is a particular dynamic DNS technique used by botnet masters whereby DNS records are frequently changed. This could be every five minutes.[74] Essentially, large volumes of IP addresses are rapidly rotated through the DNS records for a specific domain. This is similar to dynamic DNS tactics. The main difference between dynamic DNS and FastFlux is the automation and rapidity of rotation with a FastFlux botnet.[75] Some FastFlux botnets rotate IP addresses every hour, and others every day.

Distributed Command and Control (or Superbotnets) is a type of botnet that draws on a small botnet comprised of 15-20 bots. The botnet herders may have anywhere from 10 000 to 250 000 bots at their disposal, but use a select few for a particular purpose. The smaller botnet is then used to issue commands to larger botnets (hence the term distributed command and control).[76]

Encryption is the conversion of plain text into ciphertext. Encryption acts to conceal or prevent the meaning of the data from being known by parties without decryption codes. Encrypted instruction can then not be analysed making investigating, mitigation and prevention much more difficult. Public

---

[73] Lovet 2009.
[74] *See* The Honeynet Organisation at http://www.honeynet.org/node/132.
[75] Dunham 2009.
[76] Barakat et al.

key cryptography is often used. In public key cryptography, a twin pair of keys is created: one key is private, the other public. Their fundamental property is that, although one key cannot be derived from the other, a message encrypted by one key can only be decrypted by the other key.

Proxy servers refer to a service (a computer system or an application) that acts as an intermediary for requests from clients by forwarding requests to other servers. One use of proxy servers is to get around connection blocks such as authentication challenges and Internet filters. Another is to hide the origin of a connection. Proxy servers obfuscate a communication path such that User M connects to a website through proxy server B which again connects through proxy server Z whereby the packets appear to come from Z not M. Traceback, however to Z yields information of an additional hurdle as packets also appear to come from B. Other proxy servers such as Tor are anonymous. Tor is also known as an onion router. Tor is described as follows:

> "Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody from watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location."[77]

Tor is described as onion routing due to the use of multiple layers of proxy servers. This is similar to the multiple layers of an onion. Tor is used by users in heavily Internet-censored countries like China and Iran to access blocked websites as well as being used by some criminals to prevent law enforcement from traceback to the source.

Virtual Private Network Service (VPN) is a network that uses a public telecommunications infrastructure (usually the Internet) to connect remote sites or users together[78]. This connection allows a secure access to an organisation's network. Instead of a dedicated, real-world connection such as a leased line, a VPN uses "virtual" connections routed through the Internet from an organisation's private network to the remote site or employee."[79] VPN is made secure through cryptographic tunnelling protocols that provide confidentiality by blocking packet sniffing and interception software.

Rootkits are software or hardware devices designed to gain administrator-level control and sustain such control over a computer system without being detected.[80] A rootkit is used to obscure the operation of malware or a botnet from monitoring and investigation. It may also be used as a way for an ethical hacker (if he or she has installed it) to monitor the actions of a government or corporation, as well as to look and copy documents on others' servers.

Peer-to-peer Communications (P2P) "is any distributed network architecture composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances."[81] A P2P network relies on the capacity of multiple participants' computers, each of which has both client and server capabilities. This differs from conventional client-server

---

[77] Tor available at https://www.torproject.org

[78] Virtual Private Network available at http://www.en.wikipedia.org/wiki/Virtual_private_network

[79] Tyson 2009.

[80] Pfleeger 2007..

[81] The author looked any many different definitions of peer-to-peer and found the Wikipedia definition had the best description. *See* Wikipedia "Peer-to-peer" available at http://en.wikipedia.org/wiki/Peer-to-peer

architectures where a relatively low number of servers provide the core function of a service or application.[82] Such networks are useful for many purposes such as sharing of scientific information amongst researchers, file-sharing of videos and music, and for telephone traffic. P2P operates on peer nodes[83]. P2P may be used to send content in clear or encrypted format. The ad hoc distribution of P2P makes it an ideal bot server location for command and control. The use of P2P channels allows an additional layer of rapid IP address fluctuation. For this reason, botnets that use in P2P channels are seen as offering the equivalent of "double fast-flux".

Security researcher Lovet describes the difficulty of traceback to the IP address of the botnet master in the following persuasive manner:

> "To put it simply, when a stateful Internet connection (a.k.a. a TCP connection) is established between Alice and Bob, Alice sees Bob's IP address. Thus if Bob does bad things to Alice via this connection, his IP address can be reported. Now, if Cain connects to Bob, and from there, connects to Alice with bad intentions, Alice will still only see Bob's IP address. In other words, Cain has masked his IP address with Bob's. The component which allows Cain to use Bob as a relay is called a proxy (there are various types of proxies, though in cybercriminal schemes socks4 and socks5 proxies are mostly used). Such a component, of course, may have been installed on Bob's computer without his knowledge, by Cain. Or by Daniel, and Cain just rented or purchased access to it. As a matter of fact, most trojans and bots embed a proxy, and in any case, have the capability of loading one after prime infection. Given the prevalence of bot-infected machines (a.k.a. zombie computers), that makes a virtually endless resource of proxies for cybercriminals, all sitting on machines of innocent, unaware users. This is something cybercriminals understand perfectly and exploit ruthlessly, sometimes on a large scale."[84]

When an obfuscation method such as a proxy or fast-flux is utilised, traceback will often only lead back to the infected bots that form part of a botnet, or to the IP addresses of the C&C. Once the IP address is known for the bot, the individual who has registered the Internet connection from that computer to the ISP may be contacted. An IP address does not, however, tell you who used a computer to perform a crime. If a computer is used by several people, identifying the botnet master will require additional evidence other than a mere IP address. The botnet master may only be targeted upon discovering where the command and control is occurring and tracing back through proxies to the original source. Discovering the C&C point where a botnet receives its instructions from, however, neither reveals the exact computer source nor the identity of the botnet master. In the rare chance that the identity of a botnet master can be traced back, the botnet master can always use the "Trojan horse" or "bot" defences which may or may not prove successful (see section 9.4).

Many online civil disobedience participants do not have the computer skills required to use such obfuscation techniques. They are more limited to using LOIC. An encrypted version of LOIC is now being developed. This will present a further challenge to law enforcement to identify those participants in DDoS attacks using LOIC.

---

[82] Clarke 2004.
[83] Oram 2001.
[84] Lovet 2009.

9.2 Integrity, Volatility of Evidence and the Trojan Horse Defence

Digital evidence suffers from volatility. Volatility refers to the ease by which one may alter or damage evidence whether it is done accidentally or intentionally. This in turn makes it relatively easy to expunge volatile evidence and to create 'reasonable doubt'. For example, the mere making of a copy of a file and putting it onto a USB memory stick interferes with the integrity of the digital evidence. Another common example is when an employee with a company's technical division takes it upon herself to view a quick online tutorial then proceeds to install and use forensics software on the company's computer or server. When forensics software and equipment are used without proper training it is probable that the integrity of the evidence will be jeopardized. Forensics investigators, by way of example, use a device which makes tampering with evidence impossible, and take a virtual snapshot of a computer or server (if possible) which can then be analysed at a later date. Without such preventative measures, digital evidence is subject to being expunged from evidence.[85] Forensics investigators have these basic technologies which allow for proper collection and preservation of data. The concern, therefore, is not that such technologies are not widely available or that their cost is prohibitive. The concern is one of education and training. When proper forensics techniques are not used, the integrity of the evidence is lost.

Where technology is involved in a crime, the accused will often use the "Trojan horse" or "bot" defence. In this instance, a party claims that they are not responsible for an action, but rather, a malicious software program such as a "Trojan" was unknowingly downloaded to their computer by a third party. In a "bot" defence, the argument is that the defendant's computer became a bot and controlled by a malicious third party. Thus the "Trojan" or the "bot" is to blame. In the case of a botnet, it may seem odd that a "Trojan horse" defence would be tried when the criminal act is often the very installation of an unauthorised 'Trojan' onto someone else's computer. This, however, is not necessarily the case. A botnet master, for example, could argue that his/her computer was being used as a proxy to make it look as though the botnet was installing Trojans. This argument could conceivably extend to the claim that command and controls were orchestrated to come through his/her computer via malware where the bots (software programs) were installed by a third party. Alternatively, a botnet master might claim to operate a botnet but could make the argument that a third party (another botnet master) took over his/her botnet through issuing an unauthorised bot (software code) to perform illegal acts.

An example of a prosecution failure for these reasons is a judgement in the United Kingdom against Aaron Caffrey. As reported, Aaron Caffrey was a 19 year old who launched a distributed denial-of-service attack on September 20, 2001 affecting computers serving the Port of Houston, Texas.[86] The attack caused major havoc with shipping logistics. The accused claimed that a malicious program had been installed on his computer, and that he did not perform such acts. The jury acquitted in spite of the fact that upon examination, common hacker tools were found on the defendant's computer, the defendant was a known hacker who regularly participated in discussion of how to launch DDoS attacks and other types of malware, while possible forms of malware were absent on

---

[85] Klein 2010.

[86] The case is not reported in law databases but was covered by the British media and is mentioned by several cybercrime researchers. *See* BBC News, "Questions Cloud Cyber Crime Cases" October 11, 2003 available at http://www.bbc.co.uk/2/hi/technology/3202116.stm (last accessed April 27, 2010). The case is mentioned as R *v. Caffrey* (2006) in Clayton, R. "Complexities in Criminalising Denial of Service Attacks" written for the Legal Subgroup of the Internet Crime Forum (Feb. 2006) available at www.cl.ram.ac.uk/~rncl/complexity.pdf.

the defendant's computer.[87] The evidence was overwhelmingly in favour of a successful prosecution, but the technical evidence was presented in a confusing manner which one journalist describes as:

> "Had the jurors been technology experts, or even computer-literate, I wonder if the ruling would have been the same. I spent most of the first week of the trial in the public gallery and found it didn't take long before the jury's eyes glazed over because the technical arguments sounded like a Russian version of Moby Dick that had been translated into English using Babelfish. By the third day, one of the jury members had to be discharged because of a severe migraine, which was indubitably brought on by the jargon."[88]

This case reinforces that while digital evidence is volatile, even sound evidence is subject to the "Trojan horse" and "bot" defences due to the inability of jurors and judges to understand the technical complexities of some cyber crime cases.[89]

9.3 Real Time Forensics and Interception

The value of real-time forensics is perhaps best illustrated by way of analogy. CCTV surveillance cameras are installed for example, in public spaces and on highways. The cameras are used in two capacities. First, when monitored they may be used to identify potential problems before a crime is committed, or to actively alert law enforcement while the crime is being committed. Second, they might not be monitored but footage from the cameras may be used as evidence post-crime. Of course, such cameras also perform surveillance functions collecting personal information of non-criminals, potential in breach of privacy and surveillance laws.

Real-time forensics operates on a similar premise. Real-time forensics can operate in two ways: general evidence collection without a suspect in mind or specific evidence collection with a suspect in mind. Let us first consider general collection of real-time evidence. ISPs routinely monitor their networks using technologies such as Netflow for suspicious or abnormal Internet traffic. Where a crime is committed, a warrant may be issued allowing law enforcement agents to access ISP data logs (if any) stored at the time of the crime. The value of evidence collected post-crime is dependent on the monitoring and detection technologies used by the ISP. Many ISPs use medium packet inspection technologies such as Netflow. Netflow does not maintain data logs for long before they are deleted. Where more invasive technologies such as deep packet inspection are used there is potentially more value-rich information for post-crime investigations. This is either because the monitoring is more substantive or it could merely mean that the data traffic logs are stored and retained for longer periods of time. Both medium packet inspection technologies such as Netflow and deep packet inspection technologies are capable of collecting evidence in real time.

The term "real-time evidence" is not very useful. The importance lies in what type of information is collected by the packet inspection technologies, the length of time that it is stored and retained (typically data traffic logs), and the ability of law enforcement to use this information. This type of information request by law enforcement agents to ISPs is referred to colloquially as a "data dump" – any information that an ISP may have stored relevant to an IP address or range of IP addresses.

---

[87] Grabosky 2007.
[88] Brenner 2004.
[89] Walden 2010.

General ISP evidence collection without a suspect in mind is often of little value to law enforcement agents. This may be due to a number of reasons: 1) the type of data collected was not useful, or 2) the type of data was useful but was not stored, or 3) the volume of data collected is too large a quantity to be of timely use in an investigation.

The second scenario looks at real-time evidence collection when there is a suspect in mind. In this instance, a law enforcement agent may apply for an appropriate content warrant. The communications of the suspect could then be intercepted. Depending on the type of warrant, this could include website contents and email mail-box contents (stored communications warrant), or information about IP traffic to and from a target IP address/address range or VOIP traffic to and from a phone number.

Unlike crimes in the physical world, often there is little physical evidence after a cyber- crime is committed unless there is real-time data collection and retention. Real-time forensics is also known as live forensics as distinct from post-mortem forensics.[90] Real-time data collection allows the capturing of:

> "Volatile information that would not normally be present in a post-mortem investigation. This information can consist of running processes, event logs, network information, registered drivers, and registered services. Running services tell us the types of services that may be running on a computer. These services run at a much higher priority than processes ... Viewing running processes with the associated open network ports is one of the most important features of analysing the system state."[91]

Without real-time evidence, there is heavy reliance on the physical memory (RAM) of a computer. As previously seen with obfuscation tools, dynamic methods are used where information is neither stored centrally nor statically. The likelihood of stumbling on physical memory after the fact is negligible. Real-time data collection allows entire contents of an email mail-box to be captured, whether the information is local or remote.[92] Where real-time data is stored, law enforcement agents are potentially able to peer at the email mail-box pre-crime, post-crime and during the commission of a crime. The capturing and storing of real-time data requires the assistance of ISPs who are the middle men or information conduits. The co-opting of ISPs to assist law enforcement is contentious.

9.4 Damages

In theory, if there has been unauthorised access, modification or impairment of data an investigation may be mounted and perpetrators prosecuted. In practice, often a victim must be able to prove that a certain amount of money was lost or damage suffered in order to prompt an investigation.[93] The amount is often pure conjecture. Many jurisdictions have predetermined thresholds amounts in order for an investigation to be launched. Arguably, many forms of unauthorised access or a DOS attack for two hours may not cause enough damage to attract investigation. These thresholds are determined by internal police working committees. Not all law enforcement investigation units have minimal monetary amounts. In some jurisdictions, a decision to launch an investigation in the case of computer related cybercrimes is dependent on a wide range of factors which include whether the

---

[90] Reyes 2007.
[91] Reyes 2007.
[92] Reyes 2007.
[93] de Villiers 2003.

crime is serious or organised crime and whether the investigation is within the capabilities of the local police. [94]

9.5 Jurisdiction

Computer crimes often involve parties located overseas. These crimes may involve many people located in different jurisdictions whether they are different states or provinces within a country, or different countries altogether. Each jurisdiction will have its own laws dealing with an issue as well as its own unique set of evidence procedures in courts. Uniformity is a real problem. A successful prosecution often involves assistance and cooperation of authorities from an outside jurisdiction. For a variety of reasons, some jurisdictions may or may not be willing to cooperate. Such cooperation generally must proceed through the cogs of bureaucracy in cases where time and access to good digital evidence (unaltered) is of the essence. This often means applying for warrants in multiple jurisdictions which may translate into a loss of valuable time and perhaps a loss of obtainable evidence.

The greatest challenge, however, remains in identifying and determining the physical location of the computer, and then the actual individual(s) who used the computer/network to commit a crime. The Canadian police, for example, cannot obtain a warrant to wire-tap someone in Mongolia and they cannot compel an ISP in Papa New Guinea to provide data logs. This type of international policing requires the cooperation of law enforcement and courts in other jurisdictions. Law enforcement could contact law enforcement in the location of the hacker but cooperation may not be forthcoming. First, inter-jurisdictional investigations rely on the offence being given similar priority in both jurisdictions. For truly repugnant cases such as child pornography, jurisdictions tend to have similar strong mandates.[95] In the case of hacking (unauthorised access), the priorities are often disparate. This is especially true in jurisdictions without computer misuse offenses. It is of no coincidence that Wikileaks servers are located in protective jurisdictions. The LulzSec website is hosted on a cloud computing space.

The situation is somewhat reversed when subpoenas for data logs are sent to US based communication services such as Google, Twitter or Facebook. In this instance, the law of the server prevails. For example, if I am a Twitter user located in Australia, an American law enforcement entity may issue an administrative subpoena without a warrant or transparent declaration of the scope of a criminal investigation, to actively retrieve all data logs connected to a hashtag. For example, one could request all communications, IP addresses, and subscriber information for everyone who communicated in the Occupy Wallstreet movement, including those of people located around the globe. In this sense, the international criminal justice system by way of established treaties, and data protection of citizens in foreign countries, is subverted. The law of server (often the United States) prevails.

The second challenge is related to the first in that police tend to use their resources to respond to local problems. Where there is no victim in the locale of the police force, priority will not be given to an overseas investigation. Third, there is again the de minimus rule whereby in order to justify valuable police resources, a certain threshold of damages must be met. The jurisdictional hurdles stem from practical considerations as well as a lack of criminalisation of an act across jurisdictions.

---

[94] Correspondence with Detective Van der Graf, head of the Fraud Squad, New South Wales Police. Notes are on file.
[95] Wall 2007.

9.6 Issues in Ethical Hacking

One of the greatest challenges for ethical hacking prosecutions will be how the evidence was obtained. If governments are outsourcing intelligence to security firms, it is likely that many of such firms will use hacking methods to obtain their information. There is no legal mechanism that allows such firms to perform such actions. There is furthermore no way to ensure accountability of such firms at present. One assumes that evidence collected by law enforcement would have been done according to the law but this too turns out to be a murky legal area. For example, in 2001 the US Federal Bureau of Investigation ('FBI') lured two Russian criminal hackers to Seattle under the guise of a job offer with an FBI invented corporation, Invita. Alexey Ivanov and Vasily Gorshkov were promptly arrested when they arrived on US soil. What they thought would be a job interview quickly turned into an interrogation from law enforcement. The two allegedly broke into the networks of bank and other companies. The FBI remotely installed keylogging Trojans on the suspects' computers and collected evidence including the passwords to email accounts. Incriminating evidence from the suspects' computers and servers utilised for email were used to convict the two on charges under the *Computer Fraud and Abuse Act* 18 USC § 1030 (1986), as well as 20 counts to conspire and a number of fraud counts.[96] The evidence was collected without a warrant, but the Court nonetheless deemed the evidence valid, rejecting motions for its suppression. The Court ruled that the right against unreasonable search and seizure under the Fourth Amendment was not violated because the accused had no right to privacy when using computers at the fictitious offices of Invita.

On a similar note, it remains to be seen if Twitter users outside of the United States will be afforded the protection of free speech and privacy of data when they are not themselves the object of investigation, but where law enforcement solely seeks to acquire personal information. It remains unknown if a non-US Twitter user would have standing in an American court. As seen in the Invita situation, free speech and privacy protection will likely not extend to non-Americans.

A most problematic theme has emerged with hacktivism. Many hacktivists seek to rebel against what they perceive to be unjust policies or measures that infringe against civil liberties. As a consequence of the flury of hacktivist activities, however, governments around the globe are using more and more forms of surveillance, and civil liberties are eroding further than in the pre-hacktivism era. At this point, it is a vicious circle with laws being broken by both sides.

It is curious to see so much law enforcement resources being allocated to hacktivist investigations, yet so very little resources allocated to the fight of online organised crime such as mass fraud, identity theft and corporate espionage.

10. Key Findings

- Online protests will increase and the type and size of such attacks will escalate in order to continue to capture the interest of the media.

- There is a growing movement in some online communities (hackers) to ensure that "backdoors" (ways to exploit a program) are inserted into computer programs and then kept

[96] *United States v Gorshkov* (2001) WL 1024026 (Western District Washington).

quiet as a means of ensuring access to future information (especially government websites). These types of "attacks" are not done for instant media attention.

- Technologies such as LOIC will evolve to allow for encryption and anonymity. This will parallel similar developments that took place with peer to peer file-sharing networks.

- The most popular discussion threads in hacking forums are "beginner hacking" and "hacking tools and programs" indicating the likelihood of increased hacking, both ethical and for criminal purposes.

- Deterrent effect of laws and sentences only works with beginners and with younger hackers. These individuals will generally quit illegal hacking after first conviction (under 25).

- The law does not have a deterrent effect for highly skilled and often older hackers (over 25).

- Some individuals involved in hacking are considered be have an addiction in the same way that an individual may become addicted to gambling, video games, drugs or alcohol.

- A significant portion of corporations and organisations are engaged in some form of counter-attack.

- Many ethical hacking incidents are closely tied with the objective of protecting human rights and promoting an open, transparent democracy.

- Many ethical hackers view their work as acts of civil disobedience and align their actions with traditional civil disobedience as espoused by Ghandi, Martin Luther King Jr. And Henry David Thoreau.

- Other hackers identify with an ethos of hacking that developed in the 1980s forward and look to technical gurus and the writings of "Hacktivismo Declaration" by the Cult of the Dead Cow, "The Hacker Manifesto", "The Anonymous-Anonops", The Electrohippies "Client-Side Distributed Denial-of-Service" and the "Gospel According to Tux".

- Other groups are less ideal in their philosophy citing motivation as "for the laughs". However, further probing of such hackers reveals that their hacking is done out of "a streak of sense of wrongdoing" without always being able to clearly articulate what that wrongdoing is.

- Denial of Service Attacks by movements such as Anonymous require critical mass in order for an operation to be successful.

- There is often a correlation between the number of participants in a denial of service attack, and the worthiness/morality of the cause.

- Which causes will acquire critical mass is unpredictable.

- It would be incorrect for governments or organisations to assume that members of ethical hacking groups come from one type of community, race, or age.

- Many ethical hackers are not aware that their activities are illegal, especially those participating in politically motivated denial of service attacks.

- Elite hackers tend to work alone due to the higher risk of "getting caught" when groups are involved. This may support the proposition that a technically sophisticated attack may in fact be the work of only one individual, or few individuals.

- While many instances of ethical hacking may be illegal, it is interesting to note that some methods used by law enforcement and by security firms contracted to perform criminal intelligence gathering may also be illegal, or at best highly controversial.

11. Recommendations

- Develop and publicise guidelines for online civil disobedience and hacktivism.

- Run an education campaign once these guidelines are finalised.

- Allow and encourage a legitimate "space" for virtual protests.

- Investigate the licensing of security experts.

- Implement a security research exemption for computer offences.

- The idea of a public interest exemption for hacking offenses should be given further consideration. This could be done in a multi-party working group for both security research and public interest exemptions.

- Develop a code of conduct for counter-attack and have a legislative review of how principles of self-defence might apply to a counter-attack situation.

- Any governmental engagement with ethical hacking should be legal and transparent. These activities should not be contracted out to security firms unless they are closely scrutinised and held accountable in some form of safeguard or compliance mechanism.

- Review the insecure practices of corporations and organisations that hold sensitive personal data and consider implementing more effective legislation such as data breach notification and the obligation to encrypt all personal information held by such entities.

- Ensure that data owned or generated by Canadians is protected and that such data, if collected and stored, is deleted after a reasonable period when using foreign services such as Google, Facebook and Twitter (United States based). Currently, any person who uses Google, Facebook, Twitter and similar services is subject to US Internet monitoring by governments and law enforcement, and potentially is exposed to subpoenas to release personal information even in the *absence* of a criminal investigation.

12. Future Research

12.1 Canadian Charter of Human Rights and Freedoms

This report has not considered arguments that could be made to challenge charges made against ethical hackers under the Canadian *Charter of Human Rights and Freedoms*.

12.2 Internet Service Providers and Communication Companies (Facebook, Google and Twitter) Revealing Account Information

This report has not considered in any depth the thorny issues involved with revealing the account information and personal information of accused ethical hackers by social media companies such as Twitter, Facebook and Internet Service Providers.

The interim order for Twitter to produce detailed account records of Julian Assange and Bradley Manning is expected to be appealed to the Supreme Court of the United States on multiple grounds, including issues of privacy.[97] Similar requests in Canada could be fought on privacy grounds.

In a more disturbing instance, subpoenas to Twitter have been issued by Boston law enforcement to reveal personal information of any party connecting to tweet hashes connected to the Occupy Boston movement (including information communicated by journalists). This has included information of citizens around the globe. No warrants were sought nor has there been any information given as to the illegality of the criminal investigation.

This report has merely flagged some of these issues which are ripe for greater consideration and research.

12.3 Security Research Exemption or Public Interest Exemption

This report has not provided list of factors and considerations which are vital to any introduction of a security research or public interest exemptions to unauthorised access and modification provisions in criminal law. Likewise, this report has not analysed or considered recent European initiatives of licensing information security experts.

12.4 Full Exploration of Government Contracting of Surveillance and Intelligence Gathering

Anonymous has announced that, due to inadequacy of the media to report on surveillance and intelligence gathering issues, and due to the government lack of transparency, they will be targeting documents from security companies known to perform such functions under contract from the government or organisation. Further investigation into whether such studies exist, along with the exposure of such contracting as not been considered in depth in this report.

---

[97] *In re § 2703(d) Order, 2011* U.S. Dist. LEXIS 25322

13. Appendix A – Case Law Summary

The extensive caselaw review revealed a paucity of reported cases in the world on ethical hacking. In most instances, there was only media coverage on the arrest and charges laid in connection with the incident. The lack of criminal caselaw is caused by three key factors:

1) the currency of the actions (not enough time has elapsed for a trial to have occurred and a decision to have been reported in caselaw databases),
2) the accused may have settled the case, or
3) the accused may have agreed to act as an informant in exchange for all charges being dropped against him/her

The Appendix below details reported criminal caselaw, as well as reported arrests of ethical hackers in the media.

Germany

Andreas-Thomas Vogel

CaseName:	„libertad.de" - case
Citation:	File reference 1 Ss 319/05, 22nd March 2006
Jurisdiction:	decision of the Higher Regional Court, Frankfurt am Main
Main URL:	http://www.libertad.de/service/downloads/pdf/olg220506.pdf
Charged With:	Coercion, and incitement of alteration of data
Legislative Provisions:	§240 German Criminal Law: Coercion § 111 in conjunction with § 303a German Criminal Law: Incitement of alteration of data
Main Target:	
Motivation:	Denial of service attack against the websites of the German Airline "Lufthansa", in order to protest against the company. They deport illegal immigrant and make profit with this. The accused wanted to achieve more publicity of these grievances. He planned a denial of service attack at the 20th of June 2001 and programmed a small protest-software, downloadable for protestants to enable loads of pageviews. The demonstration had 13614 participants with different IP-adresses and encompassed 1,126,200 pageviews. The damages were about 5,500 € for personal costs and 42,000 € for further impairments.
Convicted Of:	Andreas-Thomas Vogel was indicted and convicted of coercion in the Frankfurt court of first instance. The Frankfurt Appellate Court reversed the decision stating the DDoS attack was a legitimate exercise of free speech.
Sentence:	Acquittal in the second instance
Additional	In the court of first instance the district court sentenced the accused with a

Important Information:	financial penalty of 90 days à 10 Euro in the first instance. The Higher Regional court reversed the verdict in the appeal

United States

United States Army v. Bradley Manning

The defendant was arrested after allegedly accessing and providing classified U.S. Government documents to Wikileaks. He was a U.S. Army soldier based in Iraq. He was charged in 2010 and is still awaiting a hearing.

ITEM	NOTES
CaseName:	United States Army v. Bradley Manning
Citation:	
Jurisdiction:	Army's Military District of Washington
Main URL:	http://en.wikipedia.org/wiki/United_States_v._Bradley_Manning, http://www.cbsnews.com/htdocs/pdf/ManningPreferralofCharges.pdf http://www.msnbc.msn.com/id/41876046/ns/us_news-security/ http://www.nytimes.com/2011/04/30/us/30brfs-PANELSAYSWIK_BRF.html?_r=1&ref=bradleyemanning
Charged With:	Transferring U.S. Government documents to a party not entitled to receive them (allegedly, Julian Assange of Wikileaks).
Legislative Provisions:	Uniform Code of Military Justice Arts. 104 (aiding the enemy), 92 (failure to obey a lawful order or regulation), and 132 (general article, including counts of offenses against the Computer Fraud and Abuse Act 1986 (U.S. Code s1030(a)), and 793, for communicating, transmitting and delivering national defence information to an Unauthorized source.
Main Target:	
Motivation:	United States Army
Convicted Of:	Public disclosure of U.S. Government (including foreign policy) documents in order to "change something" (according to the transcript of his chats with Adrian Limo, see Wikipedia).
Sentence:	
Additional Important Information:	Possibly life sentence if convicted of the most serious charge against him, aiding the enemy.
	22 charges including aiding the enemy and improperly obtaining a classified gunsight video. Proceedings have commenced in Forte Mead, Maryland.

US v Kevin George Poe

An Anonymous-affiliated Connecticut man, Poe, was arrested and charged with conspiracy and unauthorized impairment of a protected computer, after allegedly disabling Gene Simmons' website with a denial of service attack.

ITEM	NOTES
CaseName:	US v Kevin George Poe
Citation:	CR 11 01166
Jurisdiction:	Federal – US District Court for the Central District of California

Main URL:	http://techlaw.justia.com/wp-content/uploads/2011/12/poe-gene-simmons-12082011ind.pdf http://techlaw.justia.com/2011/12/14/indictment-alleges-ddos-attack-on-gene-simmons-web-site/ http://www.guardian.co.uk/technology/blog/2010/oct/14/gene-simmons-anonymous-attack-filesharing
Charged With:	Conspiracy and unauthorized impairment of a protected computer
Legislative Provisions:	18 USC 371: Conspiracy; 18 USC 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I): Unauthorized impairment of a protected computer
Typology:	
Main Target:	Gene Simmons via his website
Motivation:	Likely to be protest or retribution as it occurred shortly after Gene Simmons criticised file sharing encouraged copyright owners to commence litigation and seek extensive damages against file sharers. (See Guardian article for screenshot of Anonymous message about Gene Simmons' views).
Convicted Of:	
Sentence:	If convicted of both counts, up to 15 years in federal prison
Additional Important Information:	

Member of LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems

"A member of the LulzSec hacking group was arrested … for his role in an extensive computer attack against the computer systems of Sony Pictures Entertainment. … On September 2, 2011, a federal grand jury returned an indictment filed under seal in U.S. District Court in Los Angeles charging Kretsinger with conspiracy and the unauthorized impairment of a protected computer." [1st and 2nd paras]

ITEM	NOTES
CaseName:	
Citation:	Public Affairs Specialist Laura Eimiller, 'Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems' (FBI Press Release, 22 September 2011).
Jurisdiction:	Los Angeles, U.S. District Court
Main URL:	http://www.fbi.gov/losangeles/press-releases/2011/member-of-hacking-group-LulzSec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems
Charged With:	Conspiracy and the unauthorized impairment of a protected computer (using an SQL injection and a proxy server)
Legislative Provisions:	
Main Target:	Sony Pictures Entertainment's computer systems
Motivation:	
Convicted Of:	
Sentence:	"If convicted, Kretsinger faces a statutory maximum sentence of 15 years in prison." [8th para]
Additional Important Information:	"This case is being prosecuted by the United States Attorney's Office in Los Angeles." [2nd to last para]

Two Men Charged in New Jersey with Hacking AT&T's Servers

"Two self-described Internet "trolls" were arrested … for allegedly hacking AT&T's servers and stealing e-mail addresses and other personal information belonging to approximately 120,000 Apple iPad users who accessed the Internet via AT&T's 3G network" [1st para]. The defendants are alleged to be associates of the group Goatse Security, which according to Wikipedia is a grey-hat hacker group that exposes security flaws. (So in this sense, vaguely "ethical").

ITEM	NOTES
CaseName:	
Citation:	U.S. Attorney's Office, 'Two Men Charged in New Jersey with Hacking AT&T's Servers' (FBI Press Release, 18 January 2011).
Jurisdiction:	Newark, New Jersey
Main URL:	http://www.fbi.gov/newark/press-releases/2011/nk011811.htm
Charged With:	"Each defendant is charged with one count of conspiracy to access a computer without authorization and … fraud in connection with personal information" [14th para]
Legislative Provisions:	
Main Target:	AT&T's servers
Motivation:	unclear
Convicted Of:	Possibly to publicise security faults in AT&T's 3G network, or "criminal gain or prestige among peers in the cyber-hacking world" [5th to last para].
Sentence:	
Additional Important Information:	"Each count with which the defendants are charged carries a maximum potential penalty of five years in prison and a fine of $250,000." [4th to last para].

Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks

"Fourteen individuals were arrested ... on charges related to their alleged involvement in a cyber attack on PayPal's website as part of an action claimed by the group 'Anonymous,'" [1st para]. "In addition ... Arciszewski, 21, was arrested today ... on charges of intentional damage to a protected computer [for] allegedly access[ing] without authorization the Tampa Bay InfraGard website and upload[ing] three files... then tweet[ing] about the intrusion and direct[ing] visitors to a separate website containing links with instructions on how to exploit the Tampa InfraGard website." [8th & 9th paras]

ITEM	NOTES
CaseName:	
Citation:	Office of Public Affairs, 'Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks' (FBI Press Release, 19 July 2011).
Jurisdiction:	San Jose, Northern District of California; Orlando, Middle District of Florida. (New Jersey arrest mentioned in this press release regarding a hack of AT&T's servers is detailed above).
Main URL:	http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks
Charged With:	California charges: conspiracy and intentional damage to a protected computer Florida charges: intentional damage to a protected computer.

Legislative Provisions:	
Main Target:	California: DDoS attacks on Paypal Florida: Tampa Bay InfraGard website (which is sponsored by the FBI).
Motivation:	California: retaliation against Paypal's termination of Wikileaks' donation account Florida: disclosure of security flaws (as the defendant tweeted about the intrusion and posted instructions on how to exploit the flaws)
Convicted Of:	
Sentence:	"The charge of intentional damage to a protected computer carries a maximum penalty of 10 years in prison and a $250,000 fine. Each count of conspiracy carries a maximum penalty of five years in prison and a $250,000 fine." [5th to last para].
Additional Important Information:	

US v. Steiger (2003)

This case concerns a hacker that obtained evidence that the defendant was producing and collecting child pornography, and passed it on to law enforcement in the USA. The issue in this case was whether "the evidence was obtained in violation of the Fourth Amendment as the hacker was a government agent."

ITEM	NOTES
CaseName:	US v. Steiger (2003)
Citation:	318 F. 3d 1039
Jurisdiction:	Court of Appeals 11th circuit
Main URL:	http://scholar.google.com.au/scholar_case?case=5611821785646747519
Charged With:	(hacker not charged as he was not being prosecuted here)
Legislative Provisions:	The Fourth Amendment (right against unreasonable searches and seizures)
Typology:	
Main Target:	Steiger – producer and possesser of CP
Motivation:	To help law enforcement officers catch child predators
Convicted Of:	n/a
Sentence:	
Additional Important Information:	For a search by a private person to implicate the Fourth Amendment, the person must act as an instrument or agent of the government.[98]

US v. Jarrett (2003)

This case concerns a hacker that obtained evidence that the defendant was producing and collecting child pornography, and passed it on to law enforcement in the USA. The issue in this case was "whether evidence obtained by a hacker and used in a prosecution implicates the 4th amendment, and there has been communication between the hacker and law enforcement about the evidence".

[98] *United States v. Ford*, 765 F.2d 1088, 1090 (11th Cir.1985).

ITEM	NOTES
CaseName:	US v. Jarrett
Citation:	338 F. 3d 339
Jurisdiction:	Court of Appeals 4th circuit
Main URL:	http://scholar.google.com.au/scholar_case?case=7704360326371177621
Charged With:	(hacker not charged as he was not being prosecuted here)
Legislative Provisions:	The Fourth Amendment (right against unreasonable searches and seizures)
Typology:	
Main Target:	Steiger – producer and possesser of CP
Motivation:	To help law enforcement officers catch child predators
Convicted Of:	n/a
Sentence:	
Additional Important Information:	Whether the hacker's search was a Government search turns on "(1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation" [344]. There must be more than knowledge or acquiescence – there must be participation or affirmative encouragement.

United Kingdom

ITEM	NOTES
CaseName:	
Citation:	John E Dunn, 'Alleged LulzSec Hacker 'Kayla' Arrested By UK Police' *csoonline.com* 2 September 2011
Jurisdiction:	UK
Main URL:	<http://www.csoonline.com/article/689060/alleged-LulzSec-hacker-kayla-arrested-by-uk-police> at 10 November 2011.
Charged With:	Implied to be offenses under Computer Misuse Act (1990) (with which others arrested in similar circumstances were charged).
Legislative Provisions:	
Main Target:	"The arrests relate to our inquiries into a series of serious computer intrusions and online denial-of-service attacks recently suffered by a number of multi-national companies, public institutions and government and law enforcement agencies in Great Britain and the US," [4th para]
Motivation:	
Convicted Of:	
Sentence:	
Additional Important Information:	

British teenager charged over cyber attack on CIA as pirate group takes revenge on 'snitches who framed him'

The defendant was arrested and charged with offenses under the Computer Misuse Act 1990 in relation to a denial of service attack on the website of the Serious Organized Crime Agency.

ITEM	NOTES
CaseName:	
Citation:	Rebecca Camber, Colin Fernandez & Lucy Collins, 'British teenager charged over cyber attack on CIA as pirate group takes revenge on 'snitches who framed him" *dailymail.co.uk* 22 June 2011
Jurisdiction:	UK
Main URL:	http://www.dailymail.co.uk/sciencetech/article-2006118/Ryan-Cleary-charged-cyber-attack-CIA-LulzSec-takes-revenge.html
Charged With:	Five offences under the Computer Misuse Act
Legislative Provisions:	
Typology:	
Main Target:	Britain's Serious Organized Crime Agency website
Motivation:	
Convicted Of:	
Sentence:	
Additional Important Information:	

Australia

Matthew George, Anonymous member charged in NSW

Matthew George was an Australian member of Anonymous who participated in "Operation Titstorm". He was charged with inciting others to attack government websites and the Magistrate likened his activities to cyber-terrorism.

ITEM	NOTES
CaseName:	
Citation:	Sarah Whyte, 'Meet the hacktivism who tried to take down the government' (March 14, 2011) *smh.com.au* <http://www.smh.com.au/technology/security/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html> at 7 November 2011.
Jurisdiction:	Newcastle Local Court
Main URL:	http://www.smh.com.au/technology/security/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html
Charged With:	Inciting others to attack government websites
Legislative Provisions:	
Main Target:	Denial of service attack against the websites of the Prime Minister and Steven Conroy, in order to protest the Internet Censorship Bill and the presence of certain URLs on the proposed blacklist
Motivation:	
Convicted Of:	
Sentence:	$550 fine
Additional Important	

Information:	

Israel

Anat Kam

The defendant secretly copied thousands of classified (many confidential) military files during her military service, which she leaked.

ITEM	NOTES
CaseName:	State of Israel vs Anat Kam
Citation:	
Jurisdiction:	Israel – Tel Aviv District Court
Main URL:	http://en.wikipedia.org/wiki/Anat_Kamm-Uri_Blau_affair http://www.maannews.net/eng/ViewDetails.aspx?ID=275114 http://www.ynetnews.com/Ext/Comp/ArticleLayout/CdaArticlePrintPreview/1,2506,L-4141015,00.html
Charged With:	Severe espionage
Legislative Provisions:	
Typology:	
Main Target:	Israel Defence Forces
Motivation:	
Convicted Of:	Leaking classified materials
Sentence:	4.5 years imprisonment (from a maximum of 15 years), and 18 months probation
Additional Important Information:	

14. Appendix B – Ethical Hacking Time-Line Chart of Recent Activity (2011)

.....

1. Anonymous - OpIndependencia

Target	Mexico Government
Date:	15th September 2011
Source:	Comlay, E 15/9/2011, "Hackers target mexico government websites", Reuters: http://www.reuters.com/article/2011/09/15/us-mexico-hackers-idUSTRE78E7AC20110915 , "Operation OpIndependencia: Anonymous hit Mexican government official websites", The Hacker News 16/9/2011: http://thehackernews.com/2011/09/operation-opindependencia-anonymous-hit.html
Motivation:	None given
Type of Attack:	DDoS
Any other groups claiming responsibility:	No.
Damage Caused	Government websites offline for a number of hours.
Additional Important Information:	

2. Anonymous - New York Stock Exchange

Target	New York Stock Exchange - http://www.nyse.com/
Date:	4th-10th October 2011
Source:	Grant, D 10/10/2011, "NYSE Hacked! Is The Anonymous Infrastructure Crumbling?", New York Observer: http://www.observer.com/2011/10/nyse-remains-unhacked-is-the-anonymous-infrastructure-crumbling-video/ , Chiaramonte, P & Winter, J 4/10/2011, "Hacker Group Anonymous Threatens to Attack Stock Exchange", Fox News: http://www.foxnews.com/scitech/2011/10/04/hacker-group-anonymous-threatens-to-attack-stock-exchange/
Motivation:	Occupy wall street protest
Type of Attack:	DDoS
Any other groups claiming responsibility:	No
Damage Caused	New york stock exchange off line for 2 minutes – no trading
Additional	Conflicting information over whether the attack was successful or whether it

Important Information:	occurred at all.

3. Anonymous - OpCartel

Target	Alleged associates of Los Zetas drug cartel in Mexico – corrupt law enforcement, those involved in managing and participating in operations.
Date:	5th November 2011
Source:	**Mandell, N 31/10/11, "Anonymous hacker group threatens Mexican drug cartel Zetas in online video", New York Daily News: http://www.nydailynews.com/news/world/anonymous-hacker-group-threatens-mexican-drug-cartel-zetas-online-video-article-1.969859#ixzz1d4sAfvE6 , CBS news, CNET, SlashDot, Anonymous website, various others.**
Motivation:	Retaliation for alleged kidnapping of an anonymous activist. General threat posed by criminal organizations.
Type of Attack:	DDoS attack. Unauthorized access to communications. Threatens release of personal information of others involved in cartel operations.
Any other groups claiming responsibility:	No
Damage Caused	If information is released (or even if not released), more likely to pose a threat to Anonymous members depending on the nature and importance the cartel places on the information. Likely to retaliate on basis of increased publicity alone.
Additional Important Information:	• Current reports indicate conflicting rumours whether "Opcartel" will go ahead. Little belief that Anonymous has the ability to do any kind of damage. • Interesting note – "Anonymous likely won't be able to turn up more information than the U.S. government already has, but they are able to publicize more information than the U.S. government can." - Dispatch: Anonymous' Online Tactics Against Mexican Cartels | STRATFOR • UPDATE – No attack occurred. Pastebin - http://pastebin.com/XZRpjUZq , still confusion over whether any aspects of this crusade are actually truthful.

5. Anonymous – Operation Darknet

Target	Those in possession of child pornography and CP websites on the darknet
Date:	3rd November 2011
Source:	Liebowitz, M 3/11/2011, "Anonymous releases IP addresses of alleged child porn viewers", MSN Today: http://today.msnbc.msn.com/id/45147364/ns/today-today_tech/t/anonymous-releases-ip-addresses-alleged-child-porn-viewers/ , "Anonymous busts Internet pedophiles", RT: http://rt.com/usa/news/anonymous-child-tor-porn-513/ , "Hacktivist group

	shuts down child porn sites", Canoe Technology: http://technology.canoe.ca/2011/10/24/18871656.html
Motivation:	Expose those who are 'ruining Tor for the majority of legitimite users'. Lay ground work for investigations.
Type of Attack:	Spyware, brute force attack, Social engineering – phishing, Release of identifying information of active CP site visitors and those in possession of CP, unauthorised access.
Any other groups claiming responsibility:	No
Damage Caused	No reported damage as of yet. Reputational damage to those identifiable, however, it is up to law enforcement to validate alleged paedophiles.
Additional Important Information:	• Claims that the add-on was created with Mozilla's permission, seemingly unsubstantiated. • No differentiation between those who merely have CP on their computer, whether this is known to users.

6. Anonymous - BART

Target	San Francisco's Bay Area Rapid Transit (BART)
Date:	August 15th 2011
Source:	"BART drafts new policy on disruption of cellphone service", LA Times: http://latimesblogs.latimes.com/lanow/2011/10/bart-outlines-cell-phone-service-disruption-policy.html , Limer, E 15/8/2011, "Anonymous follows through on BART hack, organises protest", Geekosystems: http://www.geekosystem.com/anon-hacks-bart/ , Jardin, X 14/8/2011, "Anonymous hacks BART after wireless shutdown; protests planned for Monday", BoingBoing: http://boingboing.net/2011/08/14/anonymous-hacks-bart-after-wireless-shutdown-protests-planned-for-monday.html
Motivation:	Perceived breach of 1st amendment rights – restricting freedom of speech by disabling telecommunications services.
Type of Attack:	Unauthorised access, modification of data, website defaced, release of personal information.
Any other groups claiming responsibility:	no
Damage Caused	Defaced myBART website, leaked info on myBART user database which also included non-BART employees. Also 'assured' non-BART employees that "the only information that will be abused from this database is that of BART employees."
Additional Important Information:	• Undifferentiated/disorganized release of information. Though they claimed only BART employees would be abused would, it uses this as a blanket term and makes no distinction between those who may or may not have even been involved in the phone disruption. • Circumstances would include "destruction of district property" – needs much more clarification as almost anything can be twisted to fit such criteria.

7. Anonymous / TeaMp0isoN

Target	Oakland city police
Date:	October 28th
Source:	Fogarty, K 28/10/2011, "Hackers come out of shadows to attack police, support Occupy protests", IT world: http://www.itworld.com/security/217561/hackers-come-out-shadows-attack-police-support-occupy-protests
Motivation:	Retaliation against police injuring a protester.
Type of Attack:	DDoS, SQL injection, unauthorised access, modification of data, website defaced, release of personal information.
Any other groups claiming responsibility:	TeaMp0isoN – not really claiming responsibility, just engaging in different aspects of the activity.
Damage Caused	Anonymous – Took main Oakland Police Department website offline for a number of hours, infiltrated Oakland government security server and posted personal information of officers as well as information on the structure of the servers, themselves. TeaMp0isoN - Released a list of police-department web sites that are vulnerable to MSAccess SQL injections along with encouragements to participate.
Additional Important Information:	No indication of collaboration between Anonymous and TeaMp0isoN

8. Anonymous - Operation Rainbow Dark

Target	Document assets connected to Rainbow Medical Associates, Dr. Carlo Musso.
Date:	4th November 2011
Source:	Seltzer, S 22/8/2011, "For-Profit Company Oversaw Davis's Execution, Had Prompted Complaint for Illegal Purchase of Lethal Injection Drugs", Alternet: http://www.alternet.org/newsandviews/article/670237/for-profit_company_oversaw_davis%27s_execution,_had_prompted_complaint_for_illegal_purchase_of_lethal_injection_drugs/ , http://anonnews.org/?p=press&a=item&i=1162
Motivation:	Retaliation for execution of Troy Davis, alleged use of illegally-imported drugs for execution.
Type of Attack:	Possible unauthorised access, modification of data, website defacement, release of personal information.
Any other groups claiming responsibility:	No.
Damage Caused	No such attack seemingly occurred.
Additional Important Information:	• Same post that something will be done pasted into various blogs and anonymous-related sites. • No indication that they followed through or even that claims were valid.

9. Latin Hack Team – Ecuador presidential website

Target	Rafael Correa, Ecuador Government
Date:	June 20 2011
Source:	"Website of the Presidency of Ecuador suffered cyber attacks", ElUniverso: http://www.eluniverso.com/2011/06/20/1/1355/pagina-internet-presidencia-ecuatoriana-sufrio-ataque-informatico.html?p=1354&m=638
Motivation:	Accusations of political corruption
Type of Attack:	DDoS
Any other groups claiming responsibility:	Possibly Anonymous.
Damage Caused	Presidential website out of commission for over 2 hours, elciudadano.com (government e-newspaper) down for an hour.
Additional Important Information:	Conflicting information on the group responsible. Some report that this "Latin Hack Team" is a part of Anonymous.

10. Anonymous - Operation #TMX

Target	Toronto stock exchange
Date:	7th[h] November 2011
Source:	Moretti, S 27/9/2011 http://www.torontosun.com/2011/10/27/video-warns-of-possible-cyber-attack-on-tsx , Errett, J, 7/11/11 http://www.nowtoronto.com/news/webjam.cfm?content=183319
Motivation:	Part of Occupy Movement - destabilising economy, poverty, class oppression, etc.
Type of Attack:	None – Likely DDoS
Any other groups claiming responsibility:	no
Damage Caused	None
Additional Important Information:	No reports of whether any attack has occurred.

11. Chaos Computer Club (Germany)

Target	German government
Date:	Oct 26, 2011
Source:	Wikipedia, CCC website: http://ccc.de/en/updates/2011/staatstrojaner , Leyden, J, 2011 the register: http://www.theregister.co.uk/2011/10/12/bundestrojaner/ , wikileaks: http://wikileaks.org/wiki/Skype_and_the_Bavarian_trojan_in_the_middle

Motivation:	Breach of rights by government and law enforcement, use of Trojan "Bundestrojaner"
Type of Attack:	Release of information, analysis of code. Short critique available at http://web17.webbpro.de/index.php?page=analysis-of-german-bundestrojaner
Any other groups claiming responsibility:	no
Damage Caused	Reputation of government, highlights issues of government-sanctioned malware use beyond the scope of what the courts and laws provide for.
Additional Important Information:	Data encryption is non-existent or ineffective, can be accessed by almost anyone with an internet connection which presents significant privacy issues outside of direct government involvement.

12. Chaos Computer Club

Target	Hamberg bank, Bildschirmtext network
Date:	1985
Source:	**Harrington, J 8/9/11, "Hacktivism: What is the Chaos Computer Club?", Suite101: http://joharrington.suite101.com/hacktivism-what-is-the-chaos-computer-club-a387917 , Wikipedia 2011, "Chaos Computer Club" : http://en.wikipedia.org/wiki/Chaos_Computer_Club**
Motivation:	Protest use of biometric data for personal documents.
Type of Attack:	Unauthorised access, modification of data, theft.
Any other groups claiming responsibility:	no
Damage Caused	134000 DM Donated to their club "from" the bank
Additional Important Information:	• Returned money the next day apparently. • Conflicting information on date of the hack. Some say 1984, others say 1985. Possibly closer to new years 1984 though unconfirmed.

13. Chaos Computer Club

Target	Quicken database
Date:	1996
Source:	Von Leitner, F http://tbtf.com/resource/felix.html , Wikipedia 2011, "Chaos Computer Club" : http://en.wikipedia.org/wiki/Chaos_Computer_Club
Motivation:	Highlight system flaws
Type of Attack:	Data modification, unauthorized access, fraud (kind of. Not for any personal gain as far as I'm aware).
Any other groups claiming responsibility:	No.
Damage Caused	Changed personal data, cloned SIM, wrote ActiveX control which, once executed, turns of internet security.
Additional	Apparently demonstrated this capability on TV.

Important Information:	

14. Chaos Computer Club

Target	German government, Minister of the Interior Wolfgang Schäuble
Date:	2008
Source:	**Ragan, S 1/8/2008, "CCC is at it again – hands out copies of German Interior Minister's fingerprint", The Tech Herald:** http://www.thetechherald.com/article.php/200814/581/CCC-is-at-it-again---hands-out-copies-of-German-Interior-Minister-s-fingerprint
Motivation:	Protest use of biometric data for personal document authentication
Type of Attack:	Not specified whether fingerprint was obtained physically or off a database. Probable unauthorised access involved.
Any other groups claiming responsibility:	no
Damage Caused	Cloned minister of interior's fingerprint and made it widely available. Was able to fool biometric scanners.
Additional Important Information:	Though biometric data is unique to people, databases on which these records are kept are open to compromise.

15. Hacker Union

Target	U.S. Military, and Government servers and sites
Date:	April 2001
Source:	Nazario, J, "Politically Motivated Denial of Service Attacks", *The Virtual Battlefield: Perspectives on Cyber Warefare*, Arbor Networks: http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf , Thomas, TL 2001, 'The Internet in China: Civilian and Military Uses', *Information & Security: An International Journal,* vol. 7, pp. 159-173. Available at: http://fmso.leavenworth.army.mil/documents/china-internet.htm
Motivation:	Retaliation for mid-air collision of a Chinese fighter jet and U.S. spy plane which killed the Chinese pilot
Type of Attack:	DDOS, unauthorised access, modification of data, website defaced, defacement of websites.
Any other groups claiming responsibility:	Not claiming responsibility, but certainly taking part, Hacker Union of China, China Eagle Union.
Damage Caused	• Defaced or crashed 100> websites. Majority were .gov and .com domains. Defacements of U.S. sites included posting pictures of the dead Chinese pilot and anti-U.S. messages. • Similar acts perpetrated by pro-United States hackers on approximately 300 Chinese web sites.

Additional Important Information:	• Some pro-Chinese hackers wiped a number of compromised servers. • Generally considered bad form to do so.

16. Decocidio

Target	European Climate Exchange
Date:	23rd July 2010
Source:	Leyden, J 26/7/2010, "EU climate exchange website hit by green-hat hacker", The Register: http://www.theregister.co.uk/2010/07/26/climate_exchange_website_hack/ , Takver 25/7/2010, "European Climate Exchange website hacked", Independent Media Centre Australia: http://indymedia.org.au/2010/07/24/european-climate-exchange-website-hacked ,
Motivation:	Political protest against carbon credits
Type of Attack:	Unauthorised access, modification of data, website defaced.
Any other groups claiming responsibility:	no
Damage Caused	Site was defaced for a weekend. Highlighted the group's opposition to carbon trading as a means of tackling climate change.
Additional Important Information:	• Superficial solution when it may still be more profitable for a corporation to pay fines for environmental damage than to effectively minimise such damage. • Cited links to Climategate scandal in 2009, sketchy information available. Leaked communications pertaining to manipulation of climate change data by researchers. This was never found to be the work of hackers.

17. German stock exchange

Target	German Stock exchange (or may have actually targeted French rugby team fansite)
Date:	October 2011
Source:	Leyden, J 4/11/11, "Hackers mistake French rugby site for German stock exchange", The Register: http://www.theregister.co.uk/2011/11/04/french_rugby_site_hacktivist_maul/ , Liebowitz, M 4/11/11, "Hackers Target Stock Index, Hit Rugby Team Instead", Security News Daily: http://www.securitynewsdaily.com/hackers-stock-index-rugby-team-1309/
Motivation:	"…appeared to be trying to make an Anti-Wall Street style protest against the German DAX website"
Type of Attack:	DDoS
Any other groups claiming responsibility:	unknown

Damage Caused	Accidently took down French rugby team fan site allezdax.com for 2 weeks.
Additional Important Information:	• Not known who was responsible for the attack. Since no one has come forward, fairly safe assumption that the team website was not the intended target, though not conclusive. • Seemed to have been reported after the website was back up and running. Time of attack could possibly be mid October.

18. CabinCr3w

Target	Citigroup CEO, Vikram Pandit
Date:	October 18th 2011
Source:	Couts A 18/8/2011, "Hackers leak Citigroup CEO's personal data after Occupy Wall Street arrests", Digital Trends: http://www.digitaltrends.com/computing/hackers-leak-citigroup-ceos-personal-data-after-occupy-wall-street-arrests/ ,
Motivation:	Apparently to protest arrests of protesters in a Citibank bank
Type of Attack:	Unauthorised access, release of personal information.
Any other groups claiming responsibility:	No.
Damage Caused	Mobile and office phone numbers, an email address, two home addresses, legal and financial information and information about Pandit's family posted online.
Additional Important Information:	

19. DonR4ul

Target	Brazilian presidency blog
Date:	13th October 2011
Source:	Xinhua 14/10/2011, "Brazilian presidency's blog hacked in protest of corruption", ChainDaily: http://www.chinadaily.com.cn/xinhua/2011-10-14/content_4060557.html
Motivation:	Corruption in government departments; high fuel prices.
Type of Attack:	Unauthorised access, modification of data, website defaced.
Any other groups claiming responsibility:	No groups. Alleged to be the work of one hacker – "@DonR4UL".
Damage Caused	Defaced blog website for a number of hours.
Additional Important Information:	

20. TurkguvenLigi

Target	NetNames (DNS Registrar)
Date:	4th September 2009
Source:	**Kirk, J 5/9/2011, "Turkish Hackers Strike Websites with DNS Hack", PCWorld: http://www.pcworld.com/article/239501/turkish_hackers_strike_websites_with_dns_hack.ht , http://www.zone-h.org/**
Motivation:	Unknown
Type of Attack:	SQL injection, unauthorised access, modification of data, website defaced.
Any other groups claiming responsibility:	No.
Damage Caused	Affected many websites including ups.com, vodafone.com, theregister.co.uk, acer.com, betfair.com, nationalgeographic.com and telegraph.co.uk. Damage presumably lasted for different periods of time, depending on the site.
Additional Important Information:	• Unclear whether this was perpetrated with devious intent; to highlight system flaws; or just for laughs. • A message on the redirect page read: "4 Sept. We Turkguvenligi declare this day as World Hackers Day - Have fun ;) h4ck y0u."

21. Anonymous

Target	Israel government, security services websites
Date:	5/11/11
Source:	**Pfeffer, A, Yaron, O 6/11/11, "Israel government, security services websites down in suspected cyber-attack", Haarettz.com: http://www.haaretz.com/news/diplomacy-defense/israel-government-security-services-websites-down-in-suspected-cyber-attack-1.394042**
Motivation:	Retaliation for intercepted Gaza flotilla
Type of Attack:	DDoS.
Any other groups claiming responsibility:	No.
Damage Caused	Websites offline for an unspecified amount of time including that of the Israel Defence Force (IDF), Mossad and the Shin Bet security services, in addition to a number of government portals and ministries.
Additional Important Information:	

22. Unknown

Target	Hong Kong Stock Exchange: hkexnews.hk
Date:	10th August 2011
Source:	**Wisniewski, C 10/8/11, "Hong Kong stock exchange (HKEx) website**

	hacked, impacts trades", Naked Security: http://nakedsecurity.sophos.com/2011/08/10/hong-kong-stock-exchange-hkex-website-hacked-impacts-trades/ , Wisniewski, C 12/8/11, "Hong Kong stock exchange attacked for second day in a row", Naked Security: http://nakedsecurity.sophos.com/2011/08/12/hong-kong-stock-exchange-attacked-for-second-day-in-a-row/
Motivation:	Possibly to accompany occupy movements
Type of Attack:	DDoS
Any other groups claiming responsibility:	unknown
Damage Caused	Unspecified
Additional Important Information:	Scattered information available. Possibly perpetrated by Anonymous though since

23. TeaMp0isoN

Target	Foreign Governments; includes armynet.mod.uk and aph.gov.au
Date:	7th November 2011
Source:	7/11/2011, International Foreign Government E-Mails Hacked by TeaMp0isoN", The Hacker News: http://thehackernews.com/2011/11/international-foreign-government-e.html
Motivation:	Generic dislike of government
Type of Attack:	Unauthorised access, release of data
Any other groups claiming responsibility:	no
Damage Caused	Relased personal information/email username/passwords of over 200 government officials
Additional Important Information:	

24. Iranian Cyber Army

Target	Twitter
Date:	17th December 2009
Source:	"Who are the 'Iranian Cyber Army'", The Green Voice of Freedom: http://en.irangreenvoice.com/article/2010/feb/19/1236
Motivation:	Appears to be retaliation for Iranian embargo.
Type of Attack:	Unauthorised access, modification of data, re-directing communications, website defacement.

Any other groups claiming responsibility:	
Damage Caused	• Twitter and many sub-domains inaccessible for an unspecified period of time. • DNS redirection means that the site itself may not have been defaced, just that users were being sent to the wrong page
Additional Important Information:	

25. Iranian Cyber Army

Target	Baidu
Date:	11th January 2010
Source:	**12/1/2010, "Baidu hacked by 'Iranian cyber army'", BBC News: http://news.bbc.co.uk/2/hi/8453718.stm , "Who are the 'Iranian Cyber Army'", The Green Voice of Freedom: http://en.irangreenvoice.com/article/2010/feb/19/1236**
Motivation:	Protesting Democracy
Type of Attack:	DNS cache poisoning, unauthorised access, modification of data, re-directing communications, website defacement.
Any other groups claiming responsibility:	
Damage Caused	Site inaccessible for approximately 4 hours.
Additional Important Information:	Unknown whether DNS records or the site itself was compromised.

26. Iranian Cyber Army

Target	Voice of America and related sites
Date:	22/2/2011
Source:	**Ragan S, 22/2/2011, "Iranian Cyber Army defaces Voice of America and 93 other domains (Update)", The Tech Herald: http://www.thetechherald.com/article.php/201108/6849/Iranian-Cyber-Army-defaces-Voice-of-America-and-93-other-domains**
Motivation:	Protest American interference with Islamic countries
Type of Attack:	DNS cache poisoning, unauthorised access, modification of data, re-directing communications, website defacement.
Any other groups claiming responsibility:	
Damage Caused	Re-directed Voice of America home site to one with a protest message. Claim

	to have hit 90> others with the same attack (most of them VOA-related). Sites inaccessible for an unspecified period of time
Additional Important Information:	

27. Iranian Cyber Army

Target	Tech Crunch
Date:	**26/1/2010**
Source:	**"TechCrunch Hacked? (yes,Techcrunch got hacked)** " TechnoFriends 26/1/2010http://technofriends.in/2010/01/26/did-techcrunch-got-hacked/ Kirk, J 25/8/2010, "Iranian Cyber Army Moves Into Botnets", PCWorld: http://www.pcworld.com/businesscenter/article/208670/iranian_cyber_army_moves_into_botnets.html
Motivation:	Unknown/unspecified
Type of Attack:	DNS cache poisoning? Social engineering? DoS?
Any other groups claiming responsibility:	
Damage Caused	"…installed a page on TechCrunch's site that redirected visitors to a server that bombarded their PCs with exploits in an attempt to install malicious software." – PCWorld
Additional Important Information:	

28. N33

Target	Hugo Chavez opponents
Date:	1st September 2011
Source:	**Sanchex, F 27/9/2011, "Hackers hijack Twitter accounts of Chavez critics", MSNBC: http://www.msnbc.msn.com/id/44689342/ns/technology_and_science-security/t/hackers-hijack-twitter-accounts-chavez-critics/**
Motivation:	Political opposition, "improper use of twitter"
Type of Attack:	Phishing, unauthorised access, modification of data.
Any other groups claiming responsibility:	no
Damage Caused	Hacked the twitter accounts of a number of political opponents, reputational damage, release of personal information/communications/photos.
Additional	

Important Information:	

29. Anonymous

Target	Mastercard
Date:	28th June 2011
Source:	**Bergen, J 28/6/2011, "Anonymous hacktivists take down MasterCard.com again in support of WikiLeaks", Geek: http://www.geek.com/articles/news/anonymous-hacktivists-take-down-mastercard-com-again-in-support-of-wikileaks-20110628/ , "Second WikiLeaks payback vs. MasterCard: LulzSec or Anonymous?", International Business Times: http://au.ibtimes.com/articles/170985/20110629/mastercard-citibank-LulzSec-anonymous-wikileaks-hack-hactivism.htm**
Motivation:	Blocking donations to WikiLeaks
Type of Attack:	DDoS
Any other groups claiming responsibility:	LulzSec – alluded to in reports, not formally claimed.
Damage Caused	Reported that the site was down for 2 hours.
Additional Important Information:	

30. Anonymous

Target	PayPal
Date:	6-9th December 2010
Source:	Leyden, J 6/12/2010, 20/7/2011, "Anonymous attacks PayPal in 'Operation Avenge Assange'", The Register: http://www.theregister.co.uk/2010/12/06/anonymous_launches_pro_wikileaks_campaign/ "FBI Cracks Down on 'Anonymous' Over PayPal Hacking, Arrests 14", International Business Times: **http://www.ibtimes.com/articles/183495/20110720/federal-bureau-of-investigation-fbi-paypal-online-security-anonymous-hacking-cyber-attack-wikileaks.htm**
Motivation:	Operation Avenge Assange – Retaliation for blocking WikiLeaks donations
Type of Attack:	DDoS
Any other groups claiming responsibility:	no
Damage Caused	Reported that the attack lasted about 8 hours and resulted in numerous disruptions. There was no substantial clarification in what these disruptions entailed.

Additional Important Information:	14 alleged members of anonymous charged for intentional damage to protected computers, which carries a maximum penalty of 10 years (5 for conspiracy) imprisonment and a $250000 fine.

31. Anonymous

Target	Sony
Date:	4th April 2011
Source:	Mick, J 4/4/2011, "Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit", Daily Tech: http://www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm 20/7/2011, "FBI Cracks Down on 'Anonymous' Over PayPal Hacking, Arrests 14", International Business Times: **http://www.ibtimes.com/articles/183495/20110720/federal-bureau-of-investigation-fbi-paypal-online-security-anonymous-hacking-cyber-attack-wikileaks.htm**
Motivation:	Retaliation for Sony taking legal action against George Hotz, a coder who wrote a tool that "allows *homebrew* software to run on the PlayStation 3 (PS3)." The tool allows for the use of 3rd party software on the consoles.
Type of Attack:	DDoS, data theft, unauthorised access.
Any other groups claiming responsibility:	LulzSec
Damage Caused	PS3 online capabilities were disrupted for almost a month.
Additional Important Information:	Compromised personal data of 77 million users worldwide and considered the largest breach of its kind to date.

32. LulzSec

Target	Sony BMG - Greece
Date:	22nd May 2011
Source:	Wisniewski, C 22/5/2011, "Sony BMG Greece the latest hacked Sony site", Naked Security: http://nakedsecurity.sophos.com/2011/05/22/sony-bmg-greece-the-latest-hacked-sony-site/ **Mills, E 6/6/2011, "Hackers taunt Sony with more data leaks, hacks", CNET: http://news.cnet.com/8301-27080_3-20069443-245/hackers-taunt-sony-with-more-data-leaks-hacks/**
Motivation:	
Type of Attack:	SQL injection, unauthorised access, data leak
Any other groups claiming responsibility:	
Damage Caused	Release of "usernames, real names and email addresses of users registered on SonyMusic.gr." Release of internal network map
Additional Important Information:	Large quantity of information reported to be incorrect.

33. Anonymous

Target	Mastercard, Visa, Swedish prosecutor's office, Sara Palin website
Date:	8-9th December 2010
Source:	9/12/2010, "'Anonymous' hackers hit Visa, Mastercard and Sarah Palin in WikiLeaks revenge", The Australian: http://www.theaustralian.com.au/in-depth/wikileaks/anonymous-hackers-hit-visa-mastercard-in-wikileaks-revenge/story-fn775xjq-1225968083650
Motivation:	Retaliation for blocking funding to WikiLeaks – Operation Payback; also for open opposition to Julian Assange.
Type of Attack:	DDoS
Any other groups claiming responsibility:	no
Damage Caused	• Mastercard's main site was down for 7 hours on the 8th. • Visa's site was down for 2> hours on the 9th. • Sara Palin's site was down for 6 minutes; additionally, her and her husband's bank accounts were disrupted. • Swedish prosecutor's office website was taken offline for an unspecified period of time.
Additional Important	"Icelandic firm DataCell said it would sue Visa for blocking payments to WikiLeaks and accused the credit card giant of bowing to political pressure."

Information:	

34. LulzSec

Target	Infragard (Atlanta) – FBI affiliate
Date:	3rd June 2011
Source:	**Beschizza, R 3/6/2011, "LulzSec claims FBI affiliate hacked, users and botnet are exposed", Boing Boing: http://boingboing.net/2011/06/03/LulzSec-claims-fbi-a.html**
Motivation:	
Type of Attack:	Unauthorised access, data leak, modification of data, defacement.
Any other groups claiming responsibility:	No
Damage Caused	Released personal information on the user database of 180 users, defaced http://infragardatlanta.org/, reputational damage – who do you believe?
Additional Important Information:	

35. LulzSec

Target	PBS
Date:	29-30th May 2011
Source:	**Wisniewski, C 30/5/2011, "PBS.org hacked... LulzSec targets Sesame Street?", Naked Security: http://nakedsecurity.sophos.com/2011/05/30/pbs-org-hacked-LulzSec-targets-sesame-street/** Ragan, S 30/5/2011, "PBS: LulzSec attack an attempt to chill journalism", The Tech Herald: http://www.thetechherald.com/article.php/201122/7215/PBS-LulzSec-attack-an-attempt-to-chill-journalism
Motivation:	"took offense to the portrayal of Bradley Manning in a segment on PBS's Frontline news magazine program"; Anti-WikiLeaks protests
Type of Attack:	"They claim they used a zero day exploit in Movable Type 4 and were able to compromise Linux servers running outdated kernels."
Any other groups claiming responsibility:	no
Damage Caused	Released login credentials of database administrators/users as well as those of affiliates; defaced/injected their own website
Additional Important Information:	

36. LulzSec

Target	CIA www.cia.gov
Date:	15th June 2011
Source:	15/6/2011, "LulzSec's CIA hack just one of many high-profile hackings", International Business Times: http://www.ibtimes.com/articles/163678/20110615/google-LulzSec-s-cia-hack-just-one-of-many-high-profile-hackings.htm **Schroeder, S 16/6/2011, "LulzSec Hackers Take Down CIA Website", Mashable: http://mashable.com/2011/06/16/LulzSec-hackers-cia/**
Motivation:	Unspecified
Type of Attack:	DDoS
Any other groups claiming responsibility:	no
Damage Caused	CIA website was inaccessible for an unspecified period of time, though reported as "several hours".
Additional Important Information:	

37. LulzSec

Target	Lockheed Martin
Date:	May 2011
Source:	**http://www.prnewswire.com/news-releases/LulzSec-and-anonymous-blur-lines-between-hacktivism-and-criminality-according-to-pandalabs-q2-report-125068654.html** **http://news.sky.com/home/technology/article/16099978**
Motivation:	Unknown
Type of Attack:	Unauthorised access,
Any other groups claiming responsibility:	
Damage Caused	Claims that no crucial data had been taken, though that "internal systems took a few days to fully recover"
Additional Important Information:	"Shortly after the breach, the UK government announced the formation of the National Cyber Security Programme, a special unit of the Ministry of Defence tasked with reducing the UK's vulnerability to cyber crime and attacks."

38. Unknown, but reported to be either LulzSec or Anonymous

Target	CitiBank
Date:	9th June 2011
Source:	**Cout, A 9/6/2011, "Citibank hacked, more than 200,000 bank customers**

	at risk", Digital Trends: http://www.digitaltrends.com/computing/citibank-hacked-more-than-200000-bank-customers-at-risk/
Motivation:	Unknown
Type of Attack:	Unauthorised access, data theft, data leak
Any other groups claiming responsibility:	
Damage Caused	Compromised information on names, account numbers and contact info of approximately 21 million accounts.
Additional Important Information:	

39. Unknown

Target	Sony Pictures Russia
Date:	6th June 2011
Source:	**Mills, E 6/6/2011, "Hackers taunt Sony with more data leaks, hacks", CNET: http://news.cnet.com/8301-27080_3-20069443-245/hackers-taunt-sony-with-more-data-leaks-hacks/**
Motivation:	Unknown
Type of Attack:	SQL injection
Any other groups claiming responsibility:	No
Damage Caused	Site inaccessible for an unspecified amount of time
Additional Important Information:	

40. The UnderTakers

Target	Sony Music Brazil - sonymusic.com.br
Date:	
Source:	**http://thehackernews.com/2011/06/sony-music-brazil-gets-defaced.html**
Motivation:	Unknown
Type of Attack:	SQL injection, unauthorised access, defacement
Any other groups claiming responsibility:	
Damage Caused	Website down for over 12 hours
Additional Important Information:	

41. Anonymous

Target	Neo-Nazi websites
Date:	8th August 2011
Source:	**11/7/2011, "Anonymous Hackers hack neo-Nazis websites & leak personal info of 16,000 Finns", The Hacker News: http://thehackernews.com/2011/11/anonymous-hackers-hack-neo-nazis.html**
Motivation:	"…apparent desire to shame the Finnish government into improving data security."
Type of Attack:	Unauthorised access, defacement, data leak
Any other groups claiming responsibility:	
Damage Caused	Released user info on 16000 members
Additional Important Information:	

42. 3xp1r3 Cyber Army

Target	Bangladesh Supreme Court official website
Date:	10th November 2011
Source:	**11/11/2011, "Bangladesh Supreme Court website hacked", The Hacker News: http://thehackernews.com/2011/11/bangladesh-supreme-court-website-hacked.html**
Motivation:	Apparently letting admins know that the site was insecure
Type of Attack:	Unauthorised access, defacement
Any other groups claiming responsibility:	
Damage Caused	Website defaced for unspecified period of time. No data leaked or deleted.
Additional Important Information:	

43. Anonymous – Operation Brotherhood Shutdown

Target	Muslim Brotherhood websites
Date:	11th November 2011
Source:	**http://thehackernews.com/2011/11/operation-brotherhood-shutdown-by.html**

Motivation:	
Type of Attack:	
Any other groups claiming responsibility:	
Damage Caused	
Additional Important Information:	

44. Unknown

Website "Kommersant" under prolonged hacker intrusion. As a result of DNS poisoning users visiting the online news website http://www.kommersant.ru/ were redirected to a page. The page consisted of a political cartoon and rhetoric calling for public gathering in St. Petersburg and Moscow to protest the "falsified <corrupt> elections". The CEO of the publishing company Kommersant commented that the company contacted the law enforcement agency.

[redacted]	[redacted]
Case Name:	
Citation:	Sergey Smirnov, 'Website "Kommersant" under prolonged hacker intrusion.' (December 1, 2011) Vedomosti <http://www.vedomosti.ru/tech/news/1440499/kommersant_podvergsya_hakerskomu_dejstviyu_s_vidimostyu > at 2 December 2011.
Jurisdiction:	
Main URL:	http://www.vedomosti.ru/tech/news/1440499/kommersant_podvergsya_hakerskomu_dejstviyu_s_vidimostyu
Charged With:	
Legislative Provisions:	
Typology:	
Main Target:	Attack on the news website of a publishing company "Kommersant". DNS poisoning redirecting users to a webpage calling for public gathering against "falsified elections" - upcoming legislative elections. The company contacted law enforcement agency.
Motivation:	Political
Convicted of:	
Sentence:	
Additional Important Information:	

45. The Man From Leningrad

The official website of the soccer club "Zenit" hacked by foul-mouthed hackers.

A Person calling himself "a man from Leningrad" gained access to the official website of "Zenit" soccer club and posted insults towards the governor of St. Petersburg Valentina Matvienko and the speaker of the Legislative Assembly Vadim Tulipov. The text of the page suggested citizens take their ballots home to "prevent them from stealing your … choice" (appears to be for local city elections). Management of the soccer club contacted Russian law enforcement knows as "Division K". (http://kguvd.ru/ essentially the subdivision of Russia's criminal police branch dealing with cyber crime).

Case Name:	
Citation:	'The official website of the soccer club "Zenit" hacked by foul-mouthed hackers.' (April 6, 2011) Newsru (http://www.newsru.com) <http://www.newsru.com/sport/06apr2011/zenit.html > at 4 December 2011.
Jurisdiction:	
Main URL:	http://www.newsru.com/sport/06apr2011/zenit.html
Charged With:	
Legislative Provisions:	
Typology:	
Main Target:	Website of the soccer club "Zenit" was hacked. An unknown person posted insults towards the governor and the speaker of the legislative assembly and suggested voting party other than United Russia or taking their ballots home.
Motivation:	
Convicted of:	
Sentence:	
Additional Important Information:	

46. Unknown

DDoS attack before the elections. A popular blogging platform LiveJournal was under DDoS attacks a week before Russian legislative elections. LiveJournal is a popular platform for political discussions and the attack did not surprise political scientists in Russia. This was not the first time LiveJournal is under attack, although unlike previous attack against the most popular bloggers, current DDoS attack was against the whole platform. During the spring attack of 2011 the journal of a Russian president Medvedev was offline. Medvedev called these attacks "outrageous and illegal" as they annoy the users, who see government behind such attacks. While political scientist are convinced that this attack was politically motivated to deny any last minute campaign outreach before the December legislative elections, IT specialists are more skeptical.

Case Name:	
Citation:	Anastasiya Matveeva 'DDoS attack before the elections' (November 28, 2011) Gazeta.ru (http://gazeta.ru) <http://www.gazeta.ru/news/lastnews/2011/11/28/n_2113590.shtml> at 4 December 2011.
Jurisdiction:	
Main URL:	http://www.gazeta.ru/news/lastnews/2011/11/28/n_2113590.shtml
Charged With:	
Legislative Provisions:	
Typology:	
Main Target:	Popular blogging platform LiveJournal was under a DDoS attack before the legislative elections in Russia. Political scientists are convinced that the motivation behind the attack is political in nature, while IT experts state that there might be different reasons.
Motivation:	political
Convicted of:	
Sentence:	
Additional Important Information:	

47. Chinese Hacktivism

Target	Mengnui
Date:	December 28, 2011
Source:	"Hacktivism Spreads to China? Mengnui Hacked in Protest of 2nd Milk Scandal" http://web2asia.blognhanh.com/2011/12/hacktivism-spreads-to-china-mengniu.html
Motivation:	Apparently letting admins know that the site was insecure
Type of Attack:	Unauthorised access, defacement
Any other groups claiming responsibility:	None
Damage Caused	Website defaced with statements ""Do you have a conscience?" and "this is our national shame."
Additional Important Information:	Mengnui had a second milk scandal where their milk contained high levels of carcinogens.

15. Appendix C – Questionnaire

Question 1: Has there been an erosion of a common hacker ethos or has the ethos merely evolved into many different sets of ethics?

Question 2: In your experience with hackers, does the law offer a deterrent?

Question 3: Based on your experience interviewing hackers, what are their perceptions of the illegality of their activity?

Question 4: What types of hacking activity would you consider "ethical"?

Question 5: Should ethical hacking be exempt from cybercrime provisions, and if so what kinds of ethical hacking?

Question 6: Do you equate some forms of ethical hacking as the electronic equivalent of civil disobedience (sit-ins, protests) and if so, should the current civil disobedience framework apply to the online setting?

Question 7: Is there a need for security research exemption in cybercrime provisions (unauthorised access)?

Question 8: Is there a need for a public interest exemption in cybercrime provisions (unauthorised access)?

Question 9: Is there any advice in general that you wish to impart to those engaged in ethical hacking?

Question 10: Is there any advice in general that you wish to impart to governments and organisations in dealing with ethical hacking?

16. References

Legislation and Treaties

Convention to the *International Covenant on Civil and Political Rights*, 999 UNTS 302 (1967).

Council of Europe Convention on Cybercrime, 22296 UNTS 167 (2001).

Criminal Code 1995 (Cth).

Model Criminal Code (January 2001).

Caselaw

Bank Julius Baer & Co. Ltd. v. WikiLeaks (2008) U.S. Dist. LEXIS 14758 United States District Court for the Northern District of California

e360 INSIGHT and David Linhardt v. The Spamhaus Project, United States Court of Appeals for the Seventh Circuit, 500 F. 3d 594; 2007 U.S. App. LEXIS 20725.

E360 Insight, LLC et al v. The Spamhaus Project, US District Court, Northern District of Illinois, 13 September 2006 (Case no. 06 C 3958). Access to default judgment at http://www.spamhaus.org/archive/legal/Kocoras_order_to_Spamhaus.pdf..

Glaria (Gator) v Internet Advertising Bureau.

In re § 2703(d) Order, 2011 U.S. Dist. LEXIS 25322.

McAuliffe v The Queen [1995] 183 CLR 108.

McCabe v British American Tobacco Services Limited [2002] VSC 73.

Microsoft Corporation v. John Does 1027 (Feb. 22, 2010) United States District Court for the State of Victoria, Civil Action 1:10 cv 156 (LMB/JFA).

Microsoft Corporation v Newport Interenet Marketing Corporation Does 2-20 King County Superior Court Seattle, Washington (2005) No. 03-2-12648-9 SEA. A copy of these court records may be found at http://4431647708582819520-a-1802744773732722657-s-sites.googlegroups.com/site/sjwest01/court.html?attachauth=ANoY7cr1KKGuLVCCDxAl6bNx-v95BNUiKBf2bIcFSmkkVrd-AaSbI221syEjJVdydf8eJc2TGS1VS08Y5HgucrxNIXJ-plhp65AsGtlaDrCOKfE_SLPwADmGmrJnDpt28IIOgiEVoNi0tUoo-wDWpetUHTYvZvnsIJQxRqQcRB0wUisYBRS0pUcJw07tH2zQgxbdntG3qy3a&attredirects=1 (last accessed October 26, 2010).

Paracha v. Obama (2011) U.S. Dist. LEXIS 46104 United States District Court for the District of Columbia

Regan Gerard Gilmour v Director of Public Prosecutions (Commonwealth) [1996] NSWSC 55.

R v. Caffrey (2006).

R v Stevens [1999] NSWCCA 69.

R. *v. Walker*, HC HAM CRI2008-0750711 [2008] NZHC 1114.

Salter v DPP [2008] NSWSC 1325.

Sierra Corporate Design Inc. v. David Ritz, (2007) District Court, County of Cass, State of North Dakota, File No. op-05-C-01660 *See* www.spamsuite.com.com/node/351.

Specht v. Netscape Communications Corp., 306 F. 3d 17 - Court of Appeals, 2nd Circuit 2002.

State of Israel vs Anat Kam (2011) (Israel – Tel Aviv District Court).

United States Army v. Bradley Manning

United States v Gorshkov (2001) WL 1024026 (Western District Washington).

United States v. Jarrett (2003) 338 F. 3d 339 (Court of Appeals 4th Circuit).

United States v Kevin George Poe (2011) CR 11 01166 (US District Court for the Central District of California)

United States v. Steiger (2003) 318 F. 3d 1039 (Court of Appeals 11th Circuit).

Zitierung: BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (

Books

The Oxford Pocket Dictionary of Current English (2009).

AITCHISON, R., "DNS Records" in *Pro DNS and BIND* (Apress Publishers, 2003).

ANDERSON, R., *Security Engineering: A Guide to Building Dependable Distributed Systems* 2nd ed (Indianapolis: Wiley Publishing, 2008).

ATHANASOPOULOS, E., ANAGNOSTAKIS, K., and MARKATOS, E., "Misusing Unstructured P2P Systems to Perform DoS attacks: The Network that Never Forgets" (2006) Lecture Notes in Computer Science for *Applied Cryptography and Network Security* (Springer Berlin) available at http://www.springerlink.com/content/xk82663475474857/.

ATKIN, T.. et al., *Information Security Management Handbook* (CRC Press, 2006).

BARLOW, J.P. "Crime and Puzzlement" Appendix 1 in LUDLOW, P. (ed) *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (MIT Press, 1996).

BARTON, P. And YEGNESWARAN, V., "An Inside Look at Botnets" in SOMESH, J., MAUGHAN, D., SONG, D., and WANG, C. (eds) *Malware Detection* (New York: Springer, 2007).

BENTHAM, J. *Panopticon, i*n Miran Bozovic (ed.), *The Panopticon Writings* (London: Verso, 1995), 29-95.

BLOUNT, S. *Electronic Contracts: Principles for the Common Law* (Australia: Reed International Books, 2009).

BOWREY, K., *Law & Internet Cultures* (Cambridge University Press, 2005).

CHAN, J., GOGGIN, G., and BRUCE, J., "Internet Technologies and Criminal Justice" in Jewkes, Y. and Yar, M., *Handbook of Internet Crime* (Willan Publishing 2010).

CHIESA, R., DUCCI, S., CIAPPI, S., Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking (UNICRI and CRC Press, 2009).

CLAYTON, R. "Failures in a Hybrid Content Blocking System in DANEZIS, G. And MARTIN, D. (eds) *Privacy Enhancing Technologies* (June 30 2005) volume 3856 of LNCS (Springer).

COHEN, F., *A Short Course on Computer Viruses* 2nd ed (Wiley, 1994).

CORONES, S and CLARKE, P. *Consumer Protection and Product Liability Law 3rded* (Thomson Lawbook, 2008).

CURCEREAU, D. *Aspects of Regulating Freedom of Expression on the Internet* (Intersentia, 2006)

DREYFUSS, S. and ASSANGE, J. Underground (Random House Australia, 2011)

DUNHAM, K. and MELNICK, J. *Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet* (CRC Press, 2009) page 132.

FITZGERALD, B., FITZGERALD, A., MIDDLETON, G., LIM, Y. and BEALE, T., *Internet and E-Commerce Law: Technology, Law and Policy* (Thomson 2007).

FLEMING, J., *The Law of Torts 8th ed* (The Law Book Company 1992).

GARFINKEL, S. and SPAFFORD, G. *Practical UNIX & Internet Security*, 2nd Ed (California: O'Reilly, 1996).

GODWIN, M. "Some 'Property' Problems in a Computer Crime Prosecution" in LUDLOW, P. (ed) *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (MIT Press, 1996).

GRABOSKY, P., *Electronic Crime* (Prentice Hall, 2007).

HARRIS, S., HARPER, A., EAGLE, C. and NESS, J. *Grey Hat Hacking: The Ethical Hacker's Handbook* (McGraw Hill 2008).

HIMANEN, P. *The Hacker Ethic: and the Spirit of the Information Age* (Random House, 2001).

KERR, I., and GILBERT, D., "The Role of ISPs in the Investigation of Cybercrime" in MENDINA, T., and BRITZ, J. (eds) *Information Ethics in an Electronic Age: Current Issues in Africa and the World* (McFarland Press, 2004).

LEVY, S. *Hackers: Heroes of the Computer Revolution* (New York: Doubleday, 1984).

LEVY, A. *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (Viking, 2001).

LIBICKI, M. *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge 2007).

LI, Z., LIAO, Q., and STRIEGEL, A., *Botnet Economics: Uncertainty Matters* (Springer 2009).

LUDWIG, M., *The Giant Black Book of Computer Viruses* 2nd ed. (American Eale, 1998).

LYNCH, A., and WILLIAMS, G., *What Price Security?* (UNSW Press, 2006).

MALCOM, J. *Multi-Stakeholder Governance andthe Internet Governance Forum* (Terminum Press 2008).

MAURUSHAT, A. 2011. "Australia" in *Freedom on the Internet: A Global Assessment of Internet and Digital Media*, Cook S. (ed) (New York: Freedom House, 2011).

MATSWSHYN, A.(ed) *Harboring Data: Information Security, Law, and the Corporation* (Stanford University Press, 2009).

MUELLER, M. *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Massachusetts Institute of Technology, 2002).

ORAM, A. (Ed) *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (O'Reily & Associates: Sebastopol, 2001).

PFLEEGER, C. and PFLEEGER, S. *Security in Computing* 4th Ed. (Prentice Hall, 2006).

PHAIR, N. *Cybercrime: The Reality of the Threat* (self-published 2007).

POULSEN, K., *Kingpin: The True Story of Max Butler, the Master Hacker who Ran a Billion Dollar Cyber Crime Network* (Hachett, 2011).

PROVOS, N. and HOLZ, T., *Virtual Honeypots: From Botnet Tracking to Intrusion Detection* (Safari 2008).

RAYMOND, E. *The Cathedral & the Bizaar: Musings on Linux and Open Source By an Accidental Revolutionary* (O'Reily, 2001).

REYES, A. O'SHEA, K., STEELE, J., HANSEN, J., JEAN, B. and RALPH, T., *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors* (Syngress 2007).

RICE, D., *Geekonomics: The Real Cost of Insecure Software* (Addison-Wesley, 2008).

ROSS, S., *UNIX System Security Tools* (McGraw-Hill, 1999).

SALTZER, J., REED, D. and CLARK, D., "End-to-End Arguments in System Design", in PARTRIDGE, C., ed, *Innovations in Internetworking* (Artech House, 1988).

SAMUELS, A. *Hacktivism and the Future of Political Participation* (PhD Thesis, Harvard, 2004).

SCHILLER, C., BINKLEY, J., HARLEY, D., EVRON, G., BRADLEY, T., WILLEMS, C., and CROSS, M., *Botnets: The Killer Web App* (Syngress 2007).

SCHNEIER, B., *Secrets and Lies* (Robert Ipsen 2000).

SCHILLER, C., BINKLEY, J., HARLEY, D., EVRON, G., BRADLEY, T., WILLEMS, C., and CROSS, M., *Botnets: The Killer Web App* (Syngress 2007).

SINGH, S. The *Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptopgraphy* (Doubleday, 1999).

SMITH, R., GRABOSKY, P., and URBAS, G. *Cyber Criminals on Trial* (Cambridge University Press, 2004).

TAYLOR, P., " Hacktivism: In Search of Lost Ethics?" in *Crime and the Internet* (London & New York: Routledge).

THOREAU, H.D. *Resistance to Civil Government* (original title 1849) but now known as Civil *Disobedience: On the Duty of Civil Disobedience* available at http://www.transcendentalists.com/civil_disobedience.htm

TIEN, L., "Architectural Regulation and the Evolution of Social Norms" in BALKIN, J., GRIMMELMANN, J., KATZ, E., KOZLOVSKI, N., WAGMAN, S., and ZARSKY, T. (eds) *Cybercrime: Digital Cops and Laws in a Networked Environment* (New York University Press, 2006).

WALDEN, I. "Computer Forensics and the Presentation of Evidence in Criminal Cases" in JEWKES, Y. and YAR, M. *Handbook of Internet Crime* (Willan Publishing, 2010).

WALL, D., *Cybercrime: Crime and Society Series* (Polity Press, 2007).

YAR, M., "The Private Policing of Internet Crime" in JEWKES, Y. and YAR, M. (eds) *Handbook of Internet Crime* (Willan Publishing, 2010).

YAR, M., "Public Perception and Public Opinion about Internet Crime" in JEWKES, Y. and YAR, M., *Handbook of Internet Crime* (Willan Publishing 2010), pages 104-120.

YEGNESWARAN, V. And BARFORD, P., "An Inside Look at Botnets" in CHRISTODORESCU, M., JHA, S., MAUGHAN, D., SONG, D. And WANG, C. Eds. *Advances in Information Security: Malware Detection* (2007).

Journal Articles

ANDERSON, K. "Hacktivism and Politically Motivated Computer Crime" (Ensurve 2008) available at http://politicalhacking.blogspot.com.

BAMBAUER, D. and DAY, O., "The Hacker Aegis" (2011) 60 Emory Law Journal.

BRENNER, S. W., CARRIER, B. and HENNINGER, J. "The Trojan Horse Defense in Cybercrime Cases" (2004) 21 *Santa Clara Computer and High Technology Law Journal.*

BRENNER, S.W., *Law in an Era of "Smart" Technology* (2007) 173.

BROADHURST, R., 'Developments in the Global Law Enforcement of Cyber-Crime' (2006) 29(3) *Policing: An International Journal of Police Strategies and Management* 408, page 418.

CHANDLER, J. "Liability for Botnet Attacks" (2006) *Canadian Journal of Law and Technology*

CHANDLER, J. "Security in Cyberspace: Combating Distributed Denial of Service Attacks" (2003-2004) 1 *University of Ottawa Law & Technology Journal* 231.

CHANDLER, J., "Technological Self-Help and Equality in Cyberspace" (2010) 55 *McGill Law Journal.*

CLARKE, R. "Information Technology and Dataveillance" (1988) *Communications of the ACM*, Vol. 31(5), p. 499.

CLARKE, R. and MAURUSHAT, A., "The Feasibility of Consumer Device Security" (2009) *UNSW Law Review Series* 5.

CLARKE, R. and MAURUSHAT, A., "Who Will Bear the Cost of Insecure Devices" (2007) 18 *Journal of Law, Information and Science* 8.

CLAYTON, R. "Complexities in Criminalising Denial of Service Attacks" written for the *Legal Subgroup of the Internet Crime Forum* (Feb. 2006) available at www.cl.ram.ac.uk/~rncl/complexity.pdf (last accessed April 27, 2010).

COHEN, F., "Computer Viruses: Theory and Experiments" (1987) *Computers & Security*, 6(1).

COLANGELO, A. and MAURUSHAT, A., "Exploring the Limits of Computer Code as a Protected Form of Expression: A Suggested Approach to Encryption, Computer Viruses and Technological Protection Measures" (2006) 1 *McGill Law Journal* 51.

DAVIS, N., "Presumed Assent: The Judicial Acceptance of Clickwrap" (2007) 22 *Berkeley Technology Law Journal* 577.

DENNING, D., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" (2001) available at http://www.nautilus.org/infor-policy/workshop/papers/denning.html.

DE VILLIERS, "Distributed Denial of Service: Law, Technology & Policy" (2006) *World Jurist Law/Technology Journal* v. 39 n. 3

DE VILLIERS, "Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare" (2005) 4 *Northwestern Journal of Technology and Intellectual Property* 1

DE VILLIERS, "Reasonable Foreseeability in Information Security Law: A Forensic Analysis" (2008) 30 *Hastings Communications And Entertainment Law Journal.*

DE VILLIERS, M. "Virus Ex Machine Res Ipsa Loquitor" (2003) S*tanford Technology Law Review* 1

EDWARDS, L. "Dawn of the death of Distributed Denial of Service: How to Kill Zombies" (2006) 24 *Cardozo Journal of Arts and Entertainment Law* 23.

EPSTEIN, R., "The Theory and Practice of Self-Help" (2005)1(1) Journal of Law, Economics and Policy 1.

EVRON, G., "Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War," (2008) *Georgetown Journal of International Affairs*, Volume IX, Number 1.

FITRI, N., "Democracy Discourses Through the Internet Communication: Understanding the Hacktivism for the Global Changing" (2011)1 Online Journal of Communication and Media Technologies 2.

GEIST, M., "Is There a There There: Toward Greater Certain for Internet Jurisdiction" (Fall 2001) Berkely Technology Law Journal.

GILBERT, D. And KERR, I. "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" Vol. 51(4) *Criminal Law Quarterly*.

GUZMAN, L., "Unleashing a Cure for the Botnet Zombie Plague" (2010) 59 *Catholic University Law Review* 527.

HAFELE, D., "Three Different Shades of Ethical Hacking: Black, White and Grey" (Feb. 23, 2004) available at http://www.sans.org/reading_room/whitepapers/hackers/shades-ethical-hacking-black-white-grey_1390.

HANCOCK-WHITE, K,. "Ethical Hacking" 2008 available at *casper182.atspace.com/HancockWhite_ethics_paper.doc*

HARDY, K., "Operation Titstorm: Hacktivism or Terrorist Act?" (2010) *University of New South Wales Law Journal* 16:1.

HIMMA, K., "Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?" (2005) ETHICOMP Conference, Linkoping, Sweden.

HUTCHINSON, W. And WARREN, M., "Attitudes of Australian Information System Managers Against Online Attackers" (2001) 9(3) *Information Management & Computer Security* 106.

Imperva, "Hacker Intelligence Initiative" (October 2011) Monthly Trend Report #5.

JOHNSTON, L., "What is Vigilantism?" (1996) *British Journal of Criminology*, vol. 26, No. 2.

JORDAN, T., "Mapping Hacktivism" (2001) 4 Computer Fraud and Security.

KASPERSKY, E., "Cruncher – the First Beneficial Virus?" (1993) *Virus Bulletin*.

KATYAL, N. "Criminal Law in Cyberspace" (2001) 149 *University of Pennsylvania Law Review* 1004.

KERR, O. "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes" (2003) *New York University Law Review*, Vol. 78, No. 53.

KERR, O., "Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability" (2005) 1 *Journal of Law, Economics and Policy* 197.

LESSIG, L., "Reading the Constitution in Cyberspace" (1997) 45 *Emory Law Journal* 1.

LESSIG, L. and RESNICK, P.,"`The Architectures of Mandated Access Controls" available at http://cyber.law.harvard.edu/works/lessig/Tprc98_d.pdf.

LESSIG, L., "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 *Harvard Law Review* 501.

LIN, P., "Anatomy of the Mega-D Takedown" (December, 2009) 12 *Network Security*, pages 4-7.

LUTHER KING, Jr., M., "Letters From a Birmingham Jail" (April 16, 1963) available at The Martin Luther King, Jr. Research and Education Institute http://mlk-kpp01.stanford.edu/index.php/resources/article/annotated_letter_from_birmingham

MAURUSHAT, A. "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in the Era of Obfuscation Crime Tools" (2010) *University of New South Wales Law Journal* 16:1.

MAURUSHAT, A., "Data Breach Notification Law Across the World from California to Australia" (April, 2009) *Privacy Law and Business International.*

MAURUSHAT, A. "Hong Kong Anti-Terrorism Ordinance and the Surveillance Society: Privacy and Free Expression Implications" *Asia Pacific Media Educator*, Vol. 1, Iss. 12/3 (2002).

MAURUSHAT, A. and WATT, R., "Australia's Internet Filtering Proposal in the International Context" (2009) 12(2) *Internet Law Bulletin* 18.

OHM, P. "The Rise and Fall of Invasive ISP Surveillance" available at http://ssrn.com/abstract=1261344 (last accessed April 15, 2009).

OLESON, K. and DARLEY, J., "Community Perceptions of Allowable Counterforce in Self-Defense and Defense of Property"(1999) *Law and Human Behavior*, 23.

POSNER, R., "Killing or Wounding to Protect a Property Interest" (1971) 14 *Journal of Law and Economics* 201.

RYCHLICKI, T. "Legal Issues of Criminal Acts Committed Via Botnets." (2006) *Computer and Telecommunications Law Review* 12(5), p. 163.

ROSE, C., and GORDON, J., "Internet Security and the Tragedy of the Commons" (2003) 1 Journal of Business and Economics Research 11.

SALGADO, R., "The Legal Ramifications of Operating a Honeypot" (2005) *IEEE Magazine Security and Privacy*, vol. 1.

Security Spotlight, "Even Governments are not Immune to Hacktivism" (Feb. 8, 2010).

SHOCK, J. and HUPP, J., "The 'Worm' Programs – Early Experience with a Distributed Computation" (1982) *Communications of the ACM*, 25(3).

SMITH, B., "Hacking, Poaching and Counterattacking: Digital Counterstrikes and the Contours of Self-Help" (2005) 1(1)*Journal of Law, Economics and Policy* 185.

SMITH, H., "Self-help and the Nature of Property" 2005) 1(1)*Journal of Law, Economics and Policy* 69.

SOLOMON, A. and EVRON, G., "The World of Botnets" *Virus Bulletin* September 2008.

SOLOVE, D. "Privacy and Power: Computer Databases and Metaphors for Information Privacy", (2001)53 *Stanford Law Review* 1393.

STEEL, A., "The Meaning of Dishonesty in Theft" (2009) *Common Law World Review*, 38(2).

THOMAS, J., "Ethics of Hacktivism" (2001) SANS Institute InfoSec Reading Room.

US-Cert (United States Computer Emergency Readiness Team), *Quarterly Trends and Analysis Report* (2007) volume 2, Issue 4.

VAN EETEN, M., BAUER, J., ASGHARI, H., TABATABAIE, S., "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data" (2010) *OECD Science, Technology and Industry Working Papers*, 2010/5, OECD Publishing.doi: 10.1787/5km4k7m9n3vj-en

VAUGHN, Z., "Hacktivism: Civil Rights Activism in the Digital Age"

WALDEN, I. And FLANAGAN, A. "Honeypots: A Sticky Legal Landscape?" 29 *Rutgers Communications and Technology Law* 315 (2003).

WARREN, S. and BRANDEIS, L., "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.

WINN, J. "Are 'Better' Security Breach Notification Laws Possible?" (2009) *Berkeley Technology Law Journal* Volume 24:3.

WRAY, S., "Electronic Civil Disobedience and the World Wide Web of Hacktivism" A Mapping of Extraparliamentarian Direct Action Net Politics" (November, 1998) available at http://www.nyu.edu.projects/wray/wwwhack.html.

WU, T., "Application-Centered Internet Analysis" (1999) 85 *Vanderbuilt Law Review* 1163.

YOUNG, J. 'Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation' (2004) 9 *International Journal of Communications Law and Policy.*

YOUNG, J., "Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation – A Critical Anlaysis of the Council of Europe Convention on Cybercrime and the Canadian Lawful Access Proposal" (2004-2005) *Yale Journal of Law and Technology* 346.

ZENZ, K., "Cyber Crime Within the Russian Federation" presentation at *AusCERT 2008*.

Websites and Articles Published Online

"4Chan Hacks Anti Piracy Lawfirm, Leaks Porn Downloaders' Names", (approximately 23 November 2010) *BuzzFeed* available at http://www.buzzfeed.com/wecanchangetheworld/4chan-hacks-anti-piracy-lawfirm-leaks-porn-downlo-1q36 (last accessed 21 November 2011).

"'Anonymous' hackers hit Visa, Mastercard and Sarah Palin in WikiLeaks revenge", (9 December 2010) *The Australian* available at http://www.theaustralian.com.au/in-depth/wikileaks/anonymous-hackers-hit-visa-mastercard-in-wikileaks-revenge/story-fn775xjq-1225968083650 (last accessed 10 December 2010).

"Anonymous Attacks Anonymous for Being Trolls" (16 November 2011) *Softpedia* available at http://news.softpedia.com/news/Anonymous-Attacks-Anonymous-For-Being-Trolls-234949.shtml (last accessed 18 November 2011).

"Anonymous busts Internet pedophiles" (3 November 2011) *RT* available at http://rt.com/usa/news/anonymous-child-tor-porn-513/ (last accessed 15 November 2011).

"Anonymous Hackers hack neo-Nazis websites & leak personal info of 16,000 Finns", (11 July 2011) *The Hacker News* available at http://thehackernews.com/2011/11/anonymous-hackers-hack-neo-nazis.html

"Anti-Gay Website Hacked by Anonymous" (4 June 2011) *lezbelib.over-blog.com* available at http://lezbelib.over-blog.com/article-anti-gay-website-hacked-by-anonymous-75636306.html (last accessed 5 June 2011).

"Baidu hacked by 'Iranian cyber army'", (12 January 2010) *BBC News* available at http://news.bbc.co.uk/2/hi/8453718.stm (last accessed 13 January 2010).

"Bangladesh Supreme Court website hacked" (11 November 2011) *The Hacker News* available at http://thehackernews.com/2011/11/bangladesh-supreme-court-website-hacked.html (last accessed 12 November 2011).

"BART drafts new policy on disruption of cellphone service" (19 October 2011) *LA Times* available at http://latimesblogs.latimes.com/lanow/2011/10/bart-outlines-cell-phone-service-disruption-policy.html (last accessed 20 October 2011).

BENDRATH, R. "Frankfurt Appellate Court Says Online Demonstration is Not Coercion" (June 7, 2006) Digital Civil Rights in Europe http://www.edri.org/edrigram/number4.11/demonstration

"CCC is at it again – hands out copies of German Interior Minister's fingerprint" (1 April 2008) *The Tech Herald* available at http://www.thetechherald.com/article.php/200814/581/CCC-is-at-it-again-hands-out-copies-of-German-Interior-Minister-s-fingerprint (last accessed 15 July 2010).

"Customs Authority of Yemen Hacked for Protests against Government", (8 May 2011) The Hacker News available at http://thehackernews.com/2011/08/customs-authority-of-yemen-hacked-for.html (last accessed 9 May 2011).

"Cyber-Warfare: The New Global Battlefield" (31 October 2011) *news.sky.com* available at http://news.sky.com/home/technology/article/16099978 (last accessed 2 November 2011).

"FBI Cracks Down on 'Anonymous' Over PayPal Hacking, Arrests 14", (20 July 2011) *International Business Times* available at http://www.ibtimes.com/articles/183495/20110720/federal-bureau-of-investigation-fbi-paypal-online-security-anonymous-hacking-cyber-attack-wikileaks.htm (last accessed 21 July 2011).

"Hacker History & Culture" *H@cker's Handbook* available at http://www.telefonica.net/web2/vailankanni/HHB/HHB_CH03.htm (last accessed 5 January 2012).

"Hackers hit government Web sites after China embassy bombing", (9 May 1999) *CNN Tech* available at http://articles.cnn.com/1999-05-10/tech/9905_10_hack.attack.02_1_hackers-government-web-sites-interior-department-web?_s=PM:TECH (last accessed 10 November 2011).

"Is Serco Behind Stuxnet" (thread started September, 2010 and ongoing) *AboveTopSecret* available at http://www.abovetopsecret.com/forum/thread615788/pg1 (last accessed February 7, 2011).

"Japanese Web Sites Hacked", (25 January 2001) *ABC News* available at http://abcnews.go.com/Technology/story?id=99306&page=1 (last accessed 14 November 2011).

"Lulzsec and Anonymous Blur Lines Between 'Hacktivism' and Criminality, According to PandaLabs Q2 Report" (6 July 2011) *PR Newswire* available at http://www.prnewswire.com/news-releases/lulzsec-and-anonymous-blur-lines-between-hacktivism-and-criminality-according-to-pandalabs-q2-report-125068654.html (last accessed 8 July 2011).

"LulzSec's CIA hack just one of many high-profile hackings", (15 June 2011) *International Business Times* available at http://www.ibtimes.com/articles/163678/20110615/google-lulzsec-s-cia-hack-just-one-of-many-high-profile-hackings.htm (last accessed 20 June 2011).

"Nepal Telecommunications Authority Hacked by w3bd3f4c3r", (21 August 2011) *Hacking Beast* available at http://www.hackingbeast.in/2011/08/nepal-telecommunications-authority.html (last accessed 22 August 2011).

"Online activists hack into Syrian government websites" (26 September 2011) *The Jerusalem Post* available at http://www.jpost.com/MiddleEast/Article.aspx?id=239552 (last accessed 27 September 2011).

"Operation Brotherhood Shutdown: Multiple Sites taken down by Anonymous Hackers", (12 November 2011) *The Hacker News* available at http://thehackernews.com/2011/11/operation-brotherhood-shutdown-by.html (last accessed 13 November 2011).

"Operation Rainbow Dark" *AnonNews* available at http://anonnews.org/?p=press&a=item&i=1162 (last accessed 5 January 2012).

"Owning Kraken Zombies: A Detailed Dissection" (April, 2008) *DVLabs* available at http://dvlabs.tippingpoint.com/blog/2008/04/28/owning-kraken-zombies (last accessed November 11, 2010).

"Second WikiLeaks payback vs. MasterCard: LulzSec or Anonymous?", (29 June 2011) *International Business Times* available at http://au.ibtimes.com/articles/170985/20110629/mastercard-citibank-lulzsec-anonymous-wikileaks-hack-hactivism.htm (last accessed 30 June 2011).

"TechCrunch Hacked? (yes,Techcrunch got hacked)" (26 January 2010) *TechnoFriends* available at http://technofriends.in/2010/01/26/did-techcrunch-got-hacked/ (last accessed 15 November 2010).

"The Complete History of Hacking" *Scribd.com* available at http://www.scribd.com/doc/48245151/The-Complete-History-of-Hacking-1980-2010 (last accessed 5 January 2012).

"Waledac Questions Answered" *LavaSoft* available at http://www.lavasoft.com/mylavasoft/company/blog/waledac-questions-answered.

"War Hack Attacks Tit For Tat", (28 March 2003) *Wired* available at http://www.wired.com/politics/law/news/2003/03/58275 (last accessed 10 November 2011).

"Website of the Presidency of Ecuador suffered cyber attacks", (20 June 2011) *El Universo* available at http://www.eluniverso.com/2011/06/20/1/1355/pagina-internet-presidencia-ecuatoriana-sufrio-ataque-informatico.html?p=1354&m=638 (last accessed 21 June 2011).

"Who are the 'Iranian Cyber Army'", (15 December 2010) *The Green Voice of Freedom* available at http://en.irangreenvoice.com/article/2010/feb/19/1236 (last accessed 16 December 2010).

ANDERSON, N. "Vint Cerf: one quarter of all computers part of a botnet" (January 25, 2007) *Ars Technica* available at http://www.arstechnica.com/news.ars/post/20070125-8707.html. (last accessed May 31, 2011).

BARLOW, J.P., "A Declaration of Independence in Cyberspace" *Humanist* 1996 available at http://editions-hache.com/essais/pdf/barlow1.pdf (last accessed 10 December 2011).

BARROSO, D. of the European Network and Information Security Agency, *Botnets – The Silent Threat* (2007) p. 6 available at http://www.enisa.europa.eu/act/res/other-areas/botnets/botnets-2013-the-silent-threat (last accessed January 29, 2010).

BERGEN, J 28 June 2011, "Anonymous hacktivists take down MasterCard.com again in support of WikiLeaks", *Geek* available at http://www.geek.com/articles/news/anonymous-hacktivists-take-down-mastercard-com-again-in-support-of-wikileaks-20110628/ (last accessed 29 June 2011).

BERNERS-LEE, T. "Net Neutrality: This is Serious" Blog (2006) available at www.dig.csail.mit.edu/breadcrumbs/node/144 (last accessed March 3, 2010).

BESCHIZZA, R. (3 June 2011), "LulzSec claims FBI affiliate hacked, users and botnet are exposed", Boing Boing available at http://boingboing.net/2011/06/03/lulzsec-claims-fbi-a.html

BOYDON, C. "Building a Botnet Empire in Two Days" (June 30, 2006) available at http://images.google.com.au/imgres?imgurl=http://blog.spywareguide.com/upload/2006/05/ISTAdwareThroughWMVFile/ActiveX-thumb.GIF&imgrefurl=http://blog.spywareguide.com/2006/06/&usg=__aA8hJy8hCGm0aUesHouq5e9kMzM=&h=97&w=128&sz=10&hl=en&start=13&tbnid=sxNZtB3wnM9qmM:&tbnh=69&tbnw=91&prev=/images%3Fq%3Ddollarrevenue%2Bpopup%2Bactive%2BX%26gbv%3D2%26hl%3Den

Brandeis http://www.brandeis.edu/legacyfund/bio.html (accessed March 17, 2011).

BRENNER, S. "Hackback as Self-Defense, CYB3RCRIM3: Observations on Technology, Law and Lawnessness" available at http://cyb3rcrim3.blogspot.com/2007/03/hackback-as-self-defense.html. (last accessed April 16, 2010).

CAMBER, R., COLLINS, L., & FERNANDEZ, C., "British teenager charged over cyber attack on CIA as pirate group takes revenge on 'snitches who framed him'" *dailymail.co.uk* (22 June 2011) available at http://www.dailymail.co.uk/sciencetech/article-2006118/Ryan-Cleary-charged-cyber-attack-CIA-LulzSec-takes-revenge.html (last accessed November 10, 2011).

CATE, F. "Information Security Breaches: Looking Back & Thinking Ahead" *The Centre for Information Policy Leadership* (2008) available at www.informationpolicycentre.com/ (last accessed October 22, 2009).

CHIARAMONTE, P. & WINTER, J., "Hacker Group Anonymous Threatens to Attack Stock Exchange" (4 October 2011) *Fox News* available at http://www.foxnews.com/scitech/2011/10/04/hacker-group-anonymous-threatens-to-attack-stock-exchange/ last accessed 4 October 2011.

CLARKE, R., "Categories of Malware" (September 2009) available at http://www.rogerclarke.com/II/MalCat-0909.html (last accessed February 7, 2011).

CLARKE, R., "Peer-to-Peer (P2P) – An Overview" (2004) available at http://rogerclarke.com/EC/P2POview.html (last accessed February 6, 2011).

CLAYTON, R., "Missing the Wood for the Trees" comments on ICANN fast-flux-report (Feb. 2009) available at http://forum.icann.org/lists/fast-flux-initial-report/msg00022.html (last accessed February 7, 2011).

COMLAY, E., "Hackers target mexico government websites" (15 September 2011) *Reuters* available at http://www.reuters.com/article/2011/09/15/us-mexico-hackers-idUSTRE78E7AC20110915 (last accessed 18 September 2011).

CONSTANTIN, L 1 August 2011, "AntiSec Hackers Hit 77 Law Enforcement Websites", Anonymous available at http://news.softpedia.com/news/AntiSec-Hackers-Hit-77-Law-Enforcement-Websites-214555.shtml

CONSTANTIN, L 6 June 2011, Sony Pictures Russian Website Compromised, Softpedia available at http://news.softpedia.com/news/Sony-Pictures-Russian-Website-Compromised-204563.shtml

COUTS, A 9 June 2011, "Citibank hacked, more than 200,000 bank customers at risk", Digital Trends available at http://www.digitaltrends.com/computing/citibank-hacked-more-than-200000-bank-customers-at-risk/

COUTS A 18 August 2011, "Hackers leak Citigroup CEO's personal data after Occupy Wall Street arrests", Digital Trends available at http://www.digitaltrends.com/computing/hackers-leak-citigroup-ceos-personal-data-after-occupy-wall-street-arrests/ ,

DEMETRIOU, C. AND SILKE, A., "A Criminological Internet 'sting': Experimental Evidence of Illegal and Deviant Visits to a Website Trap" (2003) 43 British Journal of Criminology 213

DERIENZO, P., "Eating its Own: Hack Attack" available at http://pdr.autono.net/message2c.html (last accessed 5 January 2012).

DUNN, J. E., "Alleged LulzSec Hacker 'Kayla' Arrested By UK Police" *csoonline.com* (2 September 2011) available at <http://www.csoonline.com/article/689060/alleged-lulzsec-hacker-kayla-arrested-by-uk-police> at 10 November 2011.

ERRETT, J, "Expecting Anonymous at #TMX" (7 November 2011) *NowToronto.com* available at http://www.nowtoronto.com/news/webjam.cfm?content=183319 (last accessed 8 November 2011).

FALLIERE, N., "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems" (August 6, 2010) *Symantec* available at http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (last accessed February 7, 2011).

FARLEY, M 1 February 2001, "Dissidents Hack Holes in China's New Wall"/ "Magazine Is Sent to 250,000 in China", Los Angeles Times available at http://www.gis.net/~cht/dissidents.html

FLETCHER, O., "China Hackers Seek to Rally Peers Against Cybertheft" (3 September 2011) *WSJ.com* available at http://online.wsj.com/article/SB10001424053111903895904576546430870651962.html (last accessed 5 September 2011.

FOGARTY, K 28 October 2011, "Hackers come out of shadows to attack police, support Occupy protests", IT world available at http://www.itworld.com/security/217561/hackers-come-out-shadows-attack-police-support-occupy-protests

GALLAGHER, S., "Anonymous takes down darknet child porn site on Tor network" (24 October 2011) *arstechnica.com* available at http://arstechnica.com/business/news/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network.ars (last accessed 31 October 2011).

GRANT, D., "NYSE Hacked! Is The Anonymous Infrastructure Crumbling?", (10 October 2011), *New York Observer* available at http://www.observer.com/2011/10/nyse-remains-unhacked-is-the-anonymous-infrastructure-crumbling-video/ (last accessed 10 October 2011).

GUTMAN, P. "The Commercial Malware Industry" available at www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf *(last accessed February 4, 2011).*

HARRINGTON, J 8 September 11, "Hacktivism: What is the Chaos Computer Club?", Suite101 available at http://joharrington.suite101.com/hacktivism-what-is-the-chaos-computer-club-a387917 , Wikipedia 2011, "Chaos Computer Club" available at http://en.wikipedia.org/wiki/Chaos_Computer_Club

Honeynet Organisation at http://www.honeynet.org/node/132 (last accessed February 6, 2011).

Honeynet Project at http://old.honeynet.org/misc/project.html (last accessed November 12, 2010).

International Foreign Government E-Mails Hacked by TeaMp0isoN", (7 November 2011) The Hacker News available at http://thehackernews.com/2011/11/international-foreign-government-e.html

JARDIN, X 14 August 2011, "Anonymous hacks BART after wireless shutdown; protests planned for Monday", BoingBoing available at http://boingboing.net/2011/08/14/anonymous-hacks-bart-after-wireless-shutdown-protests-planned-for-monday.html

JIDENMA, N 28 September 2011, "Naija Cyber Hactivists Hack EFCC website to protest proposed internet censor in Nigeria", The Next Web available at http://thenextweb.com/africa/2011/05/26/nigerian-government-agency-website-hacked-by-cyberhacktivists/

KIRK, J 25 August 2010, "Iranian Cyber Army Moves Into Botnets", PCWorld available at http://www.pcworld.com/businesscenter/article/208670/iranian_cyber_army_moves_into_botnets.html

KIRK, J 5 September 2011, "Turkish Hackers Strike Websites with DNS Hack", PCWorld available at http://www.pcworld.com/article/239501/turkish_hackers_strike_websites_with_dns_hack.html , http://www.zone-h.org/

KOVACS, E 15 November 2011, "Anonymous Turns Green and Goes After Polluters", Softpedia available at http://news.softpedia.com/news/Anonymous-Turns-Green-and-Goes-After-Polluters-234681.shtml

KOVACS, E 16 November 2011, "French Nuke Company Fined After Hacking Greenpeace", Softpedia available at http://news.softpedia.com/news/French-Nuke-Company-Fined-After-Hacking-Greenpeace-234900.shtml

KOVACS, E 17 November 2011, "Anonymous Threatens Congress Over SOPA", Softpedia available at http://news.softpedia.com/news/Anonymous-Threatens-Congress-Over-SOPA-235201.shtml

KUMAR, M., "Operation OpIndependencia: Anonymous hit Mexican government official websites", *The Hacker News* available at http://thehackernews.com/2011/09/operation-opindependencia-anonymous-hit.html last accessed 30 September 2011.

KUMAR, M., "Sony Music Brazil Gets Defaced!" (5 June 2011) *thehackernews.com* available at http://thehackernews.com/2011/06/sony-music-brazil-gets-defaced.html (last accessed 6 June 2011).

LAWSON, L., "You say crackers; I say hacker: A hacking Lexicon" (April 13, 2001 available at http://articles.techrepublic.com.com/5100-10878_11-1041788.html (last accessed July 28, 2009).

LEYDEN, J 26 July 2010, "EU climate exchange website hit by green-hat hacker", The Register available at http://www.theregister.co.uk/2010/07/26/climate_exchange_website_hack/ (last accessed 27 July 2010).

LEYDEN, J 4 November 11, "Hackers mistake French rugby site for German stock exchange", The Register available at http://www.theregister.co.uk/2011/11/04/french_rugby_site_hacktivist_maul/ ,

LEYDEN, J 6 December 2010, 20 July 2011, "Anonymous attacks PayPal in 'Operation Avenge Assange'", *The Register* available at http://www.theregister.co.uk/2010/12/06/anonymous_launches_pro_wikileaks_campaign/

LEYDEN, J, 2011 *The Register* available at http://www.theregister.co.uk/2011/10/12/bundestrojaner/ ,

LEYDEN, J., "Anonymous hackers hacked by Young Turks" (22 July 2011) *The Register* available at http://www.theregister.co.uk/2011/07/22/anonplus_hacked/ (last accessed 23 July 2011).

LIEBOWITZ, M 4 November 11, "Hackers Target Stock Index, Hit Rugby Team Instead", Security News Daily available at http://www.securitynewsdaily.com/hackers-stock-index-rugby-team-1309/

LIEBOWITZ, M., "Anonymous releases IP addresses of alleged child porn viewers", (3 November 2011) *MSN Today* available at http://today.msnbc.msn.com/id/45147364/ns/today-today_tech/t/anonymous-releases-ip-addresses-alleged-child-porn-viewers/ (last accessed 4 November 2011).

LIMER, E 15 August 2011, "Anonymous follows through on BART hack, organises protest", Geekosystems available at http://www.geekosystem.com/anon-hacks-bart/ ,

MANDELL, N., "Anonymous hacker group threatens Mexican drug cartel Zetas in online video", (31 October 2011) *New York Daily News* available at http://www.nydailynews.com/news/world/anonymous-hacker-group-threatens-mexican-drug-cartel-zetas-online-video-article-1.969859#ixzz1d4sAfvE6 (last accessed 1 November 2011).

MARTIN, P 10 February 2010, "Australian Government Website Hacked In Protest", Technorati:

MARTIN, P., "Australian Government Website Hacked in Protest" (10 February 2010) *Technorati* available at http://technorati.com/politics/article/australian-government-website-hacked-in-protest/ (last accessed 11 February 2010).

MICK, J 4 April 2011, "Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit", Daily Tech available at http://www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm

MILLMAN, R 29 November 2004, "SCO hit by hacker protest", SC Magazine available at http://www.scmagazineus.com/sco-hit-by-hacker-protest/article/31510/

MILLS, E 6 June 2011, "Hackers taunt Sony with more data leaks, hacks", CNET available at http://news.cnet.com/8301-27080_3-20069443-245/hackers-taunt-sony-with-more-data-leaks-hacks/

MORETTI, S 27 September 2011 http://www.torontosun.com/2011/10/27/video-warns-of-possible-cyber-attack-on-tsx ,

MOSES, A., "Super bad: First State set police on man who showed them how 770,000 accounts could be ripped off" (18 October 2011) *smh.com.au* available at http://www.smh.com.au/it-pro/security-it/super-bad-first-state-set-police-on-man-who-showed-them-how--770000-accounts-could-be-ripped-off-20111018-1lvx1.html (last accessed 18 October 2011).

MOSES, A., "Super sloppy: First State customers kept in the dark" (19 October 2011) *smh.com.au* available at http://www.smh.com.au/it-pro/security-it/super-sloppy-first-state-customers-kept-in-the-dark-20111019-1m7g6.html (last accessed 20 October 2011).

National Cyber-Forensics Training Alliance website available at http://www.ncfta.net/ncfta-initiatives/malware-botnet (last accessed March 2, 2011).

NAZARIO, J, "Politically Motivated Denial of Service Attacks", The Virtual Battlefield: Perspectives on Cyber Warefare, Arbor Networks available at http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf , Thomas, TL 2001, 'The Internet in China: Civilian and Military Uses', Information & Security: An International Journal, vol. 7, pp. 159-173. Available at:

NEAL, D 9 August 2011,"Team Poison hacks Blackberry after riots", The Inquirer available at http://www.theinquirer.net/inquirer/news/2100557/team-poison-hacks-blackberry-riots

NUTTALL, C 19 August 1998, "Chinese protesters attack Indonesia through Net", BBC News available at http://news.bbc.co.uk/2/hi/science/nature/154079.stm

Op free condor http://knightcenter.utexas.edu/blog/hackers-attack-news-website-ecuador

Pagerghost, blog entry commenting on "How to Build a Botnet Empire in Two Days" *Security Lab blog. SpywareGuide* available at http://blog.spywareguide.com/2006/06/building_a_botnet_empire_in_tw_1.html (last accessed May 31, 2010).

PENENBERG, A., "Hacking Bhabha" (16 November 1998) *Forbes* available at http://www.forbes.com/1998/11/16/feat.html (last accessed 11 November 2011).

PFEFFER, A, YARON, O., "Israel government, security services websites down in suspected cyber-attack", (6 November 2011) *Haaretz.com* available at http://www.haaretz.com/news/diplomacy-defense/israel-government-security-services-websites-down-in-suspected-cyber-attack-1.394042 (last accessed 7 November 2011).

POSPISILLI, J., "Cyber Criminals Turn to P2P for DoS Attacks" (July 20, 2007) available at http://tech.blorge.com/Structure:%20/2007/07/20/cyber-criminals-turn-to-p2p-for-dos-attacks? (last accessed July 1, 2010).

QMI AGENCY, "Hacktivist group shuts down child porn sites" (24 October 2011) *Canoe Technology* available at http://technology.canoe.ca/2011/10/24/18871656.html (last accessed 25 October 2011).

RAGAN S, 22 February 2011, "Iranian Cyber Army defaces Voice of America and 93 other domains (Update)", The Tech Herald available at http://www.thetechherald.com/article.php/201108/6849/Iranian-Cyber-Army-defaces-Voice-of-America-and-93-other-domains

RAGAN, S 1 August 2008, "CCC is at it again – hands out copies of German Interior Minister's fingerprint", The Tech Herald:

RAGAN, S 30 May 2011, "PBS: LulzSec attack an attempt to chill journalism", The Tech Herald available at http://www.thetechherald.com/article.php/201122/7215/PBS-LulzSec-attack-an-attempt-to-chill-journalism

ROGERS, M., "Psychological Theories of Crime and Hacking" (Dec. 15, 2006) Telmatic Journal of Clinical Criminology

ROMANO, M., ROSIGNOLI, S., and GIANNINI, E. "Robot Wars – How Botnets Work" (2005) available at http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html (last accessed June 17, 2010).

SANCHEZ, F 27 September 2011, "Hackers hijack Twitter accounts of Chavez critics", MSNBC: http://www.msnbc.msn.com/id/44689342/ns/technology_and_science-security/t/hackers-hijack-twitter-accounts-chavez-critics/

SAWYER, J. "Tech Insight: The Enterprise Hacks Back!" *Dark Reading* available at http://darkreading.com/security/attacks/showArticle.jhtml?articleID=223100750.

SCHNEIER, B. "Stuxnet" (October 7, 2010) available at http://www.schneier.com/blog/archives/2010/10/stuxnet.html (last accessed November 12, 2010).

SCHNEIER, B., Benevolent Worms, Crypto-Gram Newsletter, 2003, available at http://www.schneier.com/cryptogram-0309.html (last accessed November 12, 2010).

SCHROEDER, S 16 June 2011, "LulzSec Hackers Take Down CIA Website", Mashable available at http://mashable.com/2011/06/16/lulzsec-hackers-cia/

Security Beyond Borders, "Salami technique" available at http://securitybeyondborders.org/global-security-glossary/global-security-glossary-s/ (last accessed Marc 18, 2011).

SELTZER, S 22 August 2011, "For-Profit Company Oversaw Davis's Execution, Had Prompted Complaint for Illegal Purchase of Lethal Injection Drugs", Alternet available at http://www.alternet.org/newsandviews/article/670237/for-profit_company_oversaw_davis%27s_execution,_had_prompted_complaint_for_illegal_purchase_of_lethal_injection_drugs/ ,

SYPNOWICH, C. (2001) Law and Ideology, Stanford Encyclopedia of Philosophy, available at http://www.plato.stanford.edu./entries/law-ideology

TAKVER, "European Climate Exchange website hacked", (25 July 2010) *Independent Media Centre Australia* available at http://indymedia.org.au/2010/07/24/european-climate-exchange-website-hacked (last accessed 29 July 2010).

TAYLOR, R., CAETI, T., LOPER, K., FRITSCH, E., AND LIEDERBACH, *Digital Crime and Digital Terrorism* (UK: Pearson, 2005).
The Gospel According to Tux republished from newsgroup posting to various websites such as The New Hacker's Dictionary available at http://www.fullbooks.com/The-New-Hacker-s-Dictionary-version-4-219.html.

The Wrong Guy 10 November 2011, "Activists hack French ruling party's phone numbers", WhyWeProtest available at http://forums.whyweprotest.net/threads/activists-hack-french-ruling-partys-phone-numbers.96206/

THOMAS, T. .L., "The Internet in China: Civilian and Military Uses" (2001) available at http://fmso.leavenworth.army.mil/documents/china-internet.htm (last accessed 5 January, 2012).

TICEHURST, J 20 September 2000, "HSBC internet sites hacked", V3 available at http://www.v3.co.uk/v3-uk/news/2007500/hsbc-internet-sites-hacked

TippingPoint, "Kraken Botnet Infiltration" (April 2008) available at http://www.dvlabs.tippingpoint.com/blog/2008/04/28/kraken-botnet-infiltration (last accessed Nov. 12, 2010).

Tor Project: Anonymity Online available at https://www.torproject.org (last accessed March 17 2011).

Trend MICRO, "Zeus: A Persistent Criminal Enterprise" (March , 2010) available at http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/zeusapersistentcriminalenterprise.pdf (last accessed December, 2010).

TYSON, J., "How Virtual Private Networks Work" available at https://www.computer.howstuffworks.com/vpn.com (last accessed June 30).

VON LEITNER, F http://tbtf.com/resource/felix.html , Wikipedia 2011, "Chaos Computer Club" available at http://en.wikipedia.org/wiki/Chaos_Computer_Club

WHOIS Task Force, available at http://www.gnso.icann.org/issues/whois-privacy/whois-tfl-preliminary.html#GTLDRegistriesconstituency (last accessed April 30, 2010).

WHYTE, S., "Meet the hacktivist who tried to take down the government" (March 14, 2011) *smh.com.au* available at <http://www.smh.com.au/technology/security/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html> (last accessed 7 November 2011).

Wikileaks available at http://wikileaks.org/wiki/Skype_and_the_Bavarian_trojan_in_the_middle

Wikipedia, CCC website available at http://ccc.de/en/updates/2011/staatstrojaner ,

WILLIAMS, Jeff, 'Dismantling Waledac' on *Microsoft Malware Protection Centre – Threat Research & Response Blog* (25 February 2010)
<http://blogs.technet.com/b/mmpc/archive/2010/02/25/dismantling-waledac.aspx>.

WISNIEWSKI, C 10 August 11, "Hong Kong stock exchange (HKEx) website hacked, impacts trades", Naked Security available at http://nakedsecurity.sophos.com/2011/08/10/hong-kong-stock-exchange-hkex-website-hacked-impacts-trades/ ,

WISNIEWSKI, C 12 August 11, "Hong Kong stock exchange attacked for second day in a row", Naked Security available at http://nakedsecurity.sophos.com/2011/08/12/hong-kong-stock-exchange-attacked-for-second-day-in-a-row/

WISNIEWSKI, C 22 May 2011, "Sony BMG Greece the latest hacked Sony site", Naked Security available at http://nakedsecurity.sophos.com/2011/05/22/sony-bmg-greece-the-latest-hacked-sony-site/

WISNIEWSKI, C 30 May 2011, "PBS.org hacked... LulzSec targets Sesame Street?", Naked Security:

WISNIEWSKI, C., "PBS.org hacked... LulzSec targets Sesame Street?" *Sophos* available at http://nakedsecurity.sophos.com/2011/05/30/pbs-org-hacked-lulzsec-targets-sesame-street/ (last accessed 31 May 2011).

WYSS, J 1 November 2011, "Political hackers are one of Latin America's newest headaches", Bellingham Herald available at http://www.bellinghamherald.com/2011/11/01/2252902/political-hackers-are-one-of-latin.html

Xinhua 14 October 2011, "Brazilian presidency's blog hacked in protest of corruption", ChainDaily available at http://www.chinadaily.com.cn/xinhua/2011-10-14/content_4060557.html

ZAKALWE, C 7 July 2011, "Turkish Government Websites Hacked in Protest at Internet Censorship", BlogSpot available at http://stopturkey.blogspot.com/2011/07/turkish-government-websites-hacked-in.html

Zeroday Emergency Response Team (ZERT), available at http://www.isotf.org/zert/.

ZORZ, Z., "Anonymous shuts down child porn sites, leaks usernames" (24 October 2011) *Help Net Security* available at http://www.net-security.org/secworld.php?id=11831&utm_source=twitterfeed&utm_medium=twitter&utm_campaign=s3cb0t (last accessed 31 October 2011).

Chatham House Rules Conference Presentations

Chatham House Organisation available at http://www.chathamhouse.org.uk/about/chathamhouserule/ (last accessed February 7, 2011).

Chatham House Rules. Internet Filtering and Censorship Proposal Forum" (Nov. 2008) Cyberspace law and Policy Centre, the University of New South Wales, Sydney, Australia.

Closed panel on Cybercrime at AusCERT 2008 with Chatham House Rules. Law enforcement agents from the AFP, NSW, Germany and the FBI were present.

Direct question posed to Australian Federal Police at the 2010 High Tech Crime Conference, Sydney. Chatham House Rules.

ISOI 5, Estonia, 2008, Chathom House Rules.

Technical/industry/academic reports

AYCOCK, J. and MAURUSHAT, A., 'Good' Worms and Human Rights. Technical Report 2006-846-39. Department of Computer Science, University of Calgary, 2006.

BALATAZAR, J., COSTOYA, J. And FLORES, R., "Infiltrating WALEDAC Botnet's Covert Operations", (2009) TREND MICRO.

OWENS, W., DAM, K. and LIN, H. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and use of Cyberattack Capabilities(* 2009) Committee on Offensive Information Warfare, National Research Council, Computer Science and Telecommunications Board (CSTB).

PERRIOT, F. And KNOWLES, D., "W32.Welchia.Worm" (July 28, 2004) *Symantec Security Response.*

Quarterly Report PandaLabs (January-March 2010) available at http://www.pandasecurity.om/img/enc/Quarterly_Report_Pandalabs_Q1_2010.pdf (last accessed June 24, 2010).

Symantec, Report on the Underground Economy (2008) available at http://www.symantec.com/content/en/us/about/media/pdfs/underground_Econ_Report.pdf (last accessed June 28, 2010).

TrustDefender, "In-Depth Analysis of Mebroot/Torpig Trojan Available" available at http://www.trustdefender.com/trustdefender-labs-blog-in-depth-analysis-of-mebroot-torpig-trojan-available.html (last accessed January 31, 2011).

WHEELER, D. and LARSEN, G. "Techniques for Cyber Attack Attribution" *Institute for Defense Analysis* (2003) http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf.

United States National Cyber-Forensics and Training Alliance, report on Stuxnet available at http://www.ncfta.net/ncfta-news/ncfta-cyber-alerts/stuxnet (last accessed February 7, 2011).

Briefing papers/working papers/white papers/theses/research projects

BRUNEA, G., "DNS Sinkhole" *SANS Institute InforSec Reading Room* (Aug. 7, 2010), page 2 available at http://www.sans.org/reading_room/whitepapers/dns/dns-sinkhole_33523 (last accessed Feb. 20, 2011).

CLAYTON, R., "Missing the Wood for the Trees" comments on *ICANN fast-flux-report* (Feb. 2009) available at http://forum.icann.org/lists/fast-flux-initial-report/msg00022.html (last accessed February 7, 2011).

CONNELLY, C., MAURUSHAT, A., VAILE, D., and VAN DIJK, P., *Cyber-Security Education Research Project* (2010)..

"Know Your Enemy" series of whitepapers available at http://old.honeynet.org/papers/index.html (last accessed November 12, 2010).

KROGOTH, "Botnet Construction, Control and Concealment: Looking into the Current Technology and Analysing Tendencies and Future Trends" (2008), available at http://www.shadowserver.org/wiki/uploads/Information/thesis_botnet_krogoth_2008_final.pdf (last accessed July 5, 2010)..

LUMBY, C, GREEN, L., and HARTLEY, J., "Untangling the Net: The Scope of Content Captured by Mandatory Internet Filtering" (December 2009) Report Written for Google Australia, available at http://www.saferinternetgroup.org/pdfs/lumby.pdf (last accessed January 3, 2011).

MAURUSHAT, A. "Freedom House Report on Internet Freedom: Australia" (2011).

Media Releases

CONROY, Stephen (Senator), *Budget provides policing for Internet safety*, media release, 13 May 2008, at <http://www.minister.dbcde.gov.au/media/media_releases/2008/033>

FBI Press Release: 'Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems' (Sep 22, 2011) available at http://www.fbi.gov/losangeles/press-

releases/2011/member-of-hacking-group-lulzsec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems (last accessed 20 October 2011).

FBI Press Release: Office of Public Affairs, 'Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks' (19 July 2011) available at http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks (last accessed 10 November 2011).

FBI Press Release: Public Affairs Specialist Laura Eimiller, 'Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems' (22 September 2011) available at http://www.fbi.gov/losangeles/press-releases/2011/member-of-hacking-group-lulzsec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems (last accessed 11 November, 2011).

FBI Press Release: 'Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks' (July 19, 2011) available at http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks (last accessed 20 October, 2011).

FBI Press Release: U.S. Attorney's Office, 'Two Men Charged in New Jersey with Hacking AT&T's Servers' (18 January 2011) available at http://www.fbi.gov/newark/press-releases/2011/nk011811.htm (last accessed 11 November, 2011).

U.S. Department of Justice Press Release: California Man Pleads Guilty in "Botnet" Attack That Impacted Seattle Hospital and Defense Department (May 4, 2000) available at http://www.usdoj.gov./criminal/cybercrime/maxwellPlea.htm (last accessed December, 2010).

Magazine and newspaper articles

BARLOW, J.P., "Is there a there in Cyberspace?" *Utne Reader* 1995 available at http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/3966/3537 (last accessed November 10, 2010), also at http://www.utne.com/archives/IsThereaThereinCyberspace.aspx (last accessed March 18, 2011).

BBC News, "Questions Cloud Cyber Crime Cases" October 11, 2003 available at http://www.bbc.co.uk/2/hi/technology/3202116.stm (last accessed April 27, 2010).

BBC News, "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers" (September 26, 2010) available at http://www.bbc.co.uk/news/world-middle-east-11414483 (last accessed November 12, 2010).

BERINATO, S. "Attack of the Bots" *Wired Magazine* Issue 14.11 (November 2006).

BROAD, W., MARKOFF, J. and SANDER, D., "Israeli Test Worm Called Crucial in Iran Nuclear Delay" (Janaury 15 2011) *The New York Times* available at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (last accessed February 7, 2011).

MADRIGAL, A., "Ahmadinejad Publicly Acknowledges Stuxnet Disrupted Iranian Centrifuges" (November 29, 2010) available at http://www.theatlantic.com/technology/archive/2010/11/ahmadinejad-publicly-acknowledges-stuxnet-disrupted-iranian-centrifuges/67155/# (last accessed February 7, 2011).

MOSES, A. "Super bad: First State set police on man who showed them how 770 000 accounts could be ripped off" (October 18, 2011) available at http://www.smh.com.au/it-pro/security-it/super-bad-first-state-set-police-on-man-who-showed-them-how--770000-accounts-could-be-ripped-off-20111018-1lvx1.html.

PILGER, J. "The War on Wikileaks: A John Pilger Investigation and Interview with Julian Assange" (January 13, 2011).http://johnpilger.com/articles/the-war-on-wikileaks-a-john-pilger-investigation-and-interview-with-julian-assange

RASH, M. "Mother, May I" available at http://www.securityfocus.com/print/columnists/463 (last accessed January 29, 2008).

RAYWOOD, D., "Is the Mariposa Botnet Still Functioning?" (June 24, 2010) available at http://www.securecomputing.net.au/News/217678,is_the_mariposa_botnet_still_functioning.aspx (last accessed June 26, 2010).

RISING, G., "Cody Kretsinger Arizona College Student Charged in Sony Hacking Case" The Huffington Post (January 12, 2010) at http://www.huffingtonpost.com/2011/09/23/cody-kretsinger-arizona-c_n_977490.html

SOPHO, "Sopho Assists Computer Crime Unit in Bringing Botnet Master to Justice" June 12, 1008 available at assistshttp://www.sophos.com/pressoffice/news/articles/2008/06/bentley-imprisoned.html.

The Age, "The Cyberspace Wars" (June 22, 2003) available at http://www.theage.com.au/articles/2003/06/21/1056119529509.html (last accessed December 2010).

WHYTE, S. "Meet the Hacktivist Who Tried to Take Down the Government" (March 14, 2011) Sydney Morning Herald.

ZORZ, Z., "French Hacker and Alleged Anonymous Member Arrested After Bragging on TV" (April 13, 2011) at http://www.net-security.org/secworld.php?id=10895

Online videos and podcasts

"Anonymous to Australia" available at http://www.youtube.com/watch?v=eEc80U46hIQ (last accessed January 13, 2011).

INSIGHT, "Hacktivism" (September 27, 2011) available at http://www.sbs.com.au/insight/episode/index/id/431.

KEMMER, R. "How to Steal a Botnet and What Can Happen When You Do" *Google Tech Talk* (Sept. 2010) available at http://www.youtube.com/watch?v=2GdqoQJa6r4 (last accessed June 26, 2010).

LANGILL, J., "Stuxnet Worm Detailed Examination by SANS" available on a hacker website http://www.garage4hackers.com/showthread.php?604-Stuxnet-Worm-Detailed-Examination-by-SANS (last accessed February 7, 2011).

GREY, P., Risky.biz Podcast, "RB2: AusCERT Podcast: Interview with Moscow-Based Cybercrime Analyst Kimberly Zenz" (May 20, 2009).

GREY, P. Risky.biz Podncast, "Interview on Risky Business with Michael Dwyer, Chief Executive of First State Superannuation" (October 14, 2011) http://risky.biz/minter

The Agenda, "Attack of the Hacktivists" TVO October 25, 2011

Wikipedia

Wikipedia, "Anonymous P2P" available at http://en.wikipedia.org/wiki/Anonymous_P2P (last accessed November 12, 2010).

Wikipedia, "Bennett Arron" available at http://en.wikipedia.org/wiki/Bennett_Arron (last accessed May 31, 2010).

Wikipedia, "Click Fraud", available at http://en.wikipedia.org/wiki/Click_fraud (last accessed June 30, 2010).

Wikipedia, "Denial of Service Attack (distributed)", available at http://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack (last accessed June 30, 2010).

Wikipedia, "Denial-of-service (unintentional)", available at http://www.en.wikipedia.org/wiki/Denial-of-service_attack#Unintentional_denial_of _service (last accessed June 30, 2010).

Wikipedia, "Peer-to-peer" available at http://en.wikipedia.org/wiki/Peer-to-peer (last accessed December 2011).

Wikipedia, "SPAM", available at http://en.wikipedia.org/wiki/E-mail_spam (last accessed June 30, 2010).

Wikipedia, "Virtual Private Network" available at http://www.en.wikipedia.org/wiki/Virtual_private_network (last accessed June 30, 2010).

Covo, Pierre

From: Covo, Pierre
Sent: November-05-12 11:03 AM
To: Pilon, Claude
Subject: RE: [redacted] **s.23**

[redacted]

Thanks,

From: Clow, Patrick
Sent: November-01-12 8:20 AM

Hello Pierre,

[redacted]

Thank you

From: Clow, Patrick
Sent: Friday, October 12, 2012 11:51 AM
To: Covo, Pierre
Subject: RE: [redacted] s.23

[redacted]

From: Covo, Pierre
Sent: Friday, October 12, 2012 11:49 AM
To: Clow, Patrick
Subject: FW: [redacted] s.23

Hi Patrick,

[redacted]

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

From: Covo, Pierre
Sent: October-12-12 11:19 AM
To: Clow, Patrick
Subject: [redacted] s.23

Hi Patrick,

[redacted]

Thanks,

Pierre

Pierre Covo
Counsel | Avocat

Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

From: Covo, Pierre
Sent: October-12-12 11:55 AM
To: Pilon, Claude
Subject: FW: [redacted] s.23

[redacted]

From: Clow, Patrick
Sent: October-12-12 11:51 AM
To: Covo, Pierre
Subject: RE: [redacted] s.23

[redacted]

From: Covo, Pierre
Sent: Friday, October 12, 2012 11:49 AM
To: Clow, Patrick
Subject: FW: [redacted] s.23

Hi Patrick,

[redacted]

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

From: Covo, Pierre
Sent: October-12-12 11:19 AM
To: Clow, Patrick
Subject: [redacted] s.23

Hi Patrick,

[redacted]

Thanks,

Pierre

Pierre Covo
Counsel | Avocat

Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

Department of Justice Canada
Public Safety and Emergency Preparedness Canada
269 Laurier Avenue West, 16th Floor
Ottawa, Ontario
K1A 0P8

Ministère de la Justice Canada
Sécurité publique et Protection civile Canada
269, avenue Laurier Ouest, 16e étage
Ottawa (Ontario)
K1A 0P8

Security classification -- Côte de sécurité
Protected B
Solicitor-Client privilege | Secret professionnel de l'avocat

File number -- Numéro de dossier
10036-13

Date
13 November 2012

Telephone / FAX – Téléphone / Télécopieur
(613) 990-8418

MEMORANDUM / NOTE DE SERVICE

DRAFT

TO / DEST: Patrick Clow, Manager, Technical Analysis
Canadian Cyber Incident Response Centre

FROM / ORIG: Pierre Covo, Counsel
Public Safety Legal Services

SUBJECT / OBJET: [redacted] **s.23**

Comments/Remarques

[redacted]

Pages 281 to / à 288

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

c.c.	C. Pilon	PS LSU
	H. Kousha	
	M. Shogilev	CLPS

Department of Justice Canada
Public Safety and Emergency Preparedness Canada
269 Laurier Avenue West, 16th Floor
Ottawa, Ontario
K1A 0P8

Ministère de la Justice Canada
Sécurité publique et Protection civile Canada
269, avenue Laurier Ouest, 16e étage
Ottawa (Ontario)
K1A 0P8

Security classification -- Côte de sécurité
Protected B
Solicitor-Client privilege | Secret professionnel de l'avocat

File number -- Numéro de dossier
10036-13

Date
13 November 2012

Telephone / FAX – Téléphone / Télécopieur
(613) 990-8418

MEMORANDUM / NOTE DE SERVICE

DRAFT

TO / DEST: Patrick Clow, Manager, Technical Analysis
Canadian Cyber Incident Response Centre

FROM / ORIG: Pierre Covo, Counsel
Claude Pilon, Counsel
Public Safety Legal Services

SUBJECT / OBJET: [redacted] s.23

Comments/Remarques

[redacted]

Pages 291 to / à 297

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Department of Justice Canada
Public Safety and Emergency Preparedness Canada
269 Laurier Avenue West, 16th Floor
Ottawa, Ontario
K1A 0P8

Ministère de la Justice Canada
Sécurité publique et Protection civile Canada
269, avenue Laurier Ouest, 16e étage
Ottawa (Ontario)
K1A 0P8

Security classification -- Côte de sécurité
Protected B
Solicitor-Client privilege | Secret professionnel de l'avocat

File number -- Numéro de dossier
10036-13

Date
13 November 2012

Telephone / FAX – Téléphone / Télécopieur
(613) 990-8418

MEMORANDUM / NOTE DE SERVICE

DRAFT

TO / DEST: Patrick Clow, Manager, Technical Analysis
Canadian Cyber Incident Response Centre

FROM / ORIG: Pierre Covo, Counsel
Claude Pilon, Counsel
Public Safety Legal Services

SUBJECT / OBJET: [redacted] **s.23**

Comments/Remarques

[redacted]

Pages 299 to / à 311

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

c.c. C. Pilon PS LSU
H. Kousha
M. Shogilev CLPS

Department of Justice Canada
Public Safety and Emergency Preparedness Canada
269 Laurier Avenue West, 16th Floor
Ottawa, Ontario
K1A 0P8

Ministère de la Justice Canada
Sécurité publique et Protection civile Canada
269, avenue Laurier Ouest, 16e étage
Ottawa (Ontario)
K1A 0P8

Security classification -- Côte de sécurité
Protected B
Solicitor-Client privilege | Secret professionnel de l'avocat

File number -- Numéro de dossier
10036-13

Date
13 November 2012

Telephone / FAX – Téléphone / Télécopieur
(613) 990-8418

MEMORANDUM / NOTE DE SERVICE

DRAFT

TO / DEST: Patrick Clow, Manager, Technical Analysis
Canadian Cyber Incident Response Centre

FROM / ORIG: Pierre Covo, Counsel
Claude Pilon, Counsel
Public Safety Legal Services

SUBJECT / OBJET: [redacted] **s.23**

Comments/Remarques

[redacted]

Pages 314 to / à 324

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

[redacted]

s.23

c.c. C. Pilon PS LSU
H. Kousha
M. Shogilev CLPS

Department of Justice Canada
Public Safety and Emergency Preparedness Canada
269 Laurier Avenue West, 16th Floor
Ottawa, Ontario
K1A 0P8

Ministère de la Justice Canada
Sécurité publique et Protection civile Canada
269, avenue Laurier Ouest, 16e étage
Ottawa (Ontario)
K1A 0P8

Security classification -- Côte de sécurité
Protected B
Solicitor-Client privilege | Secret professionnel de l'avocat

File number -- Numéro de dossier
10036-13

Date
13 November 2012

Telephone / FAX – Téléphone / Télécopieur
(613) 990-8418

MEMORANDUM / NOTE DE SERVICE

DRAFT

TO / DEST: Patrick Clow, Manager, Technical Analysis
Canadian Cyber Incident Response Centre

FROM / ORIG: Pierre Covo, Counsel
Claude Pilon, Counsel
Public Safety Legal Services

SUBJECT / OBJET: [redacted] **s.23**

Comments/Remarques

[redacted]

Pages 327 to / à 338

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

[redacted]

s.23

c.c. C. Pilon PS LSU
H. Kousha
M. Shogilev CLPS

Covo, Pierre

From: Covo, Pierre
Sent: December-03-12 12:05 PM
To: Covo, Pierre
Subject: [redacted]
Attachments:

s.23

[redacted]

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

From: Covo, Pierre
Sent: November-05-12 11:29 AM
To: Clow, Patrick
Cc: Pilon, Claude
Subject: RE: [redacted]

s.23

Hi Patrick,

[redacted]

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418

Email/Courriel: pierre.covo@justice.gc.ca

From: Clow, Patrick
Sent: November-01-12 8:20 AM
To: Covo, Pierre
Subject: RE: [redacted] s.23

Hello Pierre,

[redacted]

Thank you

From: Clow, Patrick
Sent: Friday, October 12, 2012 11:51 AM
To: Covo, Pierre
Subject: RE: [redacted] s.23

[redacted]

From: Covo, Pierre
Sent: Friday, October 12, 2012 11:49 AM
To: Clow, Patrick
Subject: FW: [redacted] s.23

Hi Patrick,

[redacted]

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

From: Covo, Pierre
Sent: October-12-12 11:19 AM
To: Clow, Patrick
Subject: [redacted] s.23

Hi Patrick,

Thanks for the call yesterday. Unfortunately I was unable to get back to you.

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

Pages 344 to / à 357

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Pages 358 to / à 371

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Pages 372 to / à 384

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

From: Covo, Pierre
Sent: December-14-12 10:58 AM
To: Slatkoff, Ari
Cc: Pilon, Claude; Sugunasiri, Shalin
Subject:
Attachments:

s.23

Ari,

[redacted]

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

Covo, Pierre

From: Covo, Pierre
Sent: December-27-12 9:56 AM
To: Clow, Patrick
Cc: Slatkoff, Ari; Pilon, Claude
Subject: [redacted]
Attachments:

s.23

Hello Patrick,

[redacted]

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

Pages 387 to / à 390

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Covo, Pierre

From: Covo, Pierre
Sent: December-14-12 9:29 AM
To: Slatkoff, Ari
Subject: RE: [redacted] **s.23**

Perfect. Coming over.

From: Slatkoff, Ari
Sent: December-14-12 9:28 AM
To: Covo, Pierre
Subject: RE: [redacted] **s.23**

Hi Pierre. I am available this morning if you want to drop by.

From: Covo, Pierre
Sent: December-12-12 9:57 AM
To: Slatkoff, Ari
Subject: FW: [redacted] **s.23**

Hi Ari,

[redacted]

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

From: Covo, Pierre
Sent: December-05-12 1:54 PM
To: Slatkoff, Ari
Subject: [redacted] **s.23**

Hi Ari,

Would you have about 15 minutes this afternoon?

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418

Department of Justice Canada
Public Safety and Emergency Preparedness Canada
269 Laurier Avenue West, 16th Floor
Ottawa, Ontario
K1A 0P8

Ministère de la Justice Canada
Sécurité publique et Protection civile Canada
269, avenue Laurier Ouest, 16e étage
Ottawa (Ontario)
K1A 0P8

Security classification -- Côte de sécurité **Protected B** **Solicitor-Client privilege | Secret professionnel de l'avocat**
File number -- Numéro de dossier 10036-13
Date 11 December 2012
Telephone / FAX – Téléphone / Télécopieur (613) 990-8418

MEMORANDUM / NOTE DE SERVICE

DRAFT

TO / DEST: Patrick Clow, Manager, Technical Analysis
Canadian Cyber Incident Response Centre

VIA: Ari Slatkoff, Team Leader
Public Safety Legal Services

FROM / ORIG: Pierre Covo, Counsel
Public Safety Legal Services

SUBJECT / OBJET: [redacted] **s.23**

Comments/Remarques

[redacted]

Pages 393 to / à 394

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

[redacted]

s.23

c.c. C. Pilon PS LSU
S. Shugunasiri PS LSU