Botnet Badinage: Regulatory Approaches to Combating Botnets

Alana M. Maurushat

A thesis submitted in accordance with the requirements for the award of the degree of Doctor of Philosophy, Faculty of Law,

University of New South Wales

2011

ABSTRACT

A botnet is a collection of remotely controlled and compromised computers that are controlled by a bot master. Botnets are the main crime tool used by cybercriminals. To use an analogy, many crimes may be committed with a gun ranging from murder to rape to armed robbery to assault to breaking and entering to theft. Likewise, a botnet may be used in many forms of cybercrime and civil wrong ranging from sending spam, to denial of service attacks, to child pornography distribution, to worm propagation, to click-fraud, to keylogging technology and traffic sniffing which captures passwords and credit card information, and to mass identity theft. Botnets are a major crime tool used on the internet in a similar fashion to how a gun is used on the street.

This thesis explores the regulation of botnets and the role that botnets play as a tool to commit many forms of cybercrime. In exploring regulation of botnets, countermeasures against fighting this crime tool will be analysed, and policy options evaluated as to under what circumstances society should prioritise combating botnets at the expense of encroaching on civil liberties, in particular the values of privacy and freedom of expression. This thesis argues that Internet service providers, domain name service providers and self-organised security communities are best positioned to effectively combat botnets.

In determining the most effective regulatory measures to combat botnets, this thesis has investigated, and at points discounted, a range of other measures such as data breach notification, Sarbanes-Oxley, banking law, user education and training, non-criminal legal remedies, the range of technologies that botnets utilise, economic models to disrupt profitability, national and international criminal law, and technologies non-essential to botnets.

This thesis is the result of inter-disciplinary research on botnets, combining insights from the disciplines of computer security, information systems, risk management, economics, regulation and law. Based on this inter-disciplinary research, the thesis demonstrates how cybercrime laws both at the national and international levels are rendered impotent through modern obfuscation crime tools. Reforms to the law are necessary to offer security research exemptions, remote search and seizure by law enforcement and the introduction of unwanted software legislation. At the same time, more safeguards to preserve civil liberties must also be built into Australian regulatory practice.

In the course of examining the most effective ways to regulate botnets, the thesis also provides a case study demonstrating weaknesses in Lessig's Internet regulatory theory.

Internet regulatory theories have generally placed emphasis on civil liberties and the struggles between users and governments over control of the regulation of the Internet. These theories, however, ignored the complex issues that cybercrime would bring into the discussion. The regulation of botnets is used to evaluate the utility of Lawrence Lessig's theory of Internet regulation through four modalities (market, norms, law and code). It is argued that the levels and types of cybercrime which have occurred in the last decade and in the decades to come were not anticipated by these theories and poses new theoretical issues. This thesis will demonstrate

that effective botnet regulation will involve some use of illegal means, and inevitably will challenge not only the mindset that the law plays an authoritative role in regulation, but also Lessig's theory that market, code, and norms are the only significant forms of regulation. Changes or developments of Lessig's model are required. For example, many of the actions by self-organised security groups to combat botnets may be conceived as effective and moral though, as will be demonstrated, clearly illegal. The work of self-help remedies by these groups does not fit well with Lessig's theory. Self-organised security communities do not fall within any of Lessig's modalities and yet, the efforts of such groups are the most important countermeasures in combating botnets, and possibly in combating many forms of cybercrime.

ACKNOWLEDGEMENTS

I would like to thank my husband, Michael, as well as my parents, Don and Denise, for the sacrifices made and support given to allow me to finish the PhD.

As with any PhD there were many obstacles and challenges along the way. I cannot thank enough my supervisors, Graham Greenleaf and Roger Clarke, for their excellent guidance, patience and diligence throughout this process. I am truly grateful to you both.

I am indebted to the Faculty of Law and the Graduate Research School at the University of New South Wales for their financial support in the form of scholarships, a submission extension, travel grants, and for all of the advice both professional and personal from members of the Faculty of Law.

There are two colleagues at UNSW whom I would like to expressly recognise for their generosity and support: David Vaile and Lyria Bennet-Moses. I would equally like to express my gratitude to my former colleagues from both the University of Hong Kong, Andy Halkyard and Roda Mushkat, and at the University of Ottawa, Daniel Gervais, Ian Kerr , Michael Geist and Greg Hagen.

I would also like to recognize the interns whom I have worked with at the Cyberspace Law and Policy Centre for their wit, intellect, diligence, insight and hard work. In particular, I wish to thank Renee Watt, Pauline Rappaport, Adam Arnold, Lauren Loz, Jo Brick, Sarah Lux, Michael Whitbread, Eugenie Kyung-Eun Hwang, Nathalie Pala, David Chau, Pata Gogal and Samuel Sathiakumar.

There are several friends whom I wish to thank for their willingness to help out in any way needed including final edits: Jill Matthews, Alex Colangelo, and Keiran Hardy.

Lastly, I am wrapping my children, Saskia and Alexandre, up in a bundle of warm hugs and kisses. They inspire me more than words could possibly express and make me a better person. My thesis is dedicated to them.

TABLE OF CONTENTS

FIGURES AND TABLES

ABBREVIATIONS

ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
AIC	Australian Institute of Criminology
AISI	Australian Internet Security Initiative
APEC	Asia-Pacific Economic Cooperation
ARPA	Advanced Research Projects Agency
ATC	Australian Trade Commission
AUSD	Australian Dollars
AUSTRAC	Australian Transaction Reports and Analysis Centre
BSA	Broadcasting Services Act
ccTLD	Country Code Top Level Domain
CHR	Chatham House Rules
CC	Criminal Code
CCA	Competition and Consumer Act
CCTV	Closed Circuit Television
CRTC	Canadian Radio and Telecommunications Commission
DBN	Data Breach Notification
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOS	Denial of Service Attack
DDOS	Distributed Denial of Service Attack
DDP	Días de Pesadilla
DPI	Deep Packet Inspection
DR	DollarRevenue

EFT	Electronic Funds Transfer (Code)
FCC	Federal Communications Commission
FQDN	Fully Qualified Domain Name
FTA	Fair Trading Act
gTLD	General Top Level Domain
HTML	Hypertext Markup Language
HTTP	Hyptertext Transfer Protocol
HTTP2P	Hypertext Transfer Peer to Peer Protocol
IIA	(Australian) Internet Industry Association
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRC	Internet Relay Chat
ISO	International Standards Organisation
ISP	Internet Service Provider
ITU	International Telecommunications Union
MCC	Model Criminal Code
NCFTA	National Cyber-Forensics Training Alliance
NPP	National Privacy Principles
NSW	New South Wales
OECD	Organisation for Economic Cooperation and Development
OPC	Office of the Privacy Commissioner
PBL	Policy Blocklist
SGA	Sale of Goods Act
SMTP	Simple Mail Transfer Protocol

SNDS	Smart Network Data Services
SOSC	Self-organised Security Community
SSL	Secure Socket Layer
TA	Telecommunications Act
TIAA	Telecommunications Interception Amendments Act
TPA	Trades Practices Act
TTL	Time to Live
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network

PUBLICATIONS ARISING FROM THIS THESIS

Australia's Accession to the *Cybercrime Convention*: Is the Convention Still Relevant in Combating Cybercrime in the Era of Obfuscation Crime Tools?
16:1 University of New South Wales Law Journal (2010)

Zombie Botnets
(2010) Scripted

Data Breach Notification Law Across the World from California to Australia
Privacy Law and Business International, *April, 2009*

"The benevolent health worm: comparing Western human rights-based ethics and Confucian duty-based moral philosophy,"
Ethics and Information Technology Journal, Feb. 2008 (DOI 10.1007/s10676-008-9150-1)

When internet protocols and legal provisions collide: Unauthorised Access and *Sierra v. Ritz*
Computer, Law and Security Report, February 2009
Alana Maurushat and Ron Yu (US Patent Agent and Director of Gilkron Ltd., Hong Kong)

"'Good' Worms and Human Rights"
ACM Computers & Society, Vol. 38, Issue 1, March 2008.
John Aycock (Faculty of Computer Science, University of Calgary) and Alana Maurushat

"Passing the Buck: Who Will Bear the Financial Transaction Losses from Consumer Device Insecurity?"
Journal of Law, Information Technology and Science, Vol. 1, Issue 1, 2008
Roger Clarke (Faculty of Commerce, Australian National University) and Alana Maurushat

"**Exploring the Limits of Computer Code as a Protected Form of Expression: *A Suggested Approach to Encryption, Computer Viruses and Technological Protection Measures***"
Mcgill Law Journal, Issue 1 Volume 51 (2006)
Alex Colangelo (Stikeman Elliot Law Firm, Toronto) and Alana Maurushat

"Australia's Internet Filtering Proposal in the International Context"
Internet Law Bulletin, Vol 12 No 2 (2009)
Alana Maurushat and Renee Watts (Mallesons)

Virus Bulletin 2007
Future Threats
Vienna, Austria
John Aycock (University of Calgary, Faculty Computer Science) and Alana Maurushat

Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime – The Report of the Inquiry into Cyber Crime
Invited Submissions to the House of Representatives Standing Committee on Communications, Parliament of Australia (2010)
http://aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf

Chapter 1

INTRODUCTION: BOTNETS IN CONTEXT

Table of Contents

1.1 BOTNETS AND THE INTERNET

The need to balance the interest of privacy and freedom of expression with the need to curtail criminal activity on the Internet has become a truism in scholarly works.[1] This is rooted in the false assumption that balance is indeed possible for these competing, and sometimes opposite, objectives. Balancing these competing interests is not possible. At issue is a range of values including security, privacy, due process, freedom of expression, and the right to earn a living. Choices must be made between which values are to be afforded higher protection in society. Monitoring Internet communications without a warrant, for example, prioritises criminal and terrorist deterrence above privacy and freedom of expression. In many ways, this research will continue an old theme of exploring competing values in the age of new technologies. In exploring botnets, regulatory countermeasures against fighting this crime tool will be presented, analysed, and then policy options will be determined as to under what circumstances society should lend more credence to combating cybercrime at the expense of encroaching on civil liberties, in particular the values of privacy and freedom of expression. Botnets pose substantial regulatory challenges of the technical, legal and ethical nature. Effective approaches to combating botnets lie at the heart of this research and in this process, botnets expose the deficiencies of current Internet regulatory theories. Early Internet regulatory theories placed emphasis on civil liberties and the power struggle between users and governments to have a strong-hold in the regulation of the Internet. These theories, however, all ignored the complex issues that cybercrime would bring into the discussion. As botnets shed light on existing Internet regulatory theories, they will be used as a case study to evaluate the applicability of early Internet regulatory theories to the levels and types of cybercrime witnessed on the Internet both in the last decade and in the decades to come.

[1] *See for example the following selection of articles*: O'Neill, M., "Old Crimes in New bottles: Sanctioning Cybercrime" (2001-2001) 9 George mason Law Review 237; Rustad, M., "Private Enforcement of Cybercrime on the Electronic Frontier" (2005) 11 Southern California International Law Journal 63; Wong, D. and Hoffstadt, B, "Countering the Cyber-Crime Threat" (2006) 43 American Criminal Law Review 201; Harley, B., "A Global Convention on Cybercrime?" (2010) The Columbia Science and Technology Law Review; and Hopkins, S., "Cybercrime Convention: A Positive Beginning to a Long Road Ahead" (2003) Journal of High Technology Law.

Over 1000 articles were retrieved that referenced the need to balance civil liberties with the goals of cybercrime.

1.1.1 Historical Context of Internet Security

The origins of the Internet were in the late 1960s, in the form of a U.S. military-funded project by the Advanced Research Projects Agency (ARPA). The project, known as the ARPANET, was initiated to create a robust communications network. The successor to ARPANET, following the specification of the IP and TCP protocols and their implementation in 1983, became known as the Internet. It originally linked American universities funded by the U.S. Department of Defense through DARPA, for research and educational purposes.[2] The network was designed to reroute communication traffic automatically around existing problems, and to ensure the integrity of information flows. It did so by use of a packet-switching network. A message was broken down into information packets. The packets could traverse any of a multitude of paths to reach their destination. Some packets would travel one route; others would pursue a different route where the packets would be reassembled at their final destination. Failure or attack at one node did not impede the traffic flow of information packets. The network simply rerouted around the compromised component.[3] The goals of the original design were openness, flexibility, reliability and redundancy. The Internet, however, was not designed to be secure.

The history of the Internet may be seen as evolving in three phases.[4] The first phase centred on mainframe computers – the types of computers that evoke images of large, cumbersome computers the size of lecture rooms. At this point, computers were uncommon in the every day lives of people and organisations. Commencing in the early 1990s, the second phase shifted to personal computers. The third phase commencing in the 2000s has seen the connection of many types of devices such as mobile phones, stand-alone computers, and internal business networks to the Internet. A fourth phase has yet to emerge but may be the era of total convergence where devices and applications converge and where even various small components of a toaster and clothing have multiple internet protocol addresses all connected to the Internet.

---

[2] For a comprehensive overview of the history of ARPANET *see* Hauben, M. Behind the Net – The untold history of the ARPANET available at hppt://www.dei.isep.ipp.pt/~acc/docs/arpa.html (last accessed January 14, 2008).
[3] This is only partially true. There were documented defects that would prevent the communication channels from working in the event of an attack. For example, three members of the IEEE wrote of the weakness in the routing algorithm. *See* McQuillan, J., Falk, G. and Richer, R., "A Review of the Development and Performance of the ARPANET Routing Algorithm," (December 1978) IEEE Transactions on Communications, Vol. COM-26. *See also* Crocker, S. and Bernstein, M. "ARPANET Disruptions: Insight into Future Catastrophes." TIS (Trusted Information Systems) Report, 247, 24 Aug 1989.
[4] *See generally* Schneier, B., *Secrets and Lies* (Robert Ipsen 2000).

As a research network at its inception, the Internet had limited functions. As applications and protocols developed the Internet was used for a wide range of activities. Protocols such as smtp (simple mail transfer protocol) extended the ARPANET and then the Internet from a tool for computer-to-computer communications to human-usable infrastructure. As the infrastructure became more widely accessible during the mid-1990s, further protocols such as http (hypertext transfer protocol) encouraged much more personal and corporate use. The commercial applications of the Internet have expanded exponentially in the last thirty years. Many commercial transactions are now web-based while many commercial entities, such as the finance industry in particular, have moved into the web sphere; not only do consumers use the internet for personal and commercial banking needs, similar network communication channels such as SWIFT (the Society for Worldwide Interbank Financial Telecommunication) are also used to exchange information between financial institutions.[5] The evolution of internet applications has spread from research and commerce to uses in medicine, electronic governance, information and archival repositories, content development and distribution – to name but a few. Society has become dependent on networks. The internet along with other networks have woven a pattern of intricate connectivity into the backbone of a nation's critical infrastructure, corporate structure and activities, and continue to reach deeply into our every day personal communications. With an increasing dependence on the internet comes a spiralling desire among certain parties to exploit the technology for anti-social, criminal and downright malevolent means. As a result, the field of internet security has emerged (a taxonomy will be explored later).

Threats to computer security have gone from mere cyber jokes[6] - to highly skilled and rebellious teenage hackers[7] - to those brilliant computer enthusiasts working between 1960 to 1990 who revolutionized the computer industry to develop hardware and software following the principles of hacker ethics[8] - to organized crime units operating for financial gain,[9] to espionage and

---

[5] Clarke, R. and Maurushat, A., "Who Will Bear the Cost of Insecure Devices" (2007) 18 Journal of Law, Information and Science 8.

[6] During the development of ARPANET, researchers often played jokes on one another such as annoying messages and the use of minor security breaches. The jokes are documented in Levy, S. *Hackers: Heroes of the Computer Revolution* (New York: Doubleday, 1984).

[7] A prime example of youth hooligan hacking is a Canadian teenage hacker known as "Mafiaboy." In 2000 he conducted a denial of service attack rendering a number of sites inoperable. The websites included Yahoo, eBay, Amazon.com, CNN and a few others. *See* 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.

[8] Such individuals along the line of ethical hacking – that is, the philosophy of hacking as an art-form dedicated to free information flows – include John Draper, Richard Stallman, Vinton Cerf, Bill Gates, Steve Jobs, and Marvin Minsky.

[9] For a detailed report on organized criminal activities *see* "McAfee Virtual Criminology Report: Organized Crime and the Internet" December 2006.

counter-espionage information warfare to gain information, as well as political and technical advantages,[10] to terrorists looking to attack a nation or institution's critical infrastructure[11]. Computer security affects every single person or entity that connects to the network. For this reason internet security has become a local, national and global issue.[12]

1.1.2 The Significance of Botnets

A somewhat simplistic security chain is provided below that explains the context of botnets within the larger security framework. The most important of the chain elements are security, internet security, computer security, and malware. As the chain progresses, each descending level becomes a subset of the above ascending levels. Botnets do not appear within this chain as they do not form a subset of malware but are more aptly classified as a crime tool. This will be explained in greater detail on the following page.

Security

↓

Computer Security

↓

Internet Security

↓

Malware

---

[10] For a report on espionage activities *see* "McAfee Virtual Criminology Report: Cybercrime: The Next Wave" 2007.

[11] For example, the CIA spoke at a SANS Institute Seminar outlining in vague details the cyberattack of power grids. This has been a controversial announcement with newspapers around the world reporting on the press release with little to no substantiation of the claims. Many technology blogs, on the other hand, have been quick to highlight the "conspiracy theory" nature and deliberately vague nature of the CIA release in a sensitive political time leading up to a United Stated federal election. *See for example* blog commentary at http://www.techdirt.com/articles/20080118/181113.shtml. The exact press release by the CIA reads as follows:

> "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."

Available at http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5

[12] While there is a wealth of reference information of security issues from national and international perspectives, there is a dearth of work done at the local level. One exception is the eMayor project running out of the European Union. *See* Electronic & Secure Municipal Administration for European Citizens at http://www.deloitte.com/dtt/cda/doc/content/dtt_eMayorFinalReport06_021706.pdf

Security, according to the Oxford Dictionary, is "the state of being or feeling secure" and "the safety of a state or organization". Security has two facets, the physical state of safety and a psychological state of being or feeling secure.

Definitions of **computer security** vary greatly. There is no settled definition of the term. Functional approaches to computer security utilise roughly five areas: risk avoidance, deterrence, prevention, detection and recovery.[13] Other definitions emphasize the various security environments such as physical, operational, personnel/employees, system, and network security.[14] The structure adopted in this research places emphasis on four core areas that are often referred to in computer security texts: confidentiality, integrity, authentication and availability.[15] This structure reflects the widely varying sources on computer security.

> **Confidentiality** refers to a state where information is not accessed by unauthorised parties.
>
> **Integrity** refers to the assurance that only authorised parties may make modifications to information.
>
> **Authentication** refers to the process of proving the identity of a computer or computer user.
>
> **Availability** refers the ability of authorised parties to access information.

For this research **computer security** is defined as a means ensuring the confidentiality, integrity, authentication and availability of information from threats to information which may include interception, interruption, modification, copying, fabrication, and deletion.

A simplistic definition of malware is malicious software. **Malware**, for the purpose of this research, is defined as potentially harmful software or a component of software that has been installed without authorisation to a third party device.[16] Viruses[17] and worms[18] are types of malware.

---

[13] Garfinkel, S. and Spafford, G. *Practical UNIX & Internet Security*, 2nd Ed (California: O'Reilly, 1996), page 6.
[14] Ross, S., *UNIX System Security Tools* (McGraw-Hill, 1999).
[15] *See for example*, Anderson, R. *Security Engineering* 2nd Ed. (Indianapolis: Wiley Publishing, 2008), page 4. *See also* Pfleeger, C. and Pfleeger, S. *Security in Computing* 4th Ed. (Prentice Hall, 2006), page 11.
[16] Malware has been defined in many ways. Clarke, for instance, defines malware as:
Malware is:

- software, or a software component or feature, that
- comes by some means to be invoked by a device, and that

A **botnet** is a collection of remotely controlled and compromised computers that are controlled by a bot master / botherder. Botnets utilise a series of technologies, software programs, and methods. As part of a botnet's operations, malware may be installed onto the compromised computers. A botnet receives its instructions in the form of a computer software program known as a 'bot'. Many bots may be categorised as malware.

Botnets can be used in many types of security incidents. Using the security incident categorization of the U.S.-Cert (United States Computer Emergency Readiness Team), botnets may be used in both threats and attacks in each of the categories. The U.S.-Cert classification has been used due to its international leading role in the area as well as the extent of its influence in the security field.

Figure 1(A) represents a chart categorizing Internet security incidents. It uses the categorization model of the U.S.-Cert (United States Computer Emergency Readiness Team). The chart on the following page demonstrates the potential use of botnets in each of the categories. The categories are as follows and are ranked in order of degree of severity from left to right.

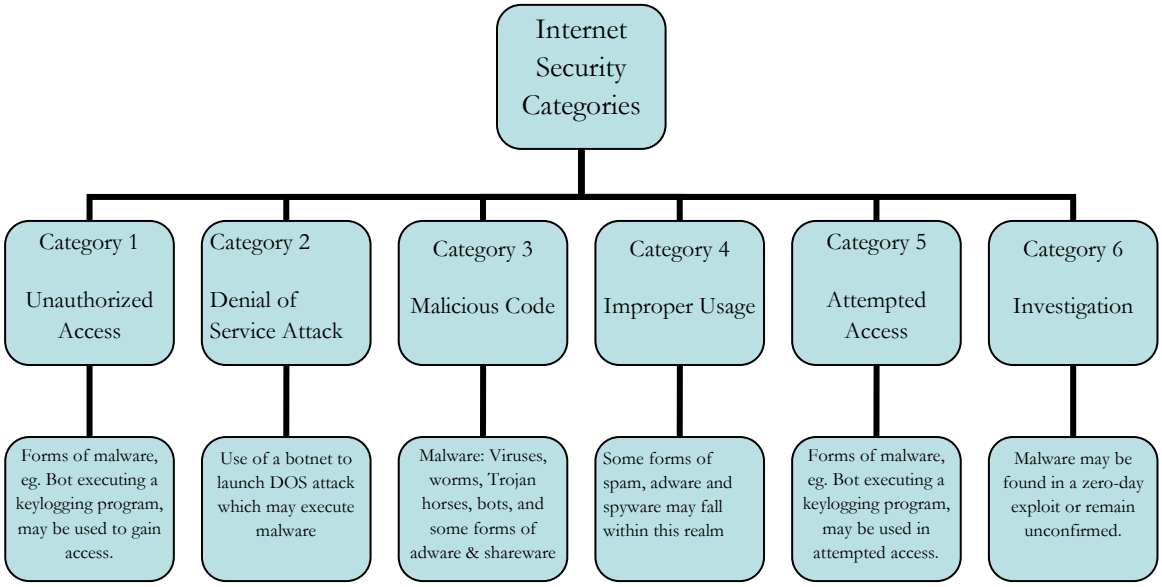
- on invocation, has an effect that is:
    - unintended by the person responsible for the device, and
    - potentially harmful to an interest of that or some other person

Clarke, R., "Categories of Malawre" (September 2009) available at http://www.rogerclarke.com/II/MalCat-0909.html (last accessed February 7, 2011).

[17] A virus is a "block of code that inserts copies of itself into other programs". Viruses generally require a positive act by the user to activate the virus. Such a positive act would include opening an email or attachment containing the virus. Viruses often delay or hinder the performance of functions on a computer, and may infect other software programs. They do not, however, propagate copies of themselves over networks. Again, a positive act is required for both infection and propagation. *See generally* Pfleeger, note 15 above, pages 116-141.

[18] A worm is a program that propagates copies of itself over networks. It does not infect other programs nor does it require a positive act by the user to activate the worm. *See generally* Pfleeger, note 15 above, pages 116-141.

Figure 1(A) U.S. Cert Internet Security Categories



As seen from the above chart, the extent to which both malware and botnets can permeate internet security is comprehensive.[19] This research emphasizes botnets within the overall

[19] US-Cert (United States Computer Emergency Readiness Team), Quarterly Trends and Analysis Report (2007) volume 2, Issue 4.

Category 1 Unauthorized Access
"In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource."
This type of activity is perceived at the highest level and could potentially include information warfare, espionage, critical infrastructure and even cyberterrorism.
Category 2 Denial of Service Attack
"An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS."
Such attacks are performed against networks and websites of all natures from government to corporations to organizations and personal sites. They are perceived as serious due to the amount of damage which can occur. DoS attacks may be used in category 1 incidents (unauthorised access of federal systems).
Category 3 Malicious Code
"Successful installation of malicious software (e.g. virus, worm, spyware, bot, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application). Agencies are not required to report malicious logic that has been successfully quarantined by antivirus (AV) software."
This category is most analogous with what is commonly referred to as malware. The clear exception is that from the U.S.-Cert perspective, the focus on the more dangerous or harmful types of malware which they have deemed to include those which are neither detected nor quarantined by antivirus software.
Category 4 Improper Usage
"A person violates acceptable computing use policies."

structure of internet security. Placing emphasis on botnets serves two purposes. Firstly, it allows the research to be narrowed to a manageable size. Secondly, and more importantly, it is a matter of looking at the problem of internet security closer to a single significant contributing source, as opposed to a mere symptom or reaction. To use an analogy, many crimes may be committed with a gun ranging from murder to rape to armed robbery to assault to breaking and entering to theft. Likewise, a botnet may be used in many forms of cybercrime and civil wrongs ranging from sending spam, to denial of service attacks, to child pornography distribution, to worm propagation, to click-fraud, to keylogging technology and traffic sniffing which captures passwords and credit card information, and to mass identity theft. Botnets are not the only crime tool used in cybercrime. Botnets, as will be fully demonstrated in **Chapter 3**, are structured to exploit a full range of other crime tools. Other crime tools include fast-flux, double fast-flux, dynamic domain name hosting, virtual private network services and encryption. These terms are explained in detail in **Chapter 3**. To return to the gun analogy, a criminal may evade detection through the use of various types of bullets, by removing serial numbers from guns, and by using gloves to ensure no fingerprints are left on the weapon, or by using a cloth to wipe the prints, and through other various mechanisms to clean the gun. Just as there are many types of guns, there are also many differently structured botnets. Botnets are a major crime tool used on the internet in a similar fashion to how a gun is used on the street.[20]

Anecdotal evidence is useful to explain the many roles that botnets play in crime. A compelling description of botnet use, compromised computers and related crimes was published on the internet from someone purporting to be within the inner sanctum of the commercial child pornography industry. The article, "My Life in Child Pornography" was posted to the wikileaks site and is considered by many security experts and cybercrime researchers to be accurate and

---

This is the catch-all category which is, arguably, likely to require the most amount of discretion as to the extent of detection and response.

Category 5 Scans, Probes, or Attempted Access

"Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service."

Category 6 Investigation

"*Unconfirmed* incidents of potentially malicious or anomalous activity deemed by the reporting entity to warrant further review."

[20] The types and levels of harm are naturally different between crimes committed with guns and botnets. Physical harm typically does not result from botnet related crimes. This is not to say, however, that physical harm cannot result from the use of botnets. Denial of service attacks to networks such as hospitals and transportation systems could easily result in physical injuries and death. A denial of service attack has been launched against the Port of Houston. Another denial of service attack in Seattle reportedly shut down many critical hospital services. There were no reported deaths or serious injuries from these events. *See* Susan W Brenner, Carrier, B. and Henninger, J. "The Trojan Horse Defense in Cybercrime Cases" (2004) 21 Santa Clara Computer and High Technology Law Journal, pages 1-7.

authoritative.[21] The anonymously written document was translated from German to English. A relevant excerpt is copied below:

> "But how, specifically, child pornography is sold? ... Today, the answer is SPAM.... In order to send spam Trojan-infected (zombie) computers are used. But zombie computers have yet another use: it will be used in a targeted fashion to steal identities. They even use the computer of the user whose identity is stolen to conduct credible transactions such as purchase of domains, etc. But that is not everything: the installed Trojans are sometimes used as a SOCKS proxy to upload CP. The Russians have even worked out a schema to use infected computer as a network combing these infected computers (each computer would be part of a huge, redundant cluster) as a kind of huge, distributed and remote servers can be (a kind of Freenet Project, however, by using infected computers as the nodes). I want to make one thing clear: if you have an email address, there is a possibility that there is child pornography on your computer because you have received CP advertising. And if your computer is not 100% safe against Trojans, viruses and rootkits, there is the possibility that your computer is part of the vast child pornography network."

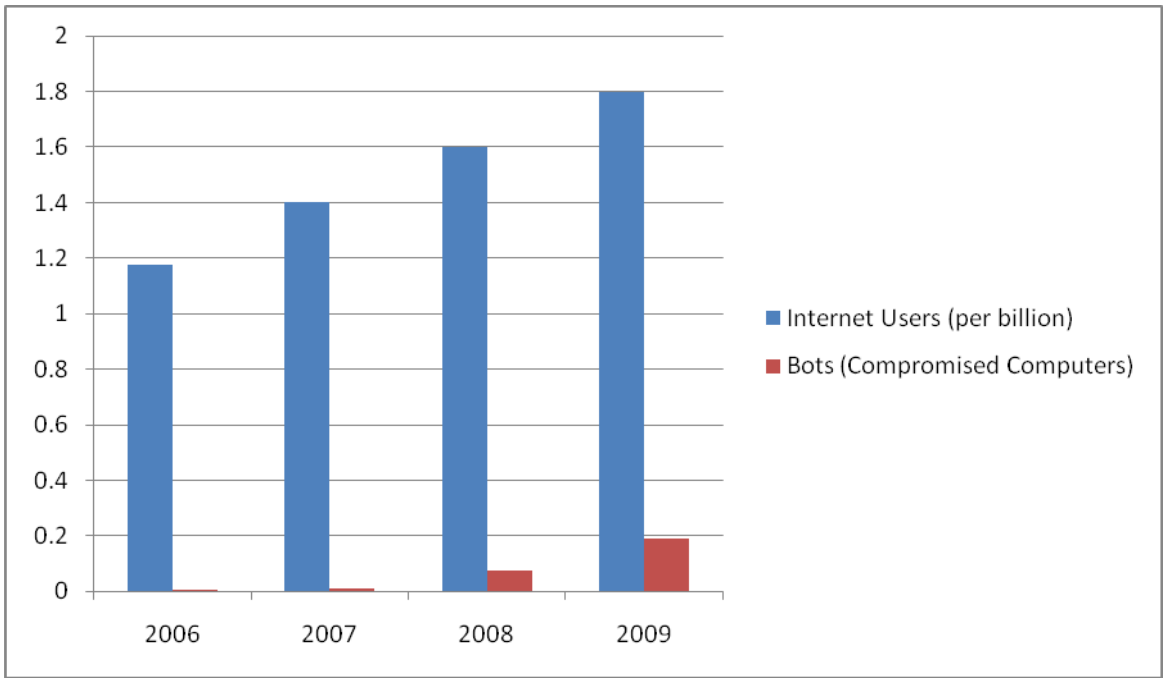
Once a computer becomes part of a botnet, it can be used in every illegal function of the child pornography distribution chain. This includes SPAM botnets which may contain links to child pornography. The links found within SPAM messages will then trigger the downloading of malware. The malware infects a computer and takes it over without your ever knowing that it has done so. Banking details are stolen. Other items related to identity are stolen (Eg. email addresses are highjacked, usernames and passwords). The stolen identity (email and credit card details) are then used to register and purchase domain names, to launder money, to store child pornography, and to distribute child pornography. All of this done typically in a manner so that the user has no idea that their computer is part of a botnet, not to mention that child pornography and other nefarious materials are being stored and later distributed using the third party computer.[22]

Statistical evidence suggests that botnets are compromising computers at a prolific rate. The number of compromised computers connected to botnets generally follows trends in the increase to the number of computers connected to the Internet. However, between 2006 and 2009 the rate of Internet users increased proportionately while the rate of compromised computers increased rather dramatically. **Figure 1(B)** on the following page represents the

[21] For example, *see* renowned security expert Schneier B., "The Techniques for Distributing Child Porn" available at Schneier on Security
http://www.schneier.com/blog/archives/2009/03/the_techniques.html (last accessed February 7, 2011).
[22] Child pornography was found on the sub-directory of a Queensland dentist in Australia. It was revealed to the public when the Australia's Internet filter blacklist (a list of websites hosting child pornography that are blocked by the filter) was leaked to wikileaks. It is suspected that the material was placed there by a botnet. Maurushat, note 87 below.

number of internet connections per given year[23] and the estimated number of compromised computers that year.[24]

Figure 1(B) Bot Propagation Trends (2006 to 2009)



[23] Determined from ITU World Telecommunication/ICT Indicators Database. Global Number of Internet Users, Total and Per 100 Inhabitants, 2000-2009 available at http://www.itu.int/IT-D/ict/statistics/material/groups/Internet_users_00-09.jpg (last accessed July 12, 2010)

[24] Estimated figures for compromised machines taken from statistics provided from Damballa, Shadowserver, and Symantec. The statistics provided were estimated by taking averages.

Damballa is the leading botnet security network corporation founded by world renowned botnet researcher David Dagon. The Damballa team consists of university professors specialising in botnets, a former Chief Security Strategist from IBM, and others from the U.S. Intelligence community, Trend Micro, F-Secure and Secure Computing. More information may be found at http://www.damballa.com/overview/index.php (last accessed July 10, 2010).

Shadowserver is a non-profit organisation comprised of security professionals who volunteer their time to gather intelligence on botnet activity, malware and electronic fraud. Shadowserver is one of the most reputed self-organised communities in the botnet area as evidenced by both the volume and diversity of entities (independent researchers, security companies, law enforcement and Internet governance agencies) that reference statistics and general information to the organisation.

Symantec is a large multi-national security software corporation. Symantec compiles comprehensive internet security statistics, particularly in the area of malware and botnets.

There is a wide range of estimates of the overall infections correlating with the number of compromised computers connecting to botnets. Problems with estimating bot populations is explored in Dagon, D. and Davis, C., "Botnet Population and Intelligence Gathering Techniques" (2008) Blackhat Conference available at http://www.blackhat.com/presentations/bh-dc-08/Dagon-Davis/Presentation/bh-dc-08-dagon-davis.pdf (last accessed June 28, 2010).

As seen above, in 2006 there were only 400,000 compromised computers connected to botnets. By 2009 that number has grown to approximately 19.3 million. Figures are provided below addressing botnets in a different context:[25]

1:3 – home PC being infected with malware with password stealing capabilities in a year

1:4 – home PC being infected with a botnet agent in a given year

1:8 – corporate PC being infected with malware with password stealing capabilities in a given year

1:12 – corporate PC being infected with a botnet agent in a given year

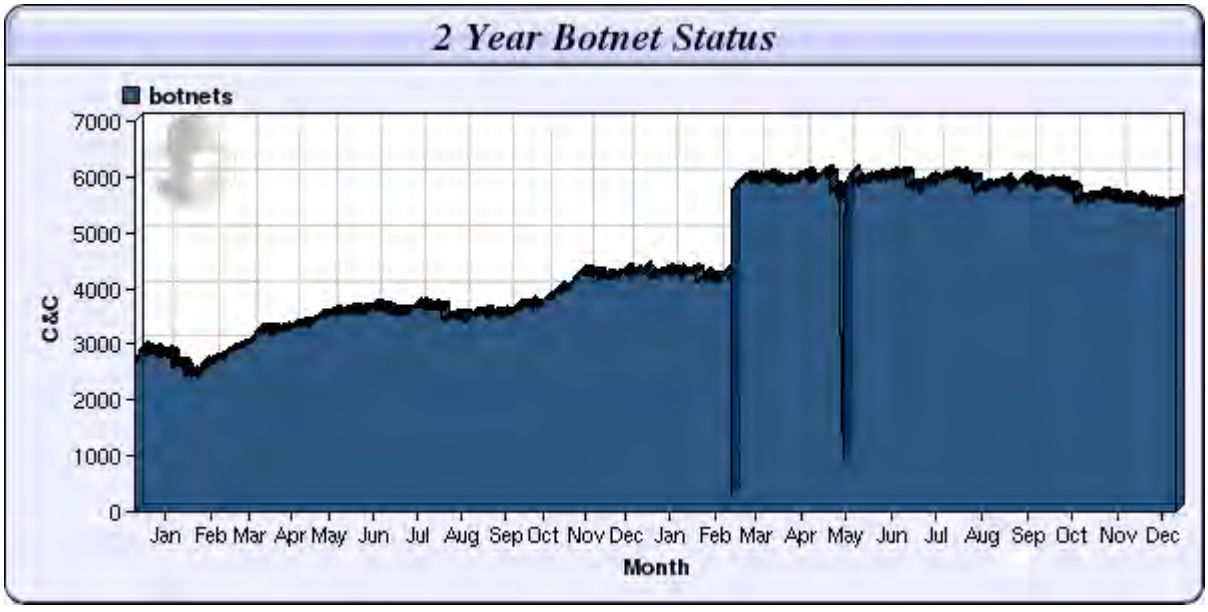
1:1160 – your car being stolen in a given year

1:700 – your home being burgled

1:600,000 – being struck by lightning

The amount of known and active command and control servers is provided by Shadowserver below in **Figure 1(C)** (from January 2009 until Dec. 2010). Where a botnet had more than one command and control source, it was counted as one botnet.

Figure 1(C) ShadowServer 2 Year Botnet Status[26]



[25] Damballa, note 24 above.
[26] Provided with permission from Shadowserver. Shadowserver botnet charts and maps may be found at http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts (last accessed December 2010).

In April 2010, for example, there were approximately 6000 active command and control servers. Shadowserver updates the botnet charts every 15 minutes. While 6000 active command and control servers may not appear to be many, consider that each botnet would have anywhere from 100 to 10 million compromised computers connected to it and that the damage caused from one botnet alone can be significant.

While the increase in bots is alarming, the number of bots worldwide, the number of botnets and the size of botnets are only partial indicators of the problem. The sophistication of botnet capabilities, the damage and harm caused, with the ease of which to acquire or rent a botnet, the resistance to countermeasures, and the rapidity of adaptation to countermeasures, are more important indicators of the problem.

There are no publicly available statistics that indicate the economic loss caused by a specific botnet.[27] Such an exercise would be fraught with statistics-gathering challenges as damages would necessarily require tracking money stolen from bank accounts, credit cards, as well as damage suffered by denial of service attacks, and the calculation of damage due to SPAM impairing Internet traffic. The ability to do statistical work in the area would require cooperation from financial institutions and private corporations located in numerous countries around the world. As such, damages resulting from botnets must be estimated through economic models and estimates.[28] Estimates put spam as accounting for approximately 77.1% of all e-mail traffic and 1.75% of all spam sent containing a form of malware in 2010.[29] Estimates of losses from internet crime (e.g. fraud and forgery) range from 3 to 5 billion AUSD per year.[30]

---

[27] This is not surprising given that cybercrime is fraught with poor statistics. The Australia *Government Response to the House of Representatives Standing Committee on Communications Report on the Inquiry into Cyber Crime, Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime* (2010) identifies the urgent need for better cyber crime statistics. This is reflected in Recommendations 1,2 and 6.

[28] *See* Judge, P., "Aplpervitch, D., and Yang, W., "Understanding and Reversing the Profit Model of Spam" (2005) Fourth Workshop on the Economics of Information Security available at http://infosecon.net/workshop/pdf/49.pdf (last accessed December 2010); and Kim, D-H., Lee, T., In, P., and Jeung, H.C., "Botnet Damage Propagation Estimation Model" (2009) KSII The First International Conference of Internet (ICONI) available at http://www.embedded.korea.ac.kr/ecel/paper/international/2009/12200910.pdf (last accessed December 2010).

[29] Kapersky Labs, Spam Statistics available at http://www.securelist.com/analysis (last accessed December 20, 2010).

[30] Estimates explored in a briefing paper for NSW Parliament by Lozusic, R. "Fraud and Identity Theft" Briefing Paper No 8/03. The higher estimate comes from Mayhw, P. "Counting the Costs of Crime in Australia" (April 2003) trends & issues in crime and criminal justice No 247.

The forms of harm arising from botnets are not limited to financial loss. At the more extreme end of the spectrum, botnets are used in the commercial child pornography industry, and to fund organized crime and terrorist groups. Other forms of harm include identity theft and misappropriation, emotional distress, and loss of trust and general sense of safety. Harm caused by botnets has resulted in the temporary closure of emergency wards in hospitals[31], misdirected signals in shipping ports[32], release of sewage into the water system,[33] and cyberwarfare.[34]

Bot agent design and bot delivery have become a commoditized service industry.[35] 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.[36] A person does not require any special computer skills to use a botnet to commit a crime. **Figure 1(D)** 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. The DOS attack could be launched for many different reasons. DOS attacks are launched and the website may be held ransom until the owner pays a fee. DOS attacks are launched as a form of retribution and as a means to inflict commercial loss to an organisation. These types of DOS attacks are increasingly being used as forms of political protest. DOS attacks may also be launched as a decoy in order

---

[31] A cyber attack was launched at a U.S. hospital causing their computer systems to crash. Doctors could not access vital patient information. Doors to operating surgeries would not open. Pagers didn't work and the intensive care unit had to be shut down. *See* U.S. Department of Justice Press Release: California Man Pleads Guilty in "Botnet" Attach That Impacted Seattle Hospital and Defense Department (May 4, 2000) available at http://www.usdoj.gov./criminal/cybercrime/maxwellPlea.htm (last accessed December, 2010).

[32] In the case of *R v. Caffrey* the accused launched a distributed denial of service attack against the Port of Houston. The logistics of the port was severely affected (Eg. ship traffic control in the port). The case was 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 (last accessed April 27, 2010).

[33] The incident was reported in the media. *See* 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).

[34] Cyber attacks were launched in 2007 and 2008 against Estonia and Georgia. In the example of Estonia, the DDoS attacks crippled the governments online infrastructure, affected banking systems, and had an enormous impact on the Estonian economy for years to come. In Georgia, the cyber attacks crippled the nation's infrastructure the night before Russian troops invaded. The attacks were done in such a way so that media could not report on what was occurring until after several days as all telecommunication infrastructure was affected including the Internet (to give you an idea of the technical feat involved here, the Internet was not affected after the 9/11 incidents). *See* 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.

[35] Quoting Gunter Ollmann in Achohido, B., "Are there 6.8 million – or 24 million – bottled PCs on the Internet?" (April10, 2010) The Last Watchdog on Internet Security available at http://lastwatchdog.com/6-8-million-24-botted-pcs-internet/ (last accessed July 12, 2010).

[36] Ollmann, G., "Your Computer is Worth 30¢: This Battle for Control of Your Computer Isn't Personal, it's Business" (April 8, 2010) available at http://www.damballa.com/knowledge/presentations.php.

to distract information technology staff while a different type of intrusion into an organisation's network takes places such as data or trade secret theft. Decoy attacks also occur in instances of critical infrastructure attacks to assist an entity (perhaps government-endorsed) while it attacks online facilities of the financial industry, electrical or sewage systems, and other forms of communications systems.

Figure 1(D) Denial of Service Attack as Commercial Service[37]

Commercialisation is also occurring within another context known as crime kits. In this instance the criminal 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.[38] 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, or they may simply hire a botnet master to perform the activity in question.

---

[37] Image from Ollmann, G., note 35 above.

[38] *See* 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).

Governments and organisations are beginning to recognise the importance of tackling botnets. The problem of botnets is described by the European Network and Information Security Agency as:

> "Botnets represent a steadily increasing problem threatening governments, industries, companies and individual users with devastating consequences that must be avoided. Urgent preventive measures must be given the highest priority if this criminal activity is to be defeated. Otherwise the effect on the basic worldwide network infrastructures could be disastrous." [39]

Governments are focusing much attention on cyber security and cyber crime with botnets driving many initiatives. The United States, the United Kingdom and Australian governments all announced major cyber security strategies in 2009 with botnets featured predominantly.[40] The Australian June 2010 Parliamentary Report on Cybercrime acknowledges the gravity of the problem of botnets.[41] Recommendation 10 states:

> **Recommendation 10**
>
> That Australia's cyber crime policy strategically targets the underground economy in malicious IT tools and personal financial information; the disruption of botnets and the identification and prosecution of botherders.[42]

Recommendations have been made by the Parliamentary Report on Cybercrime and by key organisations such as the ITU[43], OECD[44], APEC[45], as well as by Internet Service Providers.[46]

---

[39] Barroso, D, *Botnets – The Silent Threat* (2007) European Network and Information Security Agency, page at 6 (available at http://www.enisa.europa.eu/act/res/other-areas/botnets/botnets-2013-the-silent-threat (last accessed December 2010) .

[40] United States Government, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009) available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (last accessed January 29, 2010); United Kingdom Office of Cyber Security, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (2009) available at http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf (last accessed January 29, 2010); and Australian Government, *Cyber Security Strategy* (2009) available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf (last accessed January 29, 2010).

[41] Government Response to the House of Representatives Parliamentary Committee Report on Cybercrime, note 27 above. *See also* House of Representatives Standing Committee on Communications, The Report of the Inquiry into Cyber Crime, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime* (June 2010) available at http://aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf (last accessed July 13, 2010). Invited submissions were received from the Alana Maurushat of the Cyberspace Law and Policy Centre, Microsoft, the Internet Industry Association, the Attorney Generals Department and the Australian Federal Police all of which highlighted the importance of tackling botnets.

[42] Note 41 above.

[43] *See* International Telecommunications Unions, "ITU Botnet Mitigation Toolkit" (January 2008) available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf (last accessed February 7, 2011).

[44] 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

The recommendations echo similar themes. Better cooperation is needed between government, industry and key security organisations. Unified cyber crime law is required with some calling for the signing and ratifying of the *Cybercrime Convention*.[47] There is a need for better coordination and cooperation internationally between countries in cybercrime investigation. Heightened user awareness of the problem coupled with education and training for users is vital to an overall cyber security strategy. Within these overlapping recommendations three main conclusions emerge:

1) combating botnets is of the foremost importance;
2) Internet Service Providers and Domain Name Service Providers are an essential component in any effort to mitigate the effects of botnets; and
3) end users are thought to be one of the weaker links in the security chain

This research will critically analyse different strategies to counter botnets. Emphasis will be placed on the role of regulation. Both direct and indirect forms (sometimes referred to as soft law) of regulation will be considered. The law regulates directly in the form of a rule and threat of ex post sanction where "Legislatures enact; prosecutors threaten; courts convict".[48] When regulation is indirect, however, "it aims at modifying one of the other structures of constraint"[49] Indirect regulation could be aimed at altering norms, market or architecture. The term indirect 'regulation', in this context, is used broadly and encompasses, for example, Industry Codes of Conduct, standards, regulatory boards such as the Australian Communications and Media Authority (ACMA), and obligations for the adoption of secure domain name registration policies.

1.2 METHODOLOGY

The research starts from a known social problem. Features of the methodology adopted include a multi-disciplinary approach; a comparative approach drawing on laws where relevant from

---

[45] APEC Telecommunications and Information Working Group, "Guide on Policy and Technical Approaches Against Botnet" (December 2008) available at http://publications.apec.org/publication-detail.php?pub_id=145 (last accessed February 7, 2011).
[46] *See* for example, Telstra, "Telstra Submission House of Representations Communication Committee Enquiry Into Cybercrime", Submission No. 43 available at http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub43.pdf (last accessed February 7, 2011).
[47] Note 41 above, Recommendation 9.
[48] Above, page 89.
[49] Above, page 95.

Australian, other jurisdictions, and international law; a literature review of the different approaches to botnets; select interviews and participation at invitation-only closed-session workshops in North America, Europe, Eastern Europe, Asia, and Australia; and theoretical research.

The research will be multi-disciplinary where materials from computer security, information systems, risk management, economics, regulation and law will be used in a combination of ways not previously undertaken in order to present an interactive overview of botnets. As part of a multi-disciplinary approach, a literature review for each relevant discipline has been undertaken. In particular, research and exploration of botnets has predominantly been compartmentalized with analysis falling into segregated areas of expertise. The technical community, for instance, has placed emphasis on propagation methods, detection and analysis of botnets. Within the legal field, the focus shifts to crimes and civil wrongs committed using botnets. For example, online fraud, identity theft, and spam are common topics in the area. Usually only a small portion of any given research will focus on how technology is used to commit a crime whereas emphasis is generally placed on evaluation of the law and proposed changes to provide an effective means of deterrence.[50] Along the same line , the technical literature lacks in depth analysis as to how the law interacts with technical attributes of botnet propagation, detection and response. Gaps of a similar nature likewise exist in other areas such as risk management and governance. One risk management approach to botnets, for instance, addresses optimal botnet management sizes whereby an economic model is used to estimate the most effective size for a botnet to be cost effective.[51] Under this theory, if the botnet is infiltrated and either its size is significantly reduced or conversely, significantly increased, the operations of the botnet will not be able to be effectively managed. The botnet master will expend its resources "herding" compromised computers or actively trying to establish the number of machines required to be connected to the botnet in order to perform the required task such as a denial of service attack.

While there has been insufficient inter-disciplinary research in the botnet field, there are still a number of general conclusions from researchers in their respective fields that are relevant to the problem. For example, the study of botnet structures may assist economists in determining

[50] One notable exception is the topic of denial of service attacks where analysis has been extended to risk management, liability allocation theories, and regulatory means of addressing the problem looking at both legal and technical components. *See* de Villiers, M. "Virus Ex Machine Res Ipsa Loquitor" (2003) Stanford Technology Law Review 1; and Chandler, J. "Security in Cyberspace: Combating Distributed Denial of Service Attacks" (2003-2004) 1 University of Ottawa Law & Technology Journal 231.

[51] Li, Z., Liao, Q., and Striegel, A., *Botnet Economics: Uncertainty Matters* (Springer 2009).

optimal botnet sizes. This in turn may assist law enforcement and security researchers with the approach taken to botnet countermeasures. Currently, the approach is that as many compromised computers as possible should be rehabilitated and severed from the botnet. The more effective method, however, in combating a particular botnet may be to add another 100 000 or a million new compromised machines to the botnet making its management and operations unworkable. The study of botnet propagation methods may assist governance research in how best to deal with the problem. For example, there is an assumption amongst some writers that certain internet ports are hotbeds for criminal activity and that the mere blocking of these ports would lead to a reduction in cybercrime.[52] The problem with this type of analysis is that it assumes that certain ports have properties that lend themselves to cybercrime whereas other ports could not be used to perform the same acts. The deficit in the research may again be attributed to a few key factors. The first is that the topic is an emerging field. The second, and paramount point, is the difficulty in exploring the topic. That researchers are tackling problems from their respective areas of expertise is to be expected and is logical. This segregated problem-solving technique has, however, become an obstacle in successfully responding to the problems created by botnets. An inter-disciplinary approach to botnets is mandatory to any successful and potentially efficient policy response.

This research will involve Australian and international law. The law from other jurisdictions will be considered where appropriate. There is paucity of botnet related caselaw which necessitates exploring as many jurisdictions as possible for materials. For example, there is only one reported decision in the world for the prosecution of a botnet master. This is the New Zealand decision of *R v Walker* which will be explored in **Chapters 3, 4 and 6**. There have been other arrests made against botnet masters in the United States, Spain and Russia but the cases have settled out of court and are, therefore, not reported decisions. Materials from such arrests may only be obtained through media coverage of an incident, and through requests for information from those security researchers and law enforcement involved in the investigation. To the extent possible, information has been obtained from those involved in such botnet investigation either through informal means or through asking questions at closed-session workshops where Chatham House Rules apply.[53]

[52] *See for example*, 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

[53] The rule is:

Ethical clearance from the University was obtained to interview key stakeholders in 2007. As part of this process, the questions asked in the interviews were restricted to those questions previously approved by the ethics committee. In 2007 I interviewed some stakeholders in digital forensics, computer hackers, computer security researchers, chief information technology officers of internet service providers and financial institutions, and corporations with a large online presence. I quickly identified that the set of approved questions was insufficient and even, in some instances, proven to be of limited relevance. More importantly, the interviewees provided much more information as well as completely unanticipated information which led to further ethical difficulties. For instance, many of the individuals that I had interviewed were involved in illegal activities in combating malware, fraud and botnets. This often included the hiring of professional black hat hackers for specific tasks, or employing such hackers within the corporation, or by performing offensive computer counter-strategies (sometimes without authorisation of a company's Board of Directors). I faced several problems with these interviews. Firstly, I became knowledgeable about the commission of criminal acts and the intention to commit criminal acts in the future; such acts under the law profession must be reported to law enforcement. Secondly, the information given by interviewees was not restricted to the approved ethical questions and, therefore, I was not able to include this information in the thesis. Third, attribution to interviewees could have consequences for these individuals including being fired from their employment, media scrutiny or charges being laid by law enforcement. The most unanticipated obstacle, however, involved my physical safety and that of my family. Several of the people whom I spoke with early on in the research strongly recommended against my researching the Russian Business Network and naming individuals whom I had interviewed. These researchers indicated that, where they had named individuals and organisations in the past in their research, they had received death threats, suffered from online sabotage, their personal information was exposed to the public, and often denial of service attacks were performed to their respective organisations. All of the above risks contributed to my decision to not directly source the materials obtained from the interviews, to altogether avoid naming any individuals whom I have interviewed, and to additionally avoid referencing the Russian Business Network in the research. This is clearly not ideal for research. I was still able, however, to use much of the information obtained in the interviews through

---

"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

See Chatham House Organisation available at http://www.chathamhouse.org.uk/about/chathamhouserule/ (last accessed February 7, 2011).

different sourcing techniques. Many of the individuals I have interviewed participate in forums such as blogs, conferences, workshops, and media interviews where their opinions, experiences and information are publicly available. The most valuable source of much of the information in the research came from invitation-only closed-session workshops where key stakeholders participated in open discussion of the issues that they were facing. Such sessions often involved security researchers, internet service providers, financial institutions, hackers and law enforcement. I attended such closed-sessions in Australia, the United States, the United Kingdom, and Estonia. Chatham House Rules applied to all of the closed-session workshops. During these sessions I asked a number of contentious questions to workshop participants. Participants in closed-sessions are not identified and comments arising from such sessions are not attributed to individuals or organisations.

In addition, theoretical research was undertaken into Internet regulatory theories. Botnets will be used as a case study to assess whether such theories are able to account for regulatory actions taken to combat against botnets. The purpose of this was to identify any deficiencies in internet regulatory theories to account for the levels and types of internet crimes and response to such criminal activity. The theoretical framework is considered in the following section.

1.3 THEORETICAL FRAMEWORK

Criminologists have used a many criminal theories to explain cyber crimes with varying success. Traditional theories such as social learning theory[54], moral development theory[55], deindividuation theory[56], routine activity theory[57], and multiple theories[58] have been used to explain the behaviour of cyber criminals. Less traditional criminal theories such as space transition theory[59] and game theory[60] have also been used to describe online criminal behaviours. Criminal theories have not been selected in this research for many reasons. The application of these theories to cybercrime

[54] Skinner, W. and Fream, A., "A Social Learning Theory Anlaysis of Computer Crime Among College Students" (1997) 34 Journal of Research in Crime and Delinquency 495.
[55] Rogers, M., "Psychological Theories of Crime and Hacking" (Dec. 15, 2006) Telmatic Journal of Clinical Criminology.
[56] 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.
[57] Yar, M., "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory" (2005) 2(4) European Journal of Criminology 407.
[58] Taylor, R., Caeti, T., Loper, K., Fritsch, E., and Liederbach, Digital Crime and Digital Terrorism (UK: Pearson, 2005).
[59] Jaishankar, K., "Space Transition Theory of Cybercrimes" in Schmalleger, F. And Pittaro, M. *Crimes of the Internet* (Pearson: Prentice Hall, 2009).
[60] Kshetri, N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspective* (Springer, 2010) p 245.

share a common trait, they are predominantly focused on why individuals commit cybercrime and the potential consequences to the community once such crimes have been committed. While factors leading to cybercrime are both important and interesting, there is an assumption that there is sufficient empirical research on botnet masters. As noted in **Chapter 4**, there is only one publicly available case against a botnet master in the world. In order to successfully apply many of these criminological theories to botnets would require express access and contact with many botnet masters. Lastly, many prominent cyber-criminologists such as Wall and Katyal (explored in **Chapter 2**) have themselves have selected Internet regulatory theories as opposed to traditional criminological theories. For these reasons I too have chosen Internet regulatory theorists over traditional criminology theories.

Botnets may not be a problem that the law necessarily needs to respond to. More precisely, botnets may not be a problem that nation states need to respond to through the enactment of domestic laws. In fact, it may be the case that various actors are turning a blind eye to the law or, that the alternatives to law such as "taking the law into one's own hands" may deliver better results from an efficacy point of view, though not necessarily an ethical one. In this respect, this thesis will use a dichotomy to distinguish between what is legal and what is legitimate. The law - that is, what is legal - is premised on the notion that there, "is a system of enforceable rules governing social relations and legislated by a political system."[61] Breach of a rule results in an activity being classified as illegal. Legitimacy in this context is used in its broadest sense to reflect what may be moral yet illegal. Law's primary role may be to legalise some of the ethical yet illegal actions.

In commenting on hacking and information warfare, Martin Libicki of the RAND Corporation comments:

> "If the government cannot make system owners protect themselves, should it nevertheless be responsible for their protection? … If the privatization of security in cyberspace makes sense, why not encourage vigilantes in cyberspace? Suppose that the victim nation fingers the likely suspects, or they reveal themselves. It then slips to talented mischief makers a few under the table hints about the adversary's weak spots and presto: the dogs of war have been loosed in ways that prevent counterdeterrence, since the hackers cannot be recalled. But, then again, this may drag everyone into a war whose echoes die out all too slowly. As it is, difficulties in controlling the level of cyber-violence mitigate against liberating the super-patriot hackers – as if it mattered. They are unlikely to ask for permission if aroused."[62]

[61] Sypnowich, C. (2001) Law and Ideology, Stanford Encyclopedia of Philosophy, available at http://www.plato.stanford.edu./entries/law-ideology

[62] Libicki, M. *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge 2007), p.274-276.

Libicki's work implies that regulation may be more effective through illegal means. Early Internet regulatory theories reflect similar propositions to those of Libicki where their emphasis is placed on the diminishing role of law. Early Internet regulatory theorists did not account for the potential for the Internet to become a prime vehicle for criminal acts**.** Methods used to counter botnets are not easily situated within Lessig's theory due to the unconventional approaches required such as Internet Service Provider bot remediation programs and threat mitigation methods by expert security third parties to infiltrate and attack the command and control of botnets. The challenge of regulating botnets may be indicative of a larger problem of situating responses to cybercrime within existing Internet regulatory theories.

Internet regulatory theories will be analysed and applied to botnets in **Chapter 2** with emphasis on the works of Lawrence Lessig. Lessig's theory was promulgated under the belief that control of the Internet would be a tug-of-war between users (including self-governance Internet bodies such as the Internet Engineering Task Force) and national governments. The libertarians such as Barlow, Johnson and Post wrote about how the architecture of the Internet prevented governments from applying traditional forms of laws and rules. Meanwhile Lessig wrote about architectural components of the Internet and possible interaction with the law.[63] The new Chicago school was emerging in the 1990s where the works of Lessig featured as one of the main contributors.[64] The works of Lessig have become the most influential in the field of Internet regulatory theory. Central to Lessig's work is the notion of legal pluralism where regulation comes not only from traditional forms of law, but encompasses a larger body of regulation which is thought of as acting with other factors such as market, code and norms. Lessig's model is pluralistic in his acknowledgement of regulation being shaped by four modalities (market, norms, code and law) as well as by addressing how Internet governance is transnational and collective.

Chapter 2 will focus on the works of Lawrence Lessig, particularly the ideas in *Code: And Other Laws of Cyberspace*. Lessig's regulatory model looks at four modalities: market, architecture, norms, and law. As will be shown through **Chapters 3 through 8,** effective botnet regulation will involve some use of illegal means, and inevitably will challenge not only the mindset that the

---

[63] *See* Wu, T., "Application-Centered Internet Analysis" (1999) 85 Vanderbuilt Law Review 1163. *See also* Saltzer, J., Reed, D. and Clark, D., "End-to-End Arguments in System Design", in Partridge, C., ed, *Innovations in Internetworking* (Artech House, 1988).

[64] Lessig, L., "The New Chicago School" (1998) 27 Legal Studies 661; Lessig, L., "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harvard Law Review 501; Lessig, L., *Code: And Other Laws of Cyberspace* (Basic Books, 1999).

law plays an authoritative role in regulation, but equally challenges Lessig's theory that market, architecture, and norms are equally up to the task. Changes or developments of Lessig's model may be required. Many of the actions by self-organised security groups to combat botnets, which are examined in **Chapter 8**, may be conceived as effective and moral though, as will be demonstrated, clearly illegal. The final chapter of this research highlights problems with Lessig's theory in the context of botnets which will likely find relevance for addressing other areas of cybercrime.

1.4 FOCUS OF RESEARCH: REGULATORY APPROACHES TO BOTNETS

This section provides an overview of the chapters in the dissertation and establishes the concentration of the thesis, effective approaches to combating botnets.

1.4.1 Botnets

Chapter 3 is an examination of botnets. The chapter commences with looking at Design - how to build a botnet. This includes looking at social engineering methods and software used in bot acquisition, what computers are most vulnerable to being compromised (e.g. not running anti-virus software) and offers a comparison of the technical structures of different botnets. The next section addresses Motivation. In other words, why one would want to build a botnet (e.g. hacker curiosity, financial gain, involuntary coercion)? This is followed by Uses of botnets. This includes an examination of bot instructions (payload instructions) and relates them to types of criminal activities. For example, a botnet may be built or hired out to perform a denial of service attack. Associated technologies used in conjunction with botnets are next examined such as what is meant by using dynamic DNS so that a botnet operates on a fast-flux basis. Lastly, botnet countermeasures are examined. These include a mixture of technical and legal methods. Five examples of botnets at the end of the chapter provide context to the technical discussion.

1.4.2 The Australian Criminal Law Landscape For Botnet-Related Prosecutions

Chapter 4 analyses the national criminal law framework in Australia relevant to botnets. While there are many other types of offences that could conceivably fall within the Australian criminal framework, only the offences that an accused would mostly likely be charged with will be considered. The most relevant offences include: unauthorised access, modification or impairment to data or electronic communications; dishonest use of a computer; conspiracy (to

defraud); fraud and aiding and abetting. It will be argued that the current state of Australian criminal law is sufficient to prosecute a botnet master. The real challenge as seen in the previous chapters stems from generic challenges and obfuscation crime tools.

1.4.3 The International Criminal Legal Framework Relevant to Botnets

Chapter 5 analyses the most significant international treaty in the area, *The Council of Europe's Convention on Cybercrime.* This chapter outlines the articles of the *Convention* relevant to botnets, offering a comparative perspective with the *Criminal Code (Cth)* provisions. Both substantive and procedural elements of the *Convention* are explored. The advantages and disadvantages of Australia signing and ratifying the *Cybercrime Convention* are discussed, with a series of proposals offered at the end of the section.

The next section touches on the *United Nations Convention on Transnational Organized Crime.* The remainder of the chapter identifies global initiatives linked to cybercrime and security. Most global initiatives linked to cybercrime and security are unenforceable cooperative agreements between nations. While there are a number of international bodies and coalitions within the domestic and international spheres, the more prominent international bodies are Interpol and the United Nations (UN). The final section examines other international organisations and initiatives that play a role in cybercrime investigation but have a somewhat diminished role in the combat against botnets. It is shown that International instruments such as the *Convention* will do little to aid in the investigation and prosecution of botnet herders.

1.4.4 Challenges to the Investigation and Prosecution of Botnet Masters

Chapter 6 addresses botnets within the broader themes of criminal investigation and prosecution. Generic challenges to effective botnet prosecutions include: volume and volatility of digital evidence, real-time forensics, the content warrant framework, jurisdiction, and traceback and attribution. The real challenge of prosecuting botnet masters stems from generic challenges and obfuscation crime tools and not from inadequate legal provisions and treaties as detailed in the previous two chapters.

1.4.5 The Role of Connectivity Enablers in Combating Botnets: Internet Service Providers and Domain Name Service Providers

Chapter 7 will examine the role of Internet Service Providers (ISP) and Domain Name Service (DNS) providers in combating botnets. The chapter will provide details of ISP initiatives aimed at disrupting the botnet industry. The chapter addresses the Australian Internet Industry Association (IIA) Code of Practice consultation paper on "For Industry Self-Regulation in the Area of E-Security"[65] , and the Comcast initiative in the United States currently before the IETF potentially for consideration as an international standard.[66] Both initiatives involve ISP monitoring and detecting compromised computers connected to their networks, notifying customers when their computers are infected and part of a botnet, and then assisting customers to remedy the situation. A brief re-examination of botnets is provided to expand on the commentary that follows on ISP initiatives. Comments are made on the IIA and Comcast Schemes. Critical components of each scheme are analysed. A series of new and original proposals are made in the area of detecting and monitoring techniques. An examination is made of how detecting and monitoring exposes ISPs to liability under the *Privacy Act, Telecommunications Act* and *Telecommunications (Interception and Access) Act*. The chapter also discusses the new 'fit for connection' concept, and proposes that ISPs should be shielded from liability from wrongful disconnection where they act in good faith.

1.4.6 Self-Organised Security Communities

Chapter 8 provides a detailed look at the work of self-organised communities to combat botnets. It explains the critical role that self-organised communities have played in dealing with botnets. The functions of four types of communities are examined: security organisations (ShadowServer, Spamhaus, Offense-in-Depth Initiative, and Independent Spamhunters), university researchers, botnet working groups and not-for-profit security corporations. The internal workings of these groups will be discussed based on correspondence with key members, publicly available documents, and conference presentations and panels.

---

[65] Internet Industry Association, *Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security* (September 2009).
[66] Livingood, J., Mody, N. And O'Reirdan, M. of Comcast, Internet Engineering Task Force Working Draft, *Recommendations for the Remediation of Bots in ISP Networks* (September 2009) [hereinafter Comcast].

The inability of traditional constraints such as market, technologies and law enforcement to counter botnets, has led to the establishment of many self-organised anti-malware and anti-botnet communities. **Chapter 2** will examine Internet regulatory theories with a more detailed analysis of Lessig's four modalities. It will be seen in **Chapter 3** that botnets were being used to commit crime in an unprecedented and unanticipated manner that was not predicted by early Internet scholars and industry players. As a result, many existing theories do not resonate well with what is currently seen both in terms of malware proliferation, crime, and response to the problem. This chapter will demonstrate the role of self-organized security communities is not easily situated in any Internet regulatory theory, and cannot be reconciled within Lessig's four modalities of market, code, law and norms.

1.5 EXCLUDED REGULATORY MEASURES

This dissertation focuses on the set of potential regulatory mechanisms for botnets which, based on the preliminary research work, indicated are most likely to achieve the intended effect. This section briefly discusses a range of potential regulatory approaches that have limited potential, and that are not further considered in the analysis. These include end-user remedies, education and training, data breach notification, Sarbanes Oxley, non-criminal legal remedies (software producers, tort of negligence, banking law, and product liability), internet filters, and follow the money techniques.

1.5.1 End-User (Consumer) Remedies[67]

The end-user continues to be one of the weaker links in the security chain. The present form of consumer protection may be stated as running anti-virus software or putting up a firewall.[68] This checks incoming files for known instances of malware and bot acquisition. There are many such products, all with varying degrees of efficacy. No anti-virus software is entirely effective at blocking malicious software and bots.[69] The opposite holds true in that the most damaging botnets such as Storm and its variants (e.g. Waledac) were not detected by any anti-virus product

[67] Some end-user and consumer remedies are explored in Clarke and Maurushat, note 5 above.
[68] *See* critique of consumer protection through anti-virus by Yar, M., "The Private Policing of Internet Crime" in Jewkes, Y. and Yar, M. (eds) *Handbook of Internet Crime* (Willan Publishing, 2010), page 546.
[69] *See* for example 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), page 171.

for a significant amount of time.[70] New forms of sophisticated malware and bots are rarely detected by anti-virus products when they first emerge on the Internet.

While end-user remedies are important, they are not identified as the most important and efficient methods of countering botnets. The reason is that educating a billion users how to secure their machines and safely use the Internet is likely not possible, and if possible, would be a resource and time-intensive effort. This is the equivalent of teaching the world how to drive a car safely and ensuring that all vehicles are safely manufactured and driven afterwards – a process which took close to 50 years.[71] End-user remedies such as the development of secure software, the requirement of users successfully completing a licensing test with continued renewals before they use a computer, and cybersecurity education in primary schools will take a great deal of time. In addition to the time impediment, implementing anti-virus products requires understanding, patience, skills and investment. Such products need to be acquired (usually for money), installed, configured, and then run.[72] Installation of such products can also create additional vulnerabilities.[73] In addition, because malware is in a state of continual adaptation, such software and the data that supports it require frequent updating. Updating is onerous if performed manually; but if the process is automated it may create yet further vulnerabilities. All such protections are incomplete because there is a lead-time between the creation of new malware, discovery by the suppliers of protection software that it exists, discovery of the malware's 'signature' whereby it can be recognised, and distribution of the new data or software version to consumers' devices. While this research recognizes that anti-virus products assist in the reduction of compromised computers, the use of such products by the end-user will not by itself solve the botnet problem. For these reasons, end-user remedies have been excluded.

1.5.2 Education and Training[74]

Public education programs are seen as a way to reduce the incidences of users becoming victims of cyber-security incidences such as fraud and identity theft. Governments around the world are struggling to develop appropriate and cost-effective means to deliver cyber-security education

---

[70] *See* Schneier, B., "The Storm Worm" (October 4, 2007) available at http://www.schneier.com/blog/archives/2007/10/the_storm_worm.html (last accessed December 2010).
[71] *See* Rice, D., *Geekonomics: The Real Cost of Insecure Software* (Addison-Wesley, 2008), pages 19-68.
[72] Clarke, R. and Maurushat, A., note 5 above.
[73] Clarke, R., and Maurushat, A., note 5 above
[74] The Australian Communications and Media Authority (ACMA) commissioned a report on cyber-security education and training initiatives to be presented at APEC forum. *See* Connelly, C., Maurushat, A., Vaile, D., and van Dijk, P., *Cyber-Security Education Research Project* (2010). A copy of the report is on file with author.

and training. Organisations additionally find it challenging to evaluate the effectiveness of education and training initiatives. Qualitative and quantitative metrics are difficult to put into place for such initiatives. As many cyber-security education and training initiatives are relatively new, a consensus as to the most effective initiatives has not yet emerged.[75] There is also uncertainty as to whether cyber-security education and training will reduce cybercrime as the sophistication of the tools and modes of delivery of cybercrime are escalating beyond the grasp of the average user. Public education and training initiatives remain nonetheless important in spite of their overall inadequacy to significantly improve the security landscape.[76] Public education and training campaigns will not be considered in detail in the research but will be referenced within the confines of various proposals to counter botnets as for example in **Chapter 7** looking at ISP bot remediation programs.

1.5.3 Data Breach Notification for Corporations and Organisations[77]

The Australian government, in an attempt to fight escalating levels of cybercrime and inter-related privacy and security threats, is pushing for legal reform in privacy law. The Australian Law Reform Commission published a lengthy report recommending an overhaul of privacy law in Australia so that data security obligations requiring companies to take reasonable steps to protect personal information would be amended and data breach notification requirements would be introduced.[78] In essence, data breach notification legally requires corporations and organisations to notify individuals when a breach of security leads to the disclosure of personal information. Two related phrases aptly describe the impetus behind such laws: *"Sunlight as disinfectant"* and the *"Right to Know"*.[79] Data breach notification is based on the theory that the consumer has the right to know when their personal information has been stolen or compromised. Data breach notification laws would provide an incentive for corporations and other organizations to take adequate steps to secure personal information they hold. In this sense, exposing security breaches of corporations would shine "sunlight" onto an organization's security practices, and would "disinfect" those problematic security areas requiring change.

---

[75] Above.
[76] *See* notes 41 and 5 above.
[77] A draft chapter was written on Data Breach Notification and was subsequently determined to be too outside the scope of botnets to be included. *See* Maurushat, note 51 above where the article includes a table comparing data breach notification regimes from 25 jurisdictions.
[78] Australian Law Reform Commission, Review of Australian Privacy Law, Discussion Paper 72, September 2007.
[79] These phrases are attributable to Justice Louis Brandeis. *See* Warren, S. and Brandeis, L., "The Right to Privacy" (1890) 4 Harvard Law Review 193. The sunlight reference is documented at http://www.brandeis.edu/investigate/sunlight (accessed January 30, 2009). My first acquaintance with the sunlight expression came from a paper written by Romanosky, S., Telang, R., and Acquisti, A. "Do Data Breach Disclosure Laws Reduce Identity Theft? Seventh Workshop on the Economics of Information Security, June, 2008.

The scope of such notification and disclosure schemes varies greatly from country to country[80]. Many jurisdictions such as the United States, the European Union have tabled Bills or passed Acts legislating mandatory data breach disclosure. Other jurisdictions such as Canada and Japan have instituted voluntary guidelines. In many jurisdictions, data breach notification is currently sector specific (e.g. banking and financial sector or the telecommunications sector). Data breach notification laws provide incentive for corporations to improve their overall online security practices which may, in turn, have an effect on cybercrime rates, and in particular, on fraud and identity theft crimes.[81] Data breach notification laws do not, however, apply to end-users. The majority of compromised computers are the personal computers of end-users.[82] While some data breaches may be caused by malware, and a small subset of those breaches through malware which was installed due to a botnet, the majority of data breaches are caused from insiders and human error.[83] The extent to which data breach notification is linked to botnets is sufficiently remote as to remove it from the scope of the research.

1.5.4 Sarbanes Oxley Act[84]

The Sarbanes-Oxley is named after the United States Senators, Paul Sarbanes and Michael Oxley, who sponsored the *Public Company Reform and Investor Protection Act* commonly referred to as the *Sarbanes-Oxley Act.*[85] The Act introduced regulations which substantially restructured the U.S. accounting and finance industries with increased penalties including criminal offences again company executives. The Act's main thrust was to address requirements for a variety of audits, and to allow for criminal prosecution of members of the Board of Directors where it could be demonstrated that the corporation failed an audit and insufficient action to remedy the problem

---

[80] Maurushat, note 51 above.

[81] Early empirical studies indicate that data breach notification laws do not reduce fraud and identity theft rates. *See* Romanosky, note 63 above; and *see also* Ponemon Institute, 2009 Annual Study: U.S. Enterprise Encryption Trends available at http://www.encryptionreports.com/2009etrends.html (last accessed November 10, 2009). Similar studies are available for 2008 and 2007 available at http://www.encryptionreports.com/encryptiontrends.html (last accessed November 10, 2009).

Other excellent data breach notification analysis includes the works of 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); Matswshyn, A.(ed) *Harboring Data: Information Security, Law, and the Corporation* (Stanford University Press, 2009); and Winn, J. "Are 'Better' Security Breach Notification Laws Possible?" (2009) Berkeley Technology Law Journal Volume 24:3.

[82] *See* Govil, J., "Examining the Criminology of Bot Zero" Information, communications & Signal Processing 6th International Conference on (2007) available at http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4449633&tag=1 (last accessed December 2010).

[83] S*ee* Ponemon Institute, 2009 Annual Australian Enterprise Encryption Trends available at http://www.encryptionreports.com/2009etrends.html (last accessed Nov. 10, 2009).

[84] Maurushat, A."Standing Behind Technical Promises" (2008) AusCERT Asia Pacific Information Security Conference.

[85] *Sarbanes-Oxley Act 2002* , 15 U.S.C.§ 7241 (civil sections) and 18 U.S.C. § 1350 (criminal provisions).

was pursued afterwards.[86] The Act applies to all U.S. public companies as well as to foreign companies that are cross- listed on a public exchange on levels 2 or 3.[87]

Many of the auditing obligations in the *Sarbanes-Oxley Act* are replicated in Australian legislation such as the *Corporate Law Economic Reform Program (Audit Reform & Corporate Disclosure Act 2004 (Cth).* The auditing obligations include a computer security audit (or information technology audit).[88] Computer security standards, audits and related obligations in Sarbanes-Oxley style legislation play a similar role to that of data breach notification. They are meant to prevent security breaches and to act as an impetus to improve how corporations protect their data and online infrastructure. A corporation could be the target of a botnet attack, and could also have their computers compromised to a botnet. The role of the corporation is also one of victim. Again, the connection to botnets is too remote and thus has been excluded from the scope of the research.

1.5.5 Non-Criminal Legal Remedies[89]

One possible way of deterring botnet operations is to take civil action as opposed to using a criminal law framework. Civil action could be taken against two categories of parties – botnet masters, and those who use their services. This approach shares the same challenges as a criminal law approach – which is explored in **Chapter 4 through 6**. Due to the use of obfuscation tools such as fast-flux and onion routing, traceback to the source of an attack to identify the botnet master is extremely difficult. The following civil law areas are explored and excluded as major concentrations (though they will still be considered in a minor fashion) in the thesis including civil actions against software producers, the tort of negligence (and other similar torts), banking law, and product liability law.

1.5.5.1 Software Producers

---

[86] Mollett, S., "Sarbanes-Oxley 307 Domestically and Abroad: Will Section 307 Lead to International Change?" (2008-2009) 11 Duquesne. Business Law Journal. See also McGrane, B., "The Audit Committee: Director Liability in the Wake of the Sarbanes-Oxley Act and *Tello v. Dean Witter Reynolds*" (2008-2009) 18 Cornell Journal of Law & Public Policy.

[87] Litvak, K., "Sarbanes-Oxley and the Cross-Listing Premium" (2007) 105 Michigan Law Review. Level 2 and 3 cross-listing are referred to as level-23 foreign companies. Level 1 and 4 cross-listed companies are not subject to the *Sarbanes-Oxley Act*.

[88] See Atkin, T.. et al., *Information Security Management Handbook* (CRC Press, 2006).

[89] Clarke and Maurushat, note 5 above.

One option is to sue those in a position to prevent attacks such as software and hardware developers that produce insecure products. This option is currently unavailable as liability cannot be imposed on software and hardware producers for negligently-designed products.[90] Software and hardware companies are shielded from most forms of consumer protection law through warranty clauses. While computer software is inherently insecure and there is a need to take responsibility for producing more software with less severe vulnerabilities, software liability is deeply enmeshed in a long political debate with strong lobbyist protection of the industry.[91] In addition, as will be seen in **Chapter 3**, the more sophisticated botnets responsible for the greatest threats and size of criminal activity are not dependent on software vulnerabilities to acquire compromised computers. For these reasons, non-criminal remedies are not pursued further in this research.

1.5.5.2 Tort of Negligence

The decision to exclude negligence from the research required much contemplation as most of the legal literature on botnets, malware and denial of service attacks is focused on negligence and elements of torts such as reasonable foreseeability.[92]

Where an entity knew or ought to have reasonably known that the use, sale or reliance on a device, equipment or network contained security vulnerabilities, there is the possibility of a civil

---

[90] Scholars such as Jennifer Chandler and Meiring de Villiers have written on tort liability for insecure software. *See* Chandler, note 50 above. *See also* an economic model for software liability in de Villiers, M., "Information Security Standards" (2009) University of New South Wales Law Research Paper Working Paper 34..

[91] *See generally* Rice, note 71 above.

The Parliamentary Report on Cybercrime, note 41 above has taken note of the insecure nature of software and hardware products. Recommendation 25 states, "That the Treasurer direct the Productivity Commission to conduct an in depth investigation and analysis of the economic and social costs of the lack of security in the IT hardware and software products market, and its impact on the efficient functioning of the Australian economy. That, as part of its inquiry, the Productivity Commission address the merits of an industry specific regulation under the Australian Consumer Law, including a scheme for the compulsory independent testing and evaluation of IT products and a product labelling scheme." Recommendation 26 goes further and calls for a cause of action for compensation. Recommendation 26 reads, "That the Treasurer consult with State and Territory counterparts with a view to amending the Australian Consumer Law to provide a cause of action for compensation against a manufacturer who releases an IT product onto the Australian market with known vulnerabilities that causes losses that could not have reasonably been avoided."

[92] *See* the works of de Villiers, note 50. *See also* de Villiers, "Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare" (2005) 4 Northwestern Journal of Technology and Intellectual Property 1**;** de Villiers, "Distributed Denial of Service: Law, Technology & Policy" (2006) World Jurist Law/Technology Journal v. 39 n. 3; and de Villiers, "Reasonable Foreseeability in Information Security Law: A Forensic Analysis" (2008) 30 Hastings Communications And Entertainment Law Journal.
See also Chandler, J. "Liability for Botnet Attacks" (2006) Canadian Journal of Law and Technology; and chandler, J., "Technological Self-Help and Equality in Cyberspace" (2010) 55 McGill Law Journal.

suit using the tort of negligence. The scope of negligence is sufficiently broad to allow anyone in the chain of information leading to an unauthorized online banking transaction to potentially be liable.[93] This could conceivably include the consumer, device manufacturer, software developer, and financial institution. In order for an act in negligence to succeed, it must be shown that there was a duty of care between the parties, and that physical damage was sustained. There are a number of enforceable contracts and agreements leading to a duty of care. For example, a bank may be responsible for maintaining a secure network making sure that none of its equipment malfunctions. Likewise, some warranties may apply to consumer devices. Where device vendors sell insecure hardware products, they may be exposed to liability. Where a user is made aware of a threat or vulnerability and fails to take reasonable measure to remedy the defect, he or she may also be found partially liable for any damages sustained by a party.

Even in simple cases, the law of negligence provides no remedy. Due to the complexity of Internet infrastructure, linking effects to causes is infeasible, identifying the relevant party is often not easy, and collecting and presenting evidence of fault is enormously challenging.

One scholar has argued that owners of compromised computers should owe a duty of care to other users and be liable under negligence for insufficiently securing their computers allowing for a botnet master to use their computer to perform a denial of service attack.[94] This argument demonstrates both an inadequate grasp of botnet structures, propagation and dissemination, and the inappropriateness of negligence law as a solution. Firstly, the likelihood of successfully identifying the botnet master is remote as will be explored in **Chapter 6.** If a botnet master were identified and there were sufficient evidence, he or she could be found liable under negligence. Secondly, as will be seen in **Chapter 3**, botnets tend to have anywhere between 1000 and 10 million compromised computers connecting to a single botnet. These compromised computers may be located anywhere in the world. To select the individuals responsible for one or two compromised computers (likely of those located in the most convenient jurisdiction) out of possibly millions of compromised computers is at least inequitable. Moreover it is generally the cumulative effect of many compromised devices that causes the problem, and the contribution of any one of them is very small. Moreover, the most sophisticated and damaging botnets exploit vulberabilities in firewalls, anti-virus and other security products rendering them ineffective. Even if an end-user installs anti-virus software and updates it regularly the computer is still

[93] For general discussion on the tort of negligence see Fleming, J., *The Law of Torts 8th ed* (The Law Book Company 1992) pages 101-315.
[94] Guzman, L., "Unleashing a Cure for the Botnet Zombie Plague" (2010) 59 Catholic University Law Review 527.

susceptible to becoming part of a botnet. For these reasons, imposing liability on the owner of a compromised machine is not appropriate.

The last reason for dismissing non-criminal remedies is one of manageable size and scope for the research. In order to fully explore the topics, the torts of trespass, nuisance, and negligence would need to be discussed in depth including chapters devoted solely to issues of foreseeability and duty of care. As non-criminal remedies appear unlikely to play a significant role in combating botnets, they have been excluded from the research.

1.5.5.3 Banking Law[95]

Banking law is relevant where botnets are used to acquire financial information and commit fraud. In this instance, the liability scheme of who bears such loss becomes of pivotal importance. In Australia, the Electronic Funds Transfer Code is the chief source of obligations between the customer and financial institution for instances of computer and mobile phone failure, and unauthorised bank transactions. Under the current scheme, users are liable for loss due to negligent conduct such as writing a password on a yellow tab and leaving it under your keyboard.[96]

Consumers are not liable for unauthorised transactions occurring after notification. Where a bank can prove that a user contributed to the loss, the consumer is generally liable for losses. According to clause 5.5, the consumer may not, however, be liable for pre-notification losses

---

[95] Clarke and Maurushat, note 5 above.

[96] Clause 5.2

> (a) losses that are caused by the fraudulent or negligent conduct of employees or agents of the account institution or companies involved in networking arrangements or of merchants or of their agents or employees;
> (b) losses relating to any component of an access method that are forged, faulty, expired, or cancelled;
> (c) losses that arise from transactions which required the use of any device or code forming part of the user's access method and that occurred before the user has received any such device or code (including a reissued device or code). In any dispute about receipt of a device or code it is to be presumed that the item was not received by the user, unless the account institution can prove otherwise. The account institution can establish that the user did receive the device or code by obtaining an acknowledgment of receipt from the user whenever a new device or code is issued. If the device or code was sent to the user by mail or email, the account institution is not to rely only on proof of delivery to the user's correct address as proof that the device or code was received by that person. Nor will the account institution have any term in the Terms and Conditions which deems a device or code sent to the user at that person's correct address (including an email address) to have been received by the user within a certain time after sending; or
> (d) losses that are caused by the same transaction being incorrectly debited more than once to the same account.

exceeding the daily and periodic transaction limits, and losses beyond the account balance. There is no legal requirement for the financial institution to refund the money stolen, however, Australian financial institutions have routinely refunded such stolen money.

Clause 5.6 identifies situations where the customer/user would contravene the Code and, therefore, have contributed if not caused the access method to be compromised. Applicable situations include where a user voluntarily discloses the code, the code is placed on or around a device used to access the account (eg. yellow post-it under keyboard or PIN on ID token), recording PIN on article, selecting forbidden PINs(e.g. birthday or name); or otherwise acting with extreme carelessness with the PIN. In short, while users may record the access code, they have a general obligation to keep the code safe and protected.

Clauses 6 and 8 of the Code impose additional obligations on financial institutions for equipment and system malfunction, along with failed or compromised network arrangements (Eg. Retailers for EFTPos) though in practice, banks have not been held accountable for failed systems.[97] There are no further factors of banking law relevant to the research. Again, for the reason of remoteness, banking law is excluded from the research.

1.5.5.4 Product Liability (*Trade Practices Act 1974* (Cth) and *Sale of Goods Act*)[98]

Consumers are generally protected from faulty goods and onerous contractual terms by the *Trades Practices Act 1974 (Cth)* (*TPA*) and the various *Sale of Goods Acts* (*SGA*s). The *TPA* was renamed the *Competition and Consumer Act* (*CCA*) on January 1, 2011.[99] This recent amendment, however, did not alter the body of law under the former *TPA* relevant to botnets. There are no cases under the *CCA* that are relevant to botnets, therefore, reference will be made to the *TPA* and not the *CCA*. Both the *TPA* and *SGA*s include sections containing the term 'goods'. The law imposes certain terms on some contracts, and confers benefits to consumers in specific contexts when dealing with 'goods'. A contentious issue has consistently been whether software is a 'good' or a 'service'.[100]

---

[97] Clarke and Maurushat, note 5 above.
[98] Clarke and Maurushat, note 5 above.
[99] *Competition and Consumer Act 2010* (Cth). For more information on the new act see the Australian Competition and Consumer Commission available at http://www.accc.gov.au/content/index.phtml/itemId/3653 (last accessed February 2, 2011).
[100] *See Amlink Technologies and Australian Trade Commission* [2005] AARA 359.

In the 2005 Australian Trade Commission (ATC) decision in the Amlink case, software was found to be a 'good' (*Amlink Technologies and Australian Trade Commission* [2005] AATA 359). In reaching his conclusion, Senior Member McCabe compared products that were supply of know-how or intellectual property with those which provided a contract for the supply of goods. Though classifying software as a 'good' in the Amlink decision, the ATC fell short of delineating whether software which is not attached to a physical object (e.g. CD ROM) could be classified as a good. As such, software companies can continue to insert warranty clauses into their terms of use shielding them from lawsuits for software security flaws leading to financial loss. There is no obligation for manufacturers to "take any responsibility for designing security into the product."[101] The *TPA* entitles consumers to products that are "fit for purpose" and "free of defects". In the case of software these terms have not been implied into consumer contracts. As explained by the Australian Competition and Consumer Commission (ACCC) who are responsible for administrating the *TPA*:

> "We do look at these issues on a case by case basis but, in the hypothetical, something that functions quite well or quite appropriately, absent that malicious third party, is not, I would think, going to fall foul of the warranty provisions."[102]

The provisions on misleading and deceptive conduct, and misrepresentation in the *TPA* will be considered in the context of prosecuting botnet masters under the *TPA* in **Chapter 4**.

1.5.6 Internet Filters[103]

A national Internet filter colloquially referred to as 'Cleanfeed' has been proposed by the Australian Government.[104] The proposal would mandate Internet Service Providers ('ISPs') such as Optus, Telstra and iiNet to implement technical means to filter out a prescribed list of websites, as well as to use deep packet inspection to block websites deemed to be undesirable, using heuristic methods that remain unclear. The Government's stated intention is that Internet filtering would be used at least as a means to block web-pages providing access to child pornography and potentially other kinds of traffic such as that

---

[101] Parliamentary Report on Cybercrime, note 27 above at 8.78-8.79.
[102] Parliamentary Report on Cybercrime, note 27 above at 8.79.
[103] Maurushat, A. and Watts, R., "Australia's Internet Filtering Proposal in the International Context" (2009) 12(2) Internet Law Bulletin 18. A draft chapter on Internet filtering and deep packet inspection was written and then later excluded.
[104] Senator Stephen Conroy, *Budget provides policing for Internet safety*, media release, 13 May 2008, at <http://www.minister.dbcde.gov.au/media/media_releases/2008/033>

delivering malicious software. The proposal considers two broad types of filtering which are explained below.

Blacklist Filtering: The first tier comprises the mandatory filtration for all Australians (no possibility to opt-out) of sites on an ACMA-issued blacklist of 'child pornography' websites and 'other prohibited' materials. The scope of 'other prohibited materials' is unknown. However, a leaked ACMA blacklist suggests that 'prohibited materials' may also include such categories as fetish pornography, gambling sites and abortion information. ISPs must block such sites at the URL level. It is unknown whether accessing the websites contained on the blacklist through a circumvention device such as a proxy-server will be illegal. Operating only over the http protocols, and only on URLs, the filter will *not* block 'child pornography' and 'other prohibited content' found:

- on other pages on the same web-site
- using Peer-to-Peer (P2P) networks (for example: bit torrent, Winny)
- via Chatrooms and Instant Messaging services
- on Usenet groups

The second tier has been ambiguously defined. It appears that what is envisaged involves analysis of the data disclosed by means of deep packet inspection, inferral of content-type (by means as yet unexplained), and blockage of that traffic. It further appears that it is envisaged to apply to content that is unwanted (at least according to some people's standards), and the default of blocking it may be able to be over-ridden by subscribers.[105]

Although Internet service provider cooperation is imperative in the combat of botnets, Internet filtering is not likely to be an effective method of preventing botnet proliferation.

1.5.7 Follow the Money Trail

Following the money in the botnet context means that law enforcement tries to follow the routes the monetary transactions take until the money reaches the bot master. This could mean following the money from someone who rents a botnet back to the botnet master. It may involve tracing payments from adware and spyware companies to their affiliates (affiliate

[105] Conroy, note 104 above.

contracts are explored in **Chapter 3**). There are, of course, other reasons why somebody needs to pay a bot herder. One might pay for click-fraud, spam or, in the case of some DDoS attacks, a ransom might have been paid for stopping the attack. Other botnet masters who are engaged directly with financial fraud and credit card theft employ a variety of methods to launder money.

One common way to launder money involves the use of a money mule or more accurately, several money mules. A money mule is an individual who is hired by a criminal to transfer funds from an account to another account. In return, the money mule normally is paid a commission. In a typical money-mule transaction, a mule in one country will use a money-remitting or wire service to transfer funds from a victim's bank account to a separate account. In a typical transaction, several money mules are used in different jurisdictions to move the money through many different accounts and jurisdictions making the tracing of such funds extremely difficult.

Australian financial institutions are required by law to report suspicious money transfers. The Australian Transaction Reports and Analysis Centre (AUSTRAC) is an Australian government agency that provides financial intelligence to assist law enforcement, revenue and national security agencies within Australia. It cooperates with 35 partner agencies within Australia and has concluded agreements within 55 countries to exchange information and financial intelligence. In spite this reputation for diligently collecting intelligence on potential money-laundering schemes, the ability for law enforcement to follow the money in botnet transactions has not proven fruitful.[106] A key factor in the failure of the approach is that most cyber-criminals do not use banks to transfer money to the end destination. They use services such as Western Union, PayPal,eGold, Liberty, and eMoney as such services are either regulated in a limited fashion or are not regulated at all and, therefore, have no duties to monitor or report suspicious transactions. Such transactions are not detected by the intelligence radar of agencies such as AUSTRAC.

Successful investigations where following the money will lead to the arrest of a botnet master would likely require the aid of Interpol, along with cooperation between law enforcement in multiple jurisdictions. However, there are deficiencies in the relevant international treaties, in particular in relation to the scope of organisations covered and the preservation of evidence.

[106] Discussions with Bruce van der Graf, Detective Inspector of Fraud Squad and Head of the High Tech Crime Division, The New South Wales Police Force (one file). Similar opinions by law enforcement were stated at both the AusCERT 2008 Conference and the 2010 Australian High Tech Crime Conference in closed, Chatham House Rules sessions.

Although a complete overhaul of the *Cybercrime Treaty* and the *Anti-Money Laundering Treaty* is possible, such changes would likely take decades. Moreover, an in-depth discussion of how and whether to regulate and compel cooperation of non-financial institutions is again the subject of a separate post-graduate thesis. The approach of following the money is considered briefly in **Chapters 4 and 5** but will not be explored in depth.

1.6 TECHNOLOGIES THAT ARE NOT ESSENTIAL TO BOTNETS

The thesis will examine only the essential technologies that are used in conjunction with botnets. Technologies that are only tangentially relevant to botnets will not be considered in detail but may be defined where appropriate. The traditional computer security model is likewise not utilised but may be referenced from time to time. The conventional computer security model includes:

- a **threat** is a circumstance that could result in harm, and may be natural, accidental or intentional. A party responsible for an intentional threat is referred to as an **attacker**;
- a **threatening event** (e.g. a particular power outage or receipt of an email with an infected file attached to it) is an instance of a generic threat (power outages and email-borne viruses);
- **harm** is anything that has deleterious consequences, and includes injury to persons, damage to property, financial loss, loss of value of an asset, and loss of reputation and confidence. Harm arises because a threatening event impinges on a vulnerability;
- a **vulnerability** is a feature or weakness that gives rise to a susceptibility to a threat;
- a **safeguard** is a measure intended to avoid or reduce vulnerabilities. Safeguards may or may not be effective;
- safeguards may be subject to **countermeasures**;
- in response to countermeasures, safeguards may be adapted, or new ones instituted. An **attack-safeguards-countermeasures cycle** may arise, particularly if the rewards for a successful attacker are high.[107]

Under this model, threatening events impinge on vulnerabilities to cause harm. In the context of a botnet, botnet masters may acquire compromised computers by exploiting vulnerabilities in

[107] Clarke and Maurushat, note 5 above.

browsers and software. These same vulnerabilities allow a botnet master if they so elect to install malware onto compromised computers.

1.7 LEGAL AND TECHNICAL CURRENCY

The materials are current as of December 1, 2010 though some of the references refer to subsequent dates. While much diligence has been taken to ensure both the legal and technical currency of materials, this area of research is changing rapidly with new legal and technical initiatives being announced frequently, and with proposals being formalised. For example, it is by mid-2011, many of the proposed initiatives such as Internet service provider bot remediation programs will have commenced, new pieces of surveillance legislation will have been passed, recommendations from the Inquiry into CyberCrime will materialise into firm government recommendations, more botnet masters will be prosecuted, Australia will have ratified the *Cybercrime Convention,* and ICANN may have formalised changes to DNS resolution and policies. Analysis of current initiatives such as these is done in a manner that addresses both specific elements of the extant proposal and elements of a more generic nature that may emerge in the near future.

1.8 CONCLUDING REMARKS

On the Internet, there is consensus amongst law enforcement and security researchers that botnets are involved in most forms of cybercrime and civil wrong.[108] In the words of botnet researcher Jeremy Linden of Arbor Networks, "Almost every major crime problem on the Net can be traced to them."[109] Internet security guru Vincent Cerf[110] has equated botnets to a pandemic, warning that a quarter of all personal computers have already become bots. [111] Botnets are perceived by many experts as a pandemic yet most users are unaware of the term or the

[108] *See for example*, Rychlicki, T. "Legal Issues of Criminal Acts Committed Via Botnets." (2006) Computer and Telecommunications Law Review 12(5), p. 163.
[109] Quote taken from Berinato, S. "Attack of the Bots" Wired Magazine Issue 14.11 (November 2006).
[110] Vincent Cerf in many ways is "Father Internet". This is not surprising given that he was involved in the original ARPANET project, was Chair of ICANN, has worked at a number of internationally reputed universities, and has held key positions at IBM and Google. He is considered to be one of the most influential researchers in computer science and the internet.
[111] Presentation given at the World Economic Forum 2007. The statistics have been highlighted in a number of news reports and blog sites. See, for example, 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.

threat that botnets pose to the security of the Internet.[112] Whether or not the threat is as great as a pandemic remains to be proven. **Chapters 3 through 8** will demonstrate that botnets pose a significant problem that warrants focused attention and resource allocation to combat. Botnets are the preferred crime tool of cybercriminals. They pose a significant threat both in terms of escalating numbers of compromised computers, and the resulting damage and harm resulting from botnet related crimes. Moreover, the botnet industry has become commercialised in that professional crime kits and services are offered to those with lower computer skills, and at affordable prices. This research will explore effective approaches to combating botnets but first it begins with an exploration of early Internet regulatory theories.

[112] 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).

Chapter 2

INTERNET REGULATORY THEORY AND BOTNETS

Table of Contents

2.0 AIMS OF THE CHAPTER

This chapter examines Internet regulatory theories to address problems with applying such theories within the context of botnets. I seek to demonstrate through the use of Lawrence Lessig's model of the four modalities or constraints of regulation (code, law, market and norms), that botnets are being used to commit crime in an unprecedented an unanticipated manner which was not predicted by Internet scholars and industry players. Many of the former theories do not resonate well with what is currently seen both in terms of malware proliferation, botnets, crime, and responses to the problem.

The principal aim of the chapter is to demonstrate that botnets and the high level of cybercrime are not accounted for in any of the significant Internet regulatory theories because no one correctly predicted that the Internet could be controlled by any parties other than users, the government and commercial industry. It is difficult to reconcile botnets and cybercrime with these theories. Equally difficult to reconcile are the ways in which various stakeholders have

responded to the problem. The role, for example, of self-organized security communities is not easily situated in any Internet regulatory theory. The role of self-organized constituencies is touched on in **section 2.3.7 "Self-Help Remedies as a Constraint"** and is described in detail in **Chapter 8 "Self-Organised Security Communities".**

Lawrence Lessig's influential work in the field, in particular the ideas set forth in *Code: And Other Laws of Cyberspace*[1], has been selected as his work has penetrated a variety of disciplines outside mere legal discourse, is widely cited as authoritative, and has unquestionably had a great impact on Internet studies.[2] Lessig continues to be the dominant theorist in the field. A full description of Lessig's regulatory model is provided below, drawing on the four modalities of regulation: code, norms, law and the market. Regulatory approaches botnets to be discussed within Lessig's modalities. The proliferation of botnets as has already been introduced in **Chapter 1** with an extensive description provided in **Chapter 3**. **Chapters 3 through 8** offer a case study for which to challenge Lessig's regulatory theory.

First, Lessig describes how the Internet was "up by grabs" by either the government and/or commercial industry in the late 1980s and early 1990s.[3] The possibility of organized criminal groups controlling a large portion of the Internet was never contemplated in the 1999 version of *Code*. Lessig revisted his theory in 2006 with the publication of *Code 2.0*.[4] As will be shown in **section 2.3**. Lessig, in *Code 2.0,* discusses viruses and hackers but the discussion is limited to Lessig's overall thesis that governments will be even more compelled towards regulation through architecture and law. Second, while there have been responses to botnets which coincide squarely within Lessig's four modalities (code, market, norms and law), the activities of self-organised security communities, as will be demonstrated in **Chapter 8,** is not easily reconciled within any of these modalities. The activities of such self-organized security communities do not clearly fall into any of Lessig's modalities. To the extent that a modality must be found to match the type of activities seen, norms are the closest fit.

---

[1] Lessig, L., *Code: And Other Laws of Cyberspace* (Basic Books, 1999).
[2] It is difficult to find technology law scholarship or a course syllabus on Internet Studies that does not contain reference to Lessig's works. A basic search of legal texts on Google Scholar with the term "Lawrence Lessig" and "code" produces over 3700 articles referencing his work (December 2010). In a similar type of Google search I used the terms "Lessig" and ("course outline" OR syllabus) which returned 1400 results, all of which on the first three search pages were University documents assigning Lessig as compulsory or recommended readings materials.
[3] Lessig, note 1 above, page 219.
[4] Lessig, L. *Code 2.0* (Basic Books, 2006).

Lessig's exposition of 'norms' is, however, the least explored modality in *Code* and his works which follow. The work of Robert Ellickson will be used to further delineate the scope of norms. Ellickson has written extensively on how norms operate to achieve order without relying on the law. His work has largely focused on how order or regulation may be effective through norms amongst close-knit groups. It has been widely influential in regulatory scholarship in law and social sciences. It is my aim to demonstrate that the response by self-organized groups is ill-fitted to the notion of norms. This suggests that Lessig's model either requires an additional modality or that more exploration is needed on what norms might entail in the case where one is not dealing with a close-knit group. The work of not-for-profits and hybrid groups such as the National Cyber-Forensics Training Alliance (NCfTA) is also challenging under Lessig's theory as will be explored in this chapter as well as in **Chapters 8 and 9**.

2.1 AN OVERVIEW OF DIGITAL LIBERTARIANS AND REALISTS

Internet regulatory theories which emerged from the 1990s and into the first decade of the 21st Century may be divided into two camps: digital libertarianism and digital realism.[5] Digital libertarians argued that the law would be ineffective in cyberspace. Digital realists looked at ways to effectively regulate cyberspace. Both libertarians and realists noted the unique features of the Internet to defend their positions. They addressed the Internet's unique features such as the borderless nature of the Internet, the rise of norms in cyberspace as different from 'real world' norms, the desire not to be governed, the role of the market, and, of course, the role of architecture. Architecture in this case meaning technical standards, computer code, software, hardware and protocols. The arguments of each of these theorists were written within the same context, that of the desire of governments to regulate the Internet and the dangers that would arise out of such desire to regulate. Some of these theorists were equally concerned with commercial interest in the Internet. The Internet, as noted by Lessig, was "up for grabs".[6] The libertarians did not want the government to extend its reach. The realists, on the other hand, did not mind some government and commercial control, though they worried about the over-extension of governments and regulatory controls which encroached on rights guaranteed in the United States Constitution, especially free speech. Everyone, however, missed the fact that these

[5] James Boyle coined the phrase "digital libertarian" in his seminal piece, Boyle, J., "Fourcault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors" (1997) available at http://www.law.duke.edu/boylesite/foucault.htm (last accessed February 15, 2011). Graham Greenleaf coined the phrases "digital realist" in his work Greenleaf, G., "An Endnote on Regulating Cyberspace: Architecture vs. Law" (1998) 21(2) University of New South Wales Law Journal 52.
[6] Lessig, note 1 above at 219

same unique features of the Internet not only made it vulnerable to control by the government and commercial parties, but to that of organized crime.

Another concern, as voiced by Greenleaf, was the U.S. centric approach to Internet regulatory theories with the emphasis squarely placed on First Amendment analysis.[7] Most of the theories at the time came from and continue to come from U.S. scholars, therefore, they were understandably predisposed to concerns indicative of their culture. Principally, this meant any regulatory restrictions which might impede of the First Amendment rights of free speech. Privacy and other concerns external to the U.S. Constitution played a secondary role in early U.S. Internet scholarship.[8]

Tension between libertarians and realists is still seen in present day debate about Internet regulation. For example, many have argued against mandatory Internet filtering based on the principle that they do not want the government performing any censorship function. The group Anonymous launched a denial of service attack on the Australian Parliamentary website bombarding the site with images of breasts and penises as a form of protest to the government's proposal to introduce a mandatory filter.[9] The realists, while not against content regulation or appropriate censorship, have generally argued that Internet filtering will not be an effective means of blocking illegal materials.[10] And still others have concerned themselves with who will implement the filtering, looking at approaches which amalgamate the Australian Communications and Media Authority (ACMA) with the Classification Board, and other approaches which seek to leave the government out of filtering trusting Internet Service Providers (ISPs) to better implement such filters.[11] The debate between libertarians and realists will continue for as long as people mistrust government, have trepidation of censorship, and value freedom of expression.

---

[7] Greenleaf, note 5 above.

[8] Kathy Bowrey's work examines the lack of cultural considerations in both the law and Internet scholarship. Her work addresses the intersection between law and the diversity of culture and Internet communities on the Internet. She is mindful of the U.S. centric approach to most Internet scholarship, pointing out deficits in the literature from a cultural perspective. Bowrey, K., *Law & Internet Cultures* (Cambridge University Press, 2005).

[9] A video released on youtube by the group Anonymous outlines their concern of governments censoring the Internet which they declare must remain free. See "Anonymous to Australia" available at http://www.youtube.com/watch?v=eEc80U46hIQ (last accessed January 13, 2011).

[10] Maurushat, A. and Watts, R. "Australia's Internet Filtering Proposal in the International Context" (2009) 12 Internet Law Bulletin 2.

[11] Chatham House Rules. Internet Filtering and Censorship Proposal Forum" (Nov. 2008) Cyberspace law and Policy Centre, the University of New South Wales, Sydney, Australia. Members of the ACMA and Classification Board were present along with key industry members from ISPs and major technology companies such as IBM.

2.2 DIGITAL LIBERTARIANISM: JOHN PERRY BARLOW and DAVID JOHNSON AND DAVID POST

Digital libertarians are concerned with government regulation of the Internet. In particular, governmental interference with free speech is wholly undesirable in the views of libertarians. The libertarian view does not see the government as having a role to play with the Internet as sovereignty will be maintained by the users. This sentiment is aptly explained by one of the Internet's chief libertarians, John Perry Barlow in his "Declaration of the Independence of Cyberspace":

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[12]

Libertarians, such as Barlow, view the law as destined for failure in cyberspace. They emphasize self-regulation and social norms. In many ways, Barlow's view epitomizes those of libertarians.

Barlow advocates for a cyberspace where social devices emerge from the community's internal conditions and norms rather than from external sources such as a national government.[13] Barlow co-founded the Electronic Frontier Foundation which is "dedicated to protecting its interests and those of other virtual communities like from raids by physical government"[14] Barlow sees cyberspace as something similar to the wild west where traditional legal approaches to maintaining order were not initially present. One gets the feeling from Barlow's writing that he views this lack of government interference as a utopia. As Barlow writes:

> "The First Wave was agriculturally based and required law to order ownership of the principal source of production, land. In the Second Wave, manufacturing became the economic mainspring, and the structure of modern law grew around the centralized institutions that needed protection for their reserves of capital, labor, and hardware. …
>
> The Third Wave is likely to bring a fundamental shift in the purposes and methods of law which will affect far more than simply those statutes which govern intellectual property.
>
> The "terrain" itself - the architecture of the Net - may come to serve many of the purposes which could only be maintained in the past by legal imposition. For example, it may be unnecessary to constitutionally

[12] Barlow, J.P., "A Declaration of Independence in Cyberspace" Humanist 1996 available at http://editions-hache.com/essais/pdf/barlow1.pdf
[13] Barlow, J.P., "The Economy of Ideas" (March 2994) Wired Issue 2.03 available at http://www.wired.com/wired/archive/2.03/economy.ideas.html (last accessed November 10, 2010).
[14] 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).

> assure freedom of expression in an environment which, in the words of my fellow EFF co-founder John Gilmore, "treats censorship as a malfunction" and reroutes proscribed ideas around it."[15]

This above passage echoes a common theme in early Internet scholarship – the importance of architecture as a shield to regulation. Barlow clearly saw the decentralized nature of the Internet's architecture coupled by a new community of social norms as playing a pivotal role in successfully keeping physical government and its laws at bay. He did not allow for the possibility of governments regulating architecture as put forth most vividly in Lessig's work. Certainly the structure of the Internet as a utopia for the proliferation of malicious and criminal activity was very much unforeseen. This is not to say that Barlow altogether ignores the possibility of cybercrime. Indeed, he discusses hackers, crackers, phreakers and cybercrime in his work, "Crime and Puzzlement."[16] Typical of all Internet scholars writing in the earlier day is the depiction of a hacker as a welcome member of cyberspace. Hackers[17], crackers and phreakers are portrayed in Barlow's world as trying to keep information free, exposing flaws in systems, and satiating the heightened curiosity of those inclined to defeat problems and overcome challenges. They are rebels.[18] The original hackers focused on hacking for fun, progressed to phreaking and then to virus writing. The term hacking as of more recently does not evoke a positive image. Hacking has come to be understood – certainly in the media and by the layman

---

[15] Barlow, note 13 above.

[16] 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).

[17] Differentiation was made between a hacker, cracker and phreaker. Hackers were those who hacked by ethical means. Crackers, on the other hand, break into computer systems for a manevolent purpose such as theft. Phreakers were those who break into phone systems. There are a number of excellent lexicon articles on hacking in general. It should be highlighted that there is not a general consensus of these terms. As Loraine Lawson of TechRepublic aptly states:

> "The National Security Agency (NSA) defines hacking simply as the "unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network."
>
> By comparison, Hackers.com, an underground domain whose stated purpose is to "provide a place for hackers, phone phreaks, and other underground-related people to interact and expand their minds," offers a somewhat more poetic and gracious definition of hacking:
>
> "Hacking is the act of penetrating a closed computer system for the knowledge and information that is contained within. Through the study of technology and computers, a hacker can open his mind and expand his knowledge. Hacking is intended to free information and expand minds, not to be destructive nor for material gain. There is always some debate because of how the term 'hacker' has been both glorified and undermined by common media, but most will say that those who destroy data, hack for money, or hack with illegal intent should be referred to as 'crackers,' not hackers."

See 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).

[18] Steven Levy, for example, portrays the cryptography hackers as rebels. See in Levy, S. *Hackers: Heroes of the Computer Revolution* (New York: Doubleday, 1984).

– as an activity performed by computer savvy people for profit as a criminal activity.[19] It is understandable that Barlow and the other theorists did not view hackers as criminals in need of reprimand by the law but, rather, viewed them as part of the changing landscape of the new frontier, cyberspace.[20] The rise of criminal activity, organized crime, and the extent of monetary loss on the Internet was simply not envisaged at the time.

Johnson and Post advanced a theory of what they refer to as "Net Federalism"[21] and "the law of the net".[22] They argue that traditional law making on the Internet will be ineffective due the absence of territorial borders in cyberspace. Law making and enforcement of such laws relies on geographical limitations or territories. With the absence of such geographical boundaries, the law cannot, in their view, provide meaningful control over conduct. Under their theory, if governments choose to enact laws, there will be a real danger for Internet users being simultaneously subject to the laws of all territorial sovereigns. Post and Johnson point out that in order for traditional laws to be effective, an agreed upon international framework would need to be established. Post and Johnson note that comity is an unrealistic goal on the Internet as many values are neither shared nor reconcilable between diverging cultural norms. Post and Johnson's Internet governance model is one based on multiple rule sets which develop from within Internet communities. Such rules are de facto in nature, self-replicating, contain multiple sets of rules, and involve a complex interplay between such rules. This self-regulatory rule-making model is carried out predominantly in two different though interactive forms, architecture / code and social norms. Online citizens range from users to computer engineers to systems administrators to network systems to governance units. These groups, in the opinion of Post and Johnson, have the potential to be the most effective and legitimate form of the regulation of cyberspace. They argue that the architecture of the Internet facilitates consensual governance amongst those who develop its protocols and standards, and then take this argument one step further to advocate that, depending on the problem in question, the cyber-community with the most legitimate claim of self-governance should be the one whose voice is heard the

---

[19] *See for example* media studies of cybercrime and Internet technologies. 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), page s582-603; and 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.

[20] Other Internet writers such as Mike Godwin question whether a hacker can be charged with theft given that, in his view, it is questionable whether information is subject to ownership. This type of rhetoric clearly did not foresee billions of dollars stolen from credit cards and bank accounts through the work of hackers for financial gain, nor perhaps was it foreseeable how easy and desirable the Internet would be for identity theft. See 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) at 126.

[21] Post and Johnson, "Law & Borders – The Rise of Law in Cyberspace" (1995) 48 Stanford Law Review at 13

[22] Post and Johnson, note 21 above, page 17.

loudest. They do not, however, provide specific examples of which cyber-communities or network administrators would have the most legitimate claim to self-governance. This exposes a flaw in their model. They argue that comity is not possible in cyber-space due to the impossibility of shared values between nations. They wrongly assume, however, that the shared values problem magically disappears and that consensus is somehow possible in Net-based law-making institutions.

Post and Johnson used their "Net Federalism" model to address how fraud and antitrust may be addressed in cyberspace. This is expressed in the below passage:

> "Can Minnesota prohibit the establishment of a Ponzi scheme on a Web page physically based in the Cayman Islands but accessed by Minnesota citizens through the Net? … The state lacks enforcement power, cannot show specially targeted effects, and does not speak for the community with the most legitimate claim of self-governance. But that does not mean that fraud might not be made 'illegal' in at least large areas of cyberspace. Those who establish and use online systems have an interest in preserving the safety of their electronic territory and preventing crime. They are more likely to be able for enforce their own rules. And, …, insofar as a consensual based "law of the Net" needs to obtain respect and deference from local sovereigns, new Net-based law-making institutions have an incentive to avoid fostering activities that threaten the vital interests of territorial governments."[23]

Understandably Post and Johnson were unable to predict that law's impotence would not stem predominantly from territorial and jurisdictional issues but from the obfuscation techniques used to commit many forms of fraud will be examined in **Chapter 3.** Web pages may not be static. They can be dynamically hosted whereby the content rotates its location. This IP address rotation may take place every 10 minutes, every couple of days or every few weeks. The use of encryption, fast-flux rotating mechanisms, and distributed networks such as peer-to-peer, make trace-back of the source of fraud in many cases difficult to impossible. As such, prosecution is no longer the chief desired goal. Prosecution may still occur in the occasional case but security policy is increasingly focused on methods of prevention, detection, and disruption. While it may be true that "Net-based law-making institutions have an incentive to avoid fostering activities that threaten the vital interests of territorial governments", their success in doing so in the area of crimes committed with botnets has been somewhat abysmal. The prolific spread of and the damages caused by botnets, as will be seen in **Chapter 3,** are beyond arguments of whether local sovereigns should have a voice, effective or ineffective, in the arena. To be fair to Post and Johnson, their model did foresee that Net-based law-making institutions would have incentive to prevent crimes and other types of undesirable Internet activity. According to Post and Johnson this incentive would arise out of the desire to keep territorial sovereigns at bay, and not

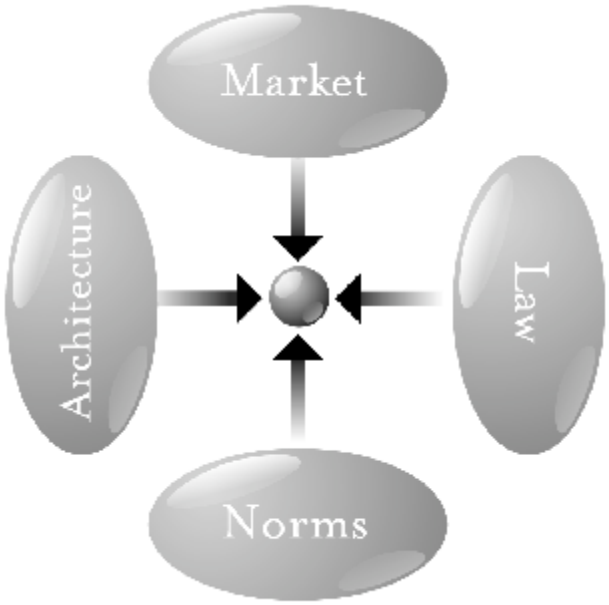
[23] Post and Johnson, note 21 above, page 1383.

necessarily to keep the Internet safe and functioning. As will be seen in **Chapter 7** many of the self-regulated groups associated with 'Net Federalism", such as ICANN, will play a role in active prevention and disruptions of botnets.

2.3 DIGITAL REALISM: LAWRENCE LESSIG'S FOUR MODALITIES

One of the most comprehensive theoretical models of cyberspace was advanced by Lawrence Lessig. While Lessig's model has evolved from a number of articles and books[24], his theory while perhaps most well-known in the essay, "The Law of the Horse: What Cyberlaw Might Teach" is broadened and better articulated in his book, *Code.*[25] Lessig's essential thesis is that online behaviour is constrained by four modalities: law, norms, the market and architecture (which he refers to as 'code'). Lessig's modalities are replicated below in **Figure 2(A)**.

Figure 2(A) Regulation as the Function of Four Modalities[26]



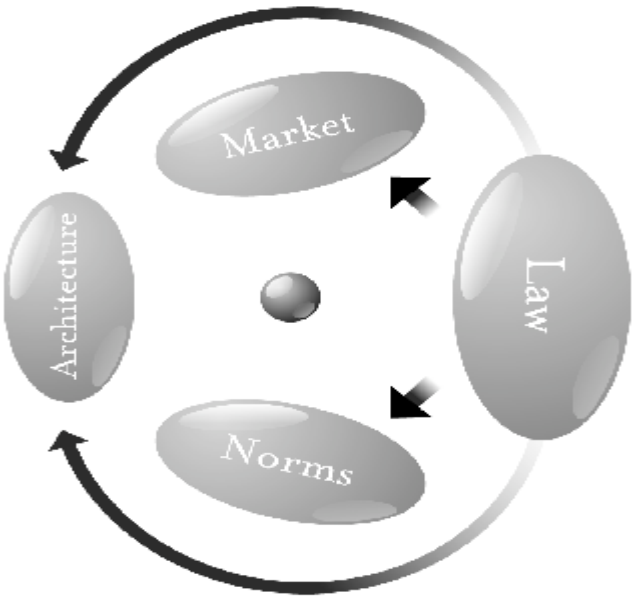
[24] Particularly, *see* Lessig, L., " The Law Of The Horse: What Cyberlaw Might Teach" (1999) 113 Harvard Law Review 2. *See also* Lessig, L., "Constitution and Code"'(1996-7) 27 Cumberland Law Review 1; Lessig, L., "Intellectual Property and Code"(1996) 11 St John's Journal of Legal Commentary 3; Lessig, 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. Other papers and books of Lawrence Lessig may be found at www.lessig.org.

[25] Lessig, note 1 above.

[26] The image is available under a creative commons license in Lessig's book *Code.* *See* note 1 above. The image was copied from https://www.socialtext.net/codev2/index.cgi?what_things_regulate (last accessed February 12, 2009).

Lessig's work focuses on how these four modalities influence the subject of regulation – the "pathetic dot" in the centre. Additionally he explores how each of the modalities may affect the other modalities as represented in **Figure 2(B)** on the following page.

Figure 2(B) Modalities Influencing Other Modalities[27]



Lessig debunks the ideas proposed by the libertarians that the law does not and should not shape online behavior, and he dispels the central line of thought of many scholars from the University of Chicago who emphasized the law's limits in comparison with the effectiveness of norms and the market.[28] Lessig's approach has been described as having an "anti-law" starting point[29] which is contrasted throughout his work with the law's ability to both indirectly and directly influence and shape the other modalities: norms, the market, and architecture. These four modalities will be explained in **sections 2.4.2 to 2.4.6.** Each modality will be explained borrowing Lessig's online examples, followed by an analysis of how the modality operates in the

[27] *See* note 1 above.
[28] The work of Ronald Coase and Richard Posner features prominently in the University of Chicago scholarship. Ronald Coase's work on law and economics in his book *The Problem of Social Cost* forms what has become known as the Coase Theorem. A complete list of Ronald Coase's work may be found at http://www.coase.org/coasepublications.htm (last accessed July 29, 2009). Richard Posner is another famous scholar contributing to the University of Chicago law and economics scholarship. A comprehensive list of Posner's publications may be found at http://www.law.uchicago.edu/node/79/publications (last accessed July 29, 2009). Lessig addresses the Chicago line of thought in the section, "Cyber-places Harvard Versus Chicago". *See* Lessig, note 1 above, page 25–29.
[29] Greenleaf, note 5 above.

context of response to botnets. I will adopt a similar approach to Lessig, explaining how each of these modalities might bear on an individual's behaviour. To do this, I will use the prototype of an individual botnet master. This approach to the analysis will highlight the limits of Lessig's model with what is taking place online with botnets. It will be shown that law, norms, market and architecture as they are presently applied pose few effective constraints on the botnet master's online behaviour. The biggest impact on botnets has largely stemmed from self-organised security communities, not-for-profit security corporations, and hybrid working groups cooperating with one another to combat botnets as will be examined in **Chapter 8**, **"Self-Organised Security Communities".** The role and influence that self-organized security groups have on botnets acts like a constraint, a constraint that is not easily positioned within any of Lessig's modalities. This notion will be explored in section **2.4.7 "Self-Organized Communities as a Constraint"**. First, **section 2.4.1** provides a pivotal point which Lessig and other scholars did not consider – that criminal groups would be such a large factor in the battle for control of the Internet – a battle which they had only considered government, corporations and users.

2.4.1 Control of the Internet

Lessig commences *Code* with an analogy of the displacement of forms of control at the collapse of Communism in Eastern Europe with the displacement of control on the Internet. Lessig describes the type of advice dispensed by many Americans to Central and Eastern European society in the late 1980s and early 1990s. He writes:

> "Just let the market reign and keep the government out of the way, and freedom and prosperity would inevitably grow. Things would take care of themselves. There was no need, and could be no place, for extensive regulation by the state.
>
> But things didn't take care of themselves. Markets didn't flourish. Governments were crippled, and crippled governments are no elixir of freedom. ***Power didn't appear – it simply shifted from state to Mafiosi, themselves often created by the state…. Private interests didn't emerge to fill the need. Instead, needs were unmet. Security evaporated.*** A modern if plodding anarchy replaced the bland communism of the previous three generations: neon lights flashed advertisements for Nike; pensioners were swindled out of their life savings by fraudulent stock deals; bankers were murdered in broad daylight on Moscow streets. One system of control had been replaced by another, but neither system was what Western libertarians would call free."[30] [emphasis mine]

[30] Lessig, note 1, page 3-4.

Lessig describes how digital libertarians shared equally flawed optimism for cyberspace as a new frontier of the libertarian utopia. The libertarian's claim was that government could not regulate behaviour in cyberspace. The rest of Lessig's book describes in detail how regulation will take place in cyberspace, through the constraints on behaviour which arise from four modalities: law, norms, the market, and architecture. He warns of the dangers of assuming the Internet's architecture is static; the Internet, as Lessig writes, suffers from "is-isms".[31] He further advances the argument that architecture, and regulation of architecture will be the most important modalities in *how* the Internet in controlled.[32] The remainder of Lessig's arguments on how the Internet will be controlled is focused on *who* is able to assert control of the architecture. Lessig points out that the Internet "is up for grabs and that, depending on who grabs it, there are several different ways it could turn out."[33] However, Lessig only foresees the possibility of government, commerce and, to a lesser extent, users grabbing control of the architecture of the Internet. Nowhere does he allow for the possibility of organized criminal groups taking power and control of the Internet from government and market forces, much the same that occurred with the demise of the former Soviet Union. This is perhaps best highlighted in a small section of the book devoted to "worms that sniff".[34]

In the section, "Worms that Sniff", Lessig describes the use of computer worms used by the FBI or other government agents to collect data about an investigation. In the case described by Lessig, the worm is used to locate National Security Agency documents that have ended up in unauthorized hands. Lessig warns of the ability of the government to "to collect data about us in a highly efficient manner." Lessig's focus when examining the dangers caused by a technology such as a worm is contextualized in a traditional American way, the danger of the government encroaching on free speech and privacy of the citizen. This is a repeated theme not only in Lessig's work but of most early Internet scholars including, as we have already seen with Barlow, and Post & Johnson. Advice is dispensed on how to effectively regulate the Internet through non-legal means, and warnings are given as to the dangers of regulating in ways which impact on liberties. Lessig develops detailed arguments concerning the Constitutionality of the United States government using worms for law enforcement activities. Nowhere in their writings do

[31] Above, page 24.
[32] Lessig, note 4 above. In *Code 2.0* Lessig only revisits the modalities of Code and Law. Chapter 4 discusses "Architectures of Control" and Chapter 5 discusses "Regulating Code."
[33] Above, page 219.
[34] Above, pages 17–18. Later Lessig references worms in **Chapters 11 and 12** which examine privacy and free speech.

Lessig, Post and Johnson, Barlow[35], Reindenberg[36] or Boyle foreshadow a commercial cybercrime industry that would use worms, especially those distributed in conjunction with botnets, to undermine national security, to threaten critical infrastructure of a nation's banking system and stock market, to appropriate identities later used in the commission of crimes, to collect, sell and steal personal information for illicit use, to perpetrate corporate espionage, and to defraud millions of people out of billions of dollars. In much the same way as Eastern European nations were encouraged to disengage from regulation, and let the market "take care of itself", we find ourselves at an equally discouraging junction in safeguarding the Internet from high levels of criminal activity. To parallel Lessig's statement on emerging communist nations shifting the power from "state to Mafioso" makes the present Internet situation a seemingly obvious inevitability.

Lessig revisits *Code* later in his work, *Code 2.0* where he briefly references computer viruses. He writes:

> "When I first wrote the book, two ideas seemed to dominate debate about the Net: first, that the government could never regulate the Net, and second, that this was a good thing. Today, attitudes are different. There is still the commonplace that government can't regulate, but in a world drowning in spam, computer viruses, identity theft, copyright "piracy," and the sexual exploitation of children, the resolve against regulation has weakened."[37]

This is the only articulation in the revised book that cybercrime would have an impact on the Internet. The impact, according to Lessig, would be that architecture would continue to play a vital role, and that there would be a dramatic increase in the regulation of architecture and the Internet in general. He goes so far as to predict in Code that, "Left to itself, cyberspace will become a perfect tool of control"[38] and then in Code 2.0 that, "Cyberspace will be the most regulable space humans have ever known."[39]

Other scholars have applied Lessig's theory to cybercrime. Katyal draws on Lessig's notion of architecture as a crime prevention tool, drawing on examples of how physical architecture in the past has been used to prevent crime.[40] Wall reinforces Lessig's and Katyal's views on the role of

---

[35] Boyle, note 5 above.
[36] *See* Reidenberg, J., "Lex Informatica: The Formulation of Information Policy Rules Through Technology" (1998) Texas Law Review 76(3).
[37] Lessig, note 4 above, page 27.
[38] Lessig, note 1 above, page 6/
[39] Lessig, note 4 above, page 32.
[40] Katyal, N. "Criminal Law in Cyberspace" (2001) 149 University of Pennsylvania Law Review 1003.

architecture in the prevention of cybercrime.[41] Wall, however, is cautious of a purely architectural approach to cybercrime prevention noting that there is a strong case to ensure that traditional law enforcement mechanisms and government accountability are still present. Uchimur reinforces Lessig's theory that architecture and the regulation of architecture will prevail as the most effective method of countering cybercrime.[42] Hofmann describes the spread of cybercrime on the Internet as an "unintended consequence" where, "the Internet began as an object of libertarian dreams of social autonomy and creativity; but became subject to growing state control and surveillance, ultimately restricting individual privacy and social liberty to a much higher degree than any other democratic communication media."[43] Each of these scholars understood that architecture would be an essential regulatory constraint to combat cybercrime. They also understood, to a varying extents, that not only did the liberal features of the Internet make it vulnerable to use by the government and commercial parties, but also to that of organized crime. However, these scholars all continue to miss the critical point that cybercriminals are not merely aided by the features and technologies of the Internet, cybercriminals control a substantial part of the Internet's architecture through botnets.[44] Botnets as part of the architecture are explored in **section 2.3.4** and in **Chapter 3**.

The technical community identified botnets as a significant threat long before they came to the attention of law and criminologists. Evron and similar security activists identified botnets as a significant emerging problem as early as 1996.[45] Vince Cerf, one of the Internet's founders, described the botnet threat as a pandemic where by the year 2012 a quarter of the world's computers would be connected to a botnet.[46] Anderson described botnets as an "online criminal revolution" where he compares the building of botnets and the rapid inventions leading up to the industrial revolution.[47]

---

[41] Wall, D. *Cybercrime* (Polity Press, 2007), pages 186-207.
[42] Uchimur, K., "Third Party 'Responabilities' Through Telecoms Policy" in Grabosky, P. And Broadhurst, R., (eds) *Cyber-Crime: The Challenge in Asia* (Hong Kong University Press, 2005).
[43] Hofmann, J., "The Liberarian Origins of Cybercrime: Unintended Side-Effect of a Political Uptopia" Economic & Social Research Council Discussion paper 62 (2010).
[44] One exception may be Jonathon Zittrain. Zittrain has spoken on panel debates with security experts who clearly articulate that the Internet is being run by cybercriminals, *See* Cerf, note 46 belove. Zittrain, however, has not directly articulated this view of the Internet being controlled by cybercrime. *See for example*, Zittrain, J., "The Generative Internet" (2006) 119 Harvard Law Review 1974.
[45] Evron, G., *Alternative Botnet C&Cs* (Syngress, 2007), page 80.
[46] Cerf, V., "Who Will Run the Internet" (2007) World Economic Forum available at http://www.weforum.org/s?s=cerf (last accessed Nov. 14, 2010).
[47] Anderson, R., Blayton, B., and Moore, T, *Security Economics and the Internal Market* (2008) Report to the European Network and Information Security Agency (ENISA) available at http://www.enisa.europa.

In spite of the identification of botnets and cybercrime as a significant problem in the technical and legal literature, Internet regulatory theories have not changed. Lessig's popular chorus echoes through the fields – architecture is a formidable regulatory modality, there will be regulation of architecture, that architecture will be the most important modality in combating cybercrime, and that the Internet will become highly regulated. While the assertions from Lessig are indeed wholly applicable to cybercrime, his theoretical model does not adequately accommodate countermeasures to botnet.

Barlow, Post and Johnsons' works suggest that self-regulatory institutions and norms will develop to solve problems in cyberspace. Lessig instructs us to use indirect and direct regulation, coupled with changes to architecture to achieve effective regulation. So far, these theories are falling short in the case of botnets and cybercrime. The possibilities are abundant as to why the cybercrime industry has been allowed to flourish to the extent that it has: lack of regulation, ineffective regulation focused on an insignificant modality (eg. law prioritized over architecture), the use of national regulatory structures when an international framework is required, architecture that permits illicit use, and so forth. The following sections analyse each of Lessig's modalities to probe potential ambiguities or shortfalls in the model. **Sections 2.4.2 through to 2.4.6** examine Lessig's four modalities from the perspective of the regulation of the botnet master.

2.3.2 The Market

Lessig refers to the market principally around the notion of price. Property is bought and sold according to an established price. The price acts as a constraint. The market, as Lessig notes, does not exist in a vacuum but is supplemented by an elaborate set of laws and norms derived from contractual and property rules.[48] The market is as important in cyberspace as it is in real space. Lessig uses the example of the price and quality of a package of cigarettes as a factor in an individual's ability to smoke.[49] He uses examples such as flat rate versus hourly priced Internet subscription services, and advertising services use of popular online sites to demonstrate how the market constrains in cyberspace. Of course, markets do not constrain in isolation but operate against the backdrop of an elaborate system of laws and norms. As Lessig describes, "laws and

---

Eu/act/sr/reports/econ-sec/economics-sec/?searchterm=Security_Economics_and_European_Policy (last accessed November 14, 2010).

[48] Lessig, note 1 above, page 236.

[49] Above, page 87.

norms defin[e] what is buyable and sellable, as well as rules of property, and contract for how things may be bought and sold."[50] The market, as seen below, does not provide a significant constraint to the botnet master.

The market does not offer a deterrent. The cost of writing and programming malware to be used for financial gain is minimal. The price, for example, to register a domain name for a year is approximately $10 while the most dynamic domain name services (Dynamic DNS) are offered for as little as $15 per year.[51] As will be discussed in **Chapter 3**, dynamic DNS is where a domain name points to an IP address that is continually rotating through a string of IP addresses. In other words, your IP address changes every time you log onto the Internet. This allows in some instances the ability to link to content hosted on innocent third party websites, normally done via a security exploit. For example, child pornography can be illegally uploaded and stored on a third party website. The ACMA Internet filter blacklist contained a webpage belonging to a dental surgeon in Queensland whose website was being used to host and store child pornography unbeknownst to the owner of the site.[52] The dentist's website was blocked by all Australian ISPs. It is possible that dynamic DNS was utilized in conjunction with a security exploit to place the materials on the dentist's website.

2.3.3 Law: Indirect and Direct Regulation

Laws are "a command backed up by the threat of a sanction."[53] While Lessig paints a landscape of how laws express the values of the community, as well as to establish rights and regulate structures, he notes that law's primary function is one of threat of punishment.[54] Regulation, according to Lessig, is either direct or indirect. Typically, the law regulates directly in the form of a rule and threat of ex post sanction where "Legislatures enact; prosecutors threaten; courts convict".[55] When regulation is indirect, however, "it aims at modifying one of the other structures of constraint"[56] Indirect regulation could be aimed at altering norms, market or architecture.

---

[50] Above, page 236.
[51] *See for example* DynDNS.com where you can pay $1.99 USD per month or $15 USD per year available at http://www.dyndns.com (last accessed March 3, 2011).
[52] Maurushat and Watts, note 10 above.
[53] Lessig, note 1, page 235.
[54] Above.
[55] Above, page 89.
[56] Above, page 95.

Lessig's description of the law is not to assess whether or not regulation is or will be effective at achieving its goal. Rather, his aim is to indicate that indeed law does have a role to play in cyberspace, through both direct and indirect regulation. As commentators on Lessig's work have noted, "law in cyberspace will often be more effective if it regulates code/architecture rather than trying to directly regulate individual behavior."[57] This is due to the nature of architecture which Lessig describes as being invisible and self-executing. [58] **Chapter 7** advocates for regulation of architecture and markets by addressing "connectivity enablers". By "enablers" I am referring to intermediaries that have the ability to exercise control over the technologies that they are responsible for but which, for liability and business reasons, elect not to. Such entities would include ISPs, DNS Registries and similar organizations. Lessig's work does not address the effectiveness of the law. The majority of Lessig's treatment of law is a warning about how certain types of regulation allow for governments and the market to invisibly control the Internet with little to no transparency. Lessig worries about invisible regulation's impact on privacy, freedom of expression and sovereignty.[59] Lessig uses the example of governmental searching surveillance technologies such as a worm or packet sniffer.[60] He argues that the questions raised are not unlike those raised in the era of wiretapping in the 1920s by Louis Brandeis and William Howard Taft.[61] The Constitutionality of such technologies is raised in the context of, once again, free speech and privacy.

How the law constrains in the context of the botnet master is analysed below. Lessig does not offer an evaluation of the effectiveness of the law. I will evaluate the law's effectiveness of combating botnets in **Chapters 4, 5 and 6**.

The law, whether through indirect regulation as seen with data breach notification schemes in **Chapter 1** or through direct regulation such as criminal provisions sanctioning unauthorized access to computers as will be seen in **Chapter 4**, does not provide a deterrent to the botnet master. There is no evidence to suggest, for example, that data breach notification schemes reduce security breaches and the harm that results from the breach.[62]

---

[57] *See generally* Greenleaf, note 5 above.
[58] Lessig, note 1 above, page 236.
[59] Lessig, note 1 above. Chapters 11, 12 and 14 respectively.
[60] Lessig, note 1 above, page 144.
[61] Warren, S. and Brandeis, L., "The Right to Privacy" (1890) 4 Harvard Law Review 193. The sunlight reference is documented at http://www.brandeis.edu/investigate/sunlight (accessed January 30, 2009).
[62] *See* Maurushat, A., "Data Breach Notification Law Across the World from California to Australia" Privacy Law and Business International (February 2009)*;* Romanosky, S., Telang, R., and Acquisti, A. "Do Data Breach

Obfuscation techniques such as encrypted proxy servers, dynamic DNS and botnets, discussed in **Chapters 3 and 6**, make traceback of criminal action and the collection of evidence extremely difficult. The difficulties of prosecution are exacerbated by many botnet masters heralding from "cybercrime friendly" jurisdictions in Eastern Europe where prosecutions are rare, and if done, usually targeted at those programmers at the lower end of the commercial spectrum. The lack of prosecutions in many nations is due to lack of law enforcement resources and these resources are operating under duress. For example, organized crime units may be linked to corrupt government members and police. In jurisdictions better resourced, evasion of law enforcement is still achieved with minimal effort. This is largely due to obfuscation techniques which present significant prosecutorial hurdles in gathering digital evidence, location of victims, and levels of harm or damage suffered. When botnet masters are prosecuted, sentences are mild, if any sentence is issued at all as in the case of New Zealand botnet herder Akill as will be discussed in **Chapters 3 and 4**. **Chapter 3** will highlight that most computer hackers, in particular those with high skill levels, are not deterred by the possibility of prosecution. Prosecution and civil liability obstacles are further addressed in **Chapter 6**.

2.3.4 Architecture

Lessig refers to architecture in two senses. The first sense refers to physical architecture known as the "built environment" where "the way the world is, or the way specific aspects of it are."[63] Fences provide a more effective means of preventing neighbouring pets from causing mischief on one's property than a by-law prohibiting animals from accessing third party properties. Architectural constraints are everywhere. So much so that we operate on a day-to-day basis without taking notice of our built environment. Architectural constraints are equally present in cyberspace, and equally unnoticeable. Lessig uses architecture in a more specific sense when referencing the Internet. The architecture of the Internet, in his words, is comprised of computer code. For example, passwords act as a barrier to unauthorized access of data. It is not sure if Lessig intends a broad meaning to include software, hardware, protocols and Internet standards.[64] I assume a more inclusive definition of architecture, extending beyond mere

---

Disclosure Laws Reduce Identity Theft? Seventh Workshop on the Economics of Information Security, June, 2008; Ponemon Institute, 2009 Annual Study: U.S. Enterprise Encryption Trends available at http://www.encryptionreports.com/2009etrends.html (last accessed November 10, 2009); 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); Matswshyn, A.(ed) *Harboring Data: Information Security, Law, and the Corporation* (Stanford University Press, 2009); and Winn, J. "Are 'Better' Security Breach Notification Laws Possible?" (2009) Berkeley Technology Law Journal Volume 24:3.

[63] Lessig, note 1 above, page 236.

[64] See Greenleaf, note 5 above.

computer software. Architecture is the core modality in Lessig's model as its core attributes, as discussed below, are different from the other constraints.

First, architecture is an immediate constraint that does not require an individual's judgment. A law forbidding unauthorized individuals from accessing content may offer a deterrent but an individual can still choose to access content. If a password system is implemented, there is an architectural barrier that is an immediate constraint. The judgment of an individual is not required in order to restrain the individual.

Second, as Lessig suggests, architecture has high plasticity.[65] That is to say that the architectonics of the many standards, protocols, and technical features of the Internet may be easily changed. Changing an architectural component of the Internet is easier and often more efficient than changing the market, norms or laws. This goes back to the concept of immediacy. An architectural change constrains immediately whereas changing an individual's behaviour through law, norms and market is a more long-term proposition.

Lessig emphasizes architecture over the other modalities due to the uncertainty of its governance. We know, for example, that law is the mandate of legislatures, law enforcement agents and the courts. We know that norms are shaped through popular actions and moral sanctions within closely-knit groups of people. We know that the market is a combination of price, and supply and demand. But the architecture of the Internet is governed in a new manner. Code-writers become the new sovereign of this space according to Lessig. Control of the Internet, however, is highly fragmented and at the time of Lessig's writing, "still up for grabs". Lessig contemplates who will grab control of the space: government, commerce or users. Again, there is no consideration of how the architecture of the Internet allows for organized criminal groups to stake a major claim. This is explored below.

The architecture of software, hardware, the Domain Name System, and protocols impose some constraints on the botnet master, most of which as will be seen in **Chapter 3** are easily circumvented. For example, anti-virus software is increasingly considered by many to be an ineffective approach to blocking malware as it is dependent on users updating their systems on a daily basis, while the most threatening malware programs often go undetected by virtually all

[65] Lessig, note 24 above, page 511.

anti-virus and anti-spyware programs for enough time as to cause significant damage.[66] Software and hardware are insecure with little incentive for producers to deliver secure software.[67] Presently, software producers are not liable for product flaws. **Chapters 3 and 7** provide an analysis of the architecture features of the domain name system which enables obfuscation techniques such as fast-flux botnets to thrive. This is not to say that the architecture cannot be changed to act as a constraint but that, currently, this is not the case. Changing the architecture to discourage botnets is explored in **Chapter 7**.

Equally important, criminals have leveraged features of the Internet to build their own infrastructure. To return to a gun analogy, the Colt 45 was part of the architecture of the wild west for both sheriffs and outlaws. Compromised computers existed pre-botnet; we merely called them infected computers. Bots too are merely malicious software (malware). It is the combination of compromised computers who respond to a C&C source(s) by receiving instructions through bots that renders the botnet a unique Internet infrastructure. As seen in **Chapter 1**, in 2009 there were approximately 19 million compromised computers with estimates placing 25% of all of the world's computers to be connected to a botnet by 2012 (there are no current botnet statistics for numbers of compromised computers worldwide).[68] In this sense, the botnet has become part of the Internet's architecture and that architecture is controlled by criminal groups.

2.3.5 Norms

Norms, from Lessig's perspective, involve the governance of social behaviour where a community imposes sanctions on one another when a norm is broken.[69] In the legal realm, the State imposes penalties often in the form of a fine or prison term; in the normative realm, people are compelled to change their behaviour due to normative expectations imposed by the community. For example, when an elderly person or a pregnant woman boards crowded public transport, norms dictate that a younger more able person should give up their seat. Seats are vacated not because there is a by-law requiring them to do so but based on certain commonly held communal values. Alternatively, the young able person may not want to relinquish their seat, but the fear of incurring the scorn of their fellow commuters compels them to act in a

[66] Dunklin, P. and Ellsmore, N., "Anti-Virus is Dead" Australian Information Security Association Meeting, August 19, 2009. I have a copy of this presentation. It is not publicly available.
[67] *See generally* Clarke, R. and Maurushat, A., "Who Will Bear the Cost of Insecure Devices" (2007) J18 Journal of Law, Information and Science 8. *See* Rice, D., *Geekonomics: The Real Cost of Insecure Software* (Addison-Wesley, 2008).
[68] Cerf, note 46 above.
[69] Lessig, note 1 above, page 235.

"right" way. In certain cultures, speaking to someone is done in proximity whereas in other cultures, close proximity when conversing will make the other person feel uncomfortable. This could result in the conversation ending abruptly, miscommunication as to intention, and perhaps put an end to what could have been a potential friendship. In cyberspace community norms also prevail. On the social network site Facebook, for example, it would not be appropriate to place photos of your animals in the act of coition. Such action would be deemed inappropriate in most online communities. The result may be that your Facebook friends would hide all of your future postings from their view, or 'de-friend' you online so that all communication is blocked, or that Facebook itself may remove the offending images after receiving a complaint. Cyberspace presents some interesting phenomena. Most people would not walk into a store and steal audio compact discs, DVD movies, or video games. Not simply because theft is illegal, but the community standards and moral sanctions operate to deter people from such action. Online, it is a different situation. The threat of legal sanction does not appear to be a sufficient deterrent against people illegally downloading content in peer-to-peer file-sharing systems. Equally influential, the lack of normative sanctions in peer-to-peer filesharing appears to be absent. If anything, online communities encourage the uploading and downloading of online content, whether there is a legal right to do so or not.

Like the law, market and architecture, norms do not provide an effective constraint on the botnet master. In the UNICRI study, "Hackers Profiling Project"[70] motivation of hackers were divided into 9 categories ranging from a "wannabe lamer" to a "cracker" to expert categories such as "skilled hacker" and "cyber warriors". The study revealed that community sanctions only appeared to play a role in the "ethical hacker" category. Such ethical hackers generally consider themselves bound to a set of hacker ethics which is explored in **Chapter 8**. Others such as the least skilled group of hackers known as the "wannabe lamers" were chiefly motivated by "it's the "in" thing to do" and generally speaking, hacked in groups.[71] More skilled hackers typically were motivated by either financial gain (criminal activity) or by professional causes as is the case with "military hackers", and in recent times, to leak information and protest political actions.[72] The botnet industry is populated with types of programmers known as "skilled

[70] Chiesa, R., Ducci, S. And Ciappi, S. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* (CRC Press, 2007).
[71] Chiesa, note 70 above, page 239.
[72] Chiesa, note 70 above, page 240. Hackers have been involved with Wikileaks. The hacker group Anonymous has been launching denial of service attacks against a number of websites for political motive. Operation Titstorm, for example, involved Anonymous shutting down the Parliamentary Website of Australia by bombarding the site with pornographic images in response to a controversial plan to filter Internet content. *See* Hardy, K., "Operation Titstorm: hacktivism or Terrorist Act?" (2010) University of New South Wales Law Journal 16(1).

hackers", and "cyber warriors" who are principally motivated by financial gain, and selfishness. According to the study, these type of programmers work alone and not in a group. Though, interesting enough, researchers of Eastern European commercial criminal groups reveals that many such programmers will only hack foreign individuals and organizations from wealthy Western countries, and then, some groups will only steal from bank accounts that contain above a prescribed limit of $1000.[73] This reflects a type of Robin Hood approach to many in the industry – robbing from the rich in Western countries to give to the poor in developing countries. It has been noted, however, that the Robin Hood trend has dissipated in the last few years with groups beginning to target local organizations and banks, as well as other organized crime groups.[74]

2.3.6 Interaction Between Modalities: Objective Versus Subjective

Lessig writes that "each modality has a complex nature, and the interaction among these four is hard to describe."[75] For this reason, Lessig added an appendix to further delineate the interaction between the modalities. Lessig explains the interaction by establishing a sub-theory which addresses objective and subjective constraints. Law, norms and markets, according to Lessig require judgment. If you decide to violate the law, a legal sanction may be imposed just as if you deviate from a social norm, the community may impose a moral sanction against you. You decide as an individual whether to purchase a product. Lessig contrasts law, norms and the market with that of architecture which he establishes as being "self-executing" in that little judgment is required on behalf of the individual.[76]

Architecture constrains until it is stopped or changed; architecture allows constraints through automatic means whereby "if we can make the machine do it, we can be that much more confident that the unseemly will be done."[77] Lessig uses the example of the nuclear missile launching. It is much more effective to launch by automatic or mechanical means such as a single button pressed at the President's desk, wired to a telecommunications system. Contrast this with a system which requires a chain of human commands. At each juncture, an individual

[73] Zenz, K., "Cyber Crime Within the Russian Federation" presentation at AusCERT 2008. Notes from presentation on file.
[74] Risky.biz Podcast, "RB2: AusCERT Podcast: Interview with Moscow-Based Cybercrime Analyst Kimberly Zenz" (May 20, 2009). *See also* Poulsen, K., Kingpin: The True Story of Max Butler, the Master Hacker Who Ran a Billion Dollar Cyber Crime Network (Hachette, 2011)
[75] Lessig, note 1 above, page 88.
[76] Lessig, note 1 above, page 237. For example, a user may choose to change the default settings.
[77] Lessig, note 1 above.

is required to make a judgment call before an order is obeyed. An individual's judgment would be made based on the possibility of moral sanction, legal sanction and the market to the extent that failure to follow orders may cost the officer employment opportunities.

The four constraints, as Lessig highlights, need to be distinguished when they are objective (someone observing when a constraint is imposed) as opposed to subjective (when someone experiences the constraint firsthand). From an objective perspective, law and norms allow you to perform an action then potentially suffer the consequences afterwards while markets and architecture impose a constraint (eg. price) prior to action. For a person who is "mature, or fully integrated, all objective constraints are subjectively effective prior to actions" providing that you know about them. In other words, they typically consider constraints before action is taken. Lessig contrasts this with the "immature" person who rarely utilized a subjective approach to constraints. Actions are performed without consideration of constraints. Borrowing from Foucault's work, Lessig argues, "the more subjective the constraint the more effective it is in regulating behaviour." [78]

2.4 CONCLUDING REMARKS

This chapter demonstrated that cybercrime and the use of botnets is unaccounted for in Internet regulatory theories because no one correctly predicted that the Internet could be controlled by any parties other than users, the government and commercial industry. As such, it is difficult to reconcile the botnet industry with these theories. While most of the theorists refer to the practice of hacking, cracking, and phreaking, it is within the paradigm of early hacking culture, the equivalent of the ever-curious individual looking to take "a peak under the hood of a car" due to the love of eloquent problem solving. No one in the 1990s correctly predicted the levels of hacking by organized criminal groups for commercial gain, or that the levels of fraudulent activity would be in the billions of dollars. Vint Cerf, one of the founders of the Internet, describes malware and botnets as a threat to the very vitality of the Internet. Equally difficult to reconcile, are the ways in which various stakeholders have responded to the problem of botnets. The role, for example, of self-organized communities is not easily situated in any Internet regulatory theory. The role of self-organized communities is explored in Chapter 8.

[78] This idea is derived from philosopher Jeremy Bentham's work on prisons. Foucault later revisited Bentham's work. *See* Bentham, J. *Panopticon, i*n Miran Bozovic (ed.), *The Panopticon Writings* (London: Verso, 1995), 29-95. Foucault, M., *Discipline and Punish: the Birth of the Prison* (New York: Random House, 1975).

where it will be demonstrated that squeezing self-organized communities' role into 'norms' is an ill-fit. Lessig's four constraints – market, law, architecture and norms – do not appear to provide sufficient constraint to botnet masters to shape their behavior. If anything, these supposed constraints act more like enablers allowing for the proliferation of online crime and malware. It is either the case that not enough research has been done on the commercial malware industry to better know how such groups fit in with Internet regulation theories, or, these existing theories need to evolve to account for the types of activities seen in the botnet industry.

Chapters 3 to 8 will form a detailed case study using botnets to demonstrate that Lessig's theory does not adequately accommodate the role of self-organised communities, not-for-profit corporations and working groups. **Chapter 9** will propose a modification to Lessig's theory to accommodate the role of self-organised security communities.

Chapter 3

BOTNETS

Table of Contents

3.0 AIMS OF CHAPTER

This chapter forms the foundation for the thesis on which all subsequent chapters will act as building blocks. The aim of the chapter is to establish an understanding of botnets. Understanding botnets requires knowledge first of the core elements that are involved in a botnet. A botnet involves "compromised computers", "bots", "bot servers", "botnet masters" and "command and control"sources. There are, however, other technologies or technical services that are used in conjunction with botnets. These too will be explored and include encryption, "fast-flux", "double fast-flux", "proxy","dynamic DNS", rootkits, and multihoming. These key terms are explained in the first part of the chapter. This is followed by an analysis of botnet design (how to make a botnet), motivation (what motivates botnet masters), use (botnet useage and business models), countermeasures (botnet take down methods), and botnet case studies. Botnets will be described first in plain language. A more technical explanation follows when looking at botnet uses and in the examination of sample botnets. Five botnets have been selected for analysis: aKill's amateur botnet, Torpig, Mariposa, Waledac, and Mega-D. These botnets have been selected as there is good information available about these particular botnets and they represent a variety of both botnet usage and methods of takedown.

In summary, this chapter provides the foundation of the thesis by explaining the mechanisms of botnets. This chapter exposes some of the technical challenges in tackling botnets and includes reference to obfuscation crime tools that are used in conjunction with botnets. It will be argued in later chapters that, due to the nature of botnets and their ability to rapidly mutate, a pure technical solution to the problem of botnets will not be feasible. As will be seen in the botnet examples of Waledac, Mariposa, Torpig, and Mega-D tackling botnets requires a collaborative effort between researchers, enablers such as Internet Service Providers (ISPs) and Domain Name System providers (DNS providers), law enforcement, and self-organised security communities such as Shadowserver.

3.1 BOTNETS

3.1.1 Key Terms

A botnet is comprised of core elements[1]. They are defined below for clarity and will be re-examined in more specific contexts in the analysis that follows this section:

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

Compromised Computer: The term "compromised computer"[2] is commonly used interchangeably, and in some cases wrongly, in the literature with "zombie", "bot" and "bot client", which confuses hardware with software, creates inconsistency of usage and may be confusing to users.[3] In this dissertation, a "compromised computer" is a computer that is connected to the Internet (an internet is any network of any size that uses the protocol TCP/IP,

[1] Solomon, A. and Evron, G., "The World of Botnets" Virus Bulletin September 2008.

[2] The term "compromised computer" has been selected over the term "compromised device". A computer may be as little as a processor, often a personal computer will contain multiple processors, or may be the world's largest computer. The term 'computer' is used here to refer to any computing device, even if is commonly called by some other name, and includes current and future devices with computing capabilities which may be connected to the Internet, including mobile phones, tablets, surveillance cameras, controllers for ADCs (analogue-digital converters) monitoring water-levels, etc. For this reason, Clarke, for example, prefers "device" (personal correspondence, Dr Roger Clarke). I have chosen "compromised computer", however, because it reflects the terminology used in computer science and information studies on botnets.

[3] The term 'zombie' has been appropriated by the computer security community as colloquial jargon for a compromised computer in a botnet. The reference of 'zombies' to botnets has been used humorously in writing on botnets:

> "In *The Night of the Living Dead*, zombies sucked brain matter in a frenzied hunger. In the computer world, a Trojan can be used to turn your PC into its own computing matter - turning it into a zombie machine. Once under the control of such an illicit program, the Trojan can be accessed by attackers intent on any number of ominous deeds." [3]

While the term 'zombie' is still used in association with botnets, the rhetoric among computer security experts has shifted from this humorous term to one which better connotes the serious problem of botnets. The term "bot" or "compromised computer" is replacing "zombie" in much of the botnet research and writing, including my own. My own personal reluctance to use the term "zombie" stems in part from my personal disdain for horror films and the monster genre but more importantly, from my experience in researching botnets and crime. I find it difficult to associate over-dramatised horror films and humour with a tool that is used to distribute child pornography, launch distributed denial of service attacks, steal personal information and perpetrate fraud, and to launch cyber warfare attacks, particularly if cyber warfare is followed by an actual war.

and the Internet is the largest such internet)[4] and on which a bot is installed[5]. The computer is thus said to be compromised.

Bot: A bot is software that is capable of being invoked from a remote location in order to provide the invoker with the capacity to cause the computer to perform a function.[6] Botnets have a modular structure whereby modules (bots) may be added or taken away from each bot to add new exploits and capabilities to it. This ensures a botnet master's ability to rapidly respond to technical measures set up to infiltrate and take down the botnet.[7]

Bot-Server and Command and Control Source (C&C): Command and control refers to the communications infrastructure of a botnet. A botnet master issues commands and exercises control over the performance of bots. Bots fetch data from a pre-programmed location, and interpret that data as triggers for action, and instructions on what function to perform. The pre-programmed location is known as "the bot server" or "command and control" source. Command and Control is achieved by means of what is commonly called a 'bot-server'. The term 'server' refers to any software that provide services on request by another piece of software, which is called a client. The bot requests and the server responds. Where the client is a bot, the server is reasonably enough called a bot-server. Common bot servers are Internet Relay Chat (IRC) servers, HTTP-servers, the DNS (by means of TXT records), and peer-to-peer (P2P) nodes.

Traffic between the command and control source and its bots may be in clear or encrypted form. For example, IRC is an open network protocol which can also be used with SSL (Secure Sockets Layer). SSL enables the establishment of an encrypted channel. Where the command and control of a botnet occurs in IRC alone, the information is openly available for viewing and tracking. When SSL is used in conjunction with IRC, the information is encrypted and is,

---

[4] TCP/IP is often used as a single acronym when in fact it references two key protocols. TCP refers to Transmission control Protocol. TCP is a connection oriented protocol that establishes a communication channel known as a data stream between two network hosts. IP refers to internet protocol and is an addressing scheme that links to IP addresses. *See* Plfeeger, C. and Pfleeger, S. , *Security in Computing 4th ed.* (Prentice Hall 2007), page 4.

[5] A computer may still be compromised in the absence of a botnet master. Where a controller is gone but where a botnet continues to infect computers, it is referred to as an "orphan botnet". *See* Gutman, P. "The Commercial Malware Industry" available at www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf (last accessed February 4, 2011).

[6] Modified definition of Clarke's where he defines bots as "(Generally, a program that operates as an agent for a user or another program. More specifically) software that is capable of being invoked remotely in order to perform a particular function." Clarke, Clarke, R., "Categories of Malware" (September 2009) available at http://www.rogerclarke.com/II/MalCat-0909.html (last accessed February 7, 2011).

[7] Dunham, K. and Melnick, J., *Malicious Bots* (CRC Press, 2009), page 54.

therefore, not visible to anyone who lacks access to the relevant decryption key. For the purpose of clarity, there will be no further reference to the term "bot server" unless found in a quote. Command and Control source (C&C) will be the term used throughout.

Botnet Master and Botnet Herder: The term botnet master is used interchangeably in the literature with botnet herder and attacker.[8] In this dissertation, the terms are defined more precisely. A botnet herder refers to someone who both builds the botnet and then issues instructions to it. A botnet master, by contrast, is anyone who can distribute instruction to any given botnet, whether or not they were also the botnet herder. A botnet master uses any device convenient to them in order to make changes to the content on the bot-server that will be fetched by the bots.

3.1.2 Obfuscation Methods

Many different techniques exist to make botnets robust, covert, and undetectable. These technologies/techniques will be described as "obfuscation tools", as such tools allow botnet masters to evade technological controls and legal sanction.[9]

Botnets are difficult to detect, filter or block. 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 the C&C host to change its location intermittently as required to keep a botnet functioning. They also allow botnet masters to hide behind a cloak of anonymity and low possibility of traceback of an attack to its source. These key terms are defined below and later explained in greater detail in the context of the case studies in **section 2.6**.

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.

---

[8] Provos, N. and Holz, T., *Vitual Honeypots: From Botnet Tracking to Intrusion Detection* (Safari 2008), page 370

[9] *See* Lovet, G., "Fighting Cybercrime: Technical, Juridical and Ethical Challenges" (Paper presented at the Virus Bulletin Conference 2009, Geneva, 23, September 2009). This was examined in 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.

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. **Chapter 7** will explore DNS policy to prevent dynamic DNS being used by botnet masters.

FastFlux is a particular dynamic DNS technique used by botnet masters whereby DNS records are frequently changed. This could be every five minutes.[10] 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.[11] Some FastFlux botnets rotate IP addresses every five minutes, and others every hour. Introducing a policy whereby IP addresses are not allowed to quickly rotate at the domain name server level will be explored in **Chapter 7**.[12]

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).[13]

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. Botnet instructions commonly use encryption. Encrypted instruction can then not be analysed making investigating, mitigation and prevention much more difficult. Public 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.

---

[10] *See* The Honeynet Organisation at http://www.honeynet.org/node/132 (last accessed February 6, 2011).
[11] Dunham, note 7 above, page 81.
[12] Gaaster, L., GNSO Council Issues Report on FastFlux Hosting (March 31, 2008) available at http://www.icann.org
[13] Barakat, A., and Khattab,S., "A Comparative Study of Traditional Botnets Versus Super-Botnet" in INFOSEC 2010. *See also* Vogt, R., Aycock, J., and Jacobson, M., "Army of Botnets" (2007) Network And Distributed System Security Symposium (ISOC) available at http://www.74.125.155.132/scholar?q=cache:x9cPT4RLO0J:scholar.google.com/&hl=en&as_sdt=2000 (last accessed June 29, 2010).

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."[14]

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. Professional botnet masters, however, do not use Tor to obfuscate the origin as virtual private network services are more popular..[15]

Virtual Private Network Service (VPN) is a network that uses a public telecommunications infrastructure (usually the Internet) to connect remote sites or users together[16]. 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."[17] VPN is made secure through cryptographic tunnelling protocols that provide confidentiality by blocking packet sniffing and interception software. VPN is used by many companies and government agencies as well as by cybercriminal gangs such as will be seen in **section 2.6** with the Mariposa botnet.

---

[14] Tor available at https://www.torproject.org (last accessed June 30, 2010). There are many other types of anonymising proxy servers and similar technologies such as Phantom Access Agent. See Zhao, X., Howe, D., Nissenbaum, H., and Mazeres, D.,"Phantom Access Agent: a Client-Side Approach to Personal Information Control" available at http://www.nyu.edu/projects/nissenbaum/papers/paa.pdf (last accessed June 30, 2010).
[15] Wouters, P., "Defending Your DNS in a Post-Kaminsky World" (2009) Black Hat Computer Security Conference available at http://www.blackhat.com/presentations/bh-dc-09-Wouters/BlackHat-DC-09-Wouters-Post-Dan-Kaminsky-slides.pdf (last accessed June 30, 2010).
[16] Virtual Private Network available at http://www.en.wikipedia.org/wiki/Virtual_private_network (last accessed June 30, 2010).
[17] Tyson, J., "How Virtual Private Networks Work" available at https://www.computer.howstuffworks.com/vpn.com (last accessed June 30).

Rootkits are software or hardware devices designed to gain administrator-level control and sustain such control over a computer system without being detected.[18] A rootkit is used to obscure the operation of malware or a botnet from monitoring and investigation.

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."[19] As will be seen in **section 2.6,** botnets such as Waledac, Torpig and Mariposa use P2P protocol as their back-up command and control. 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 architectures where a relatively low number of servers provide the core function of a service or application.[20] 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[21]. 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".

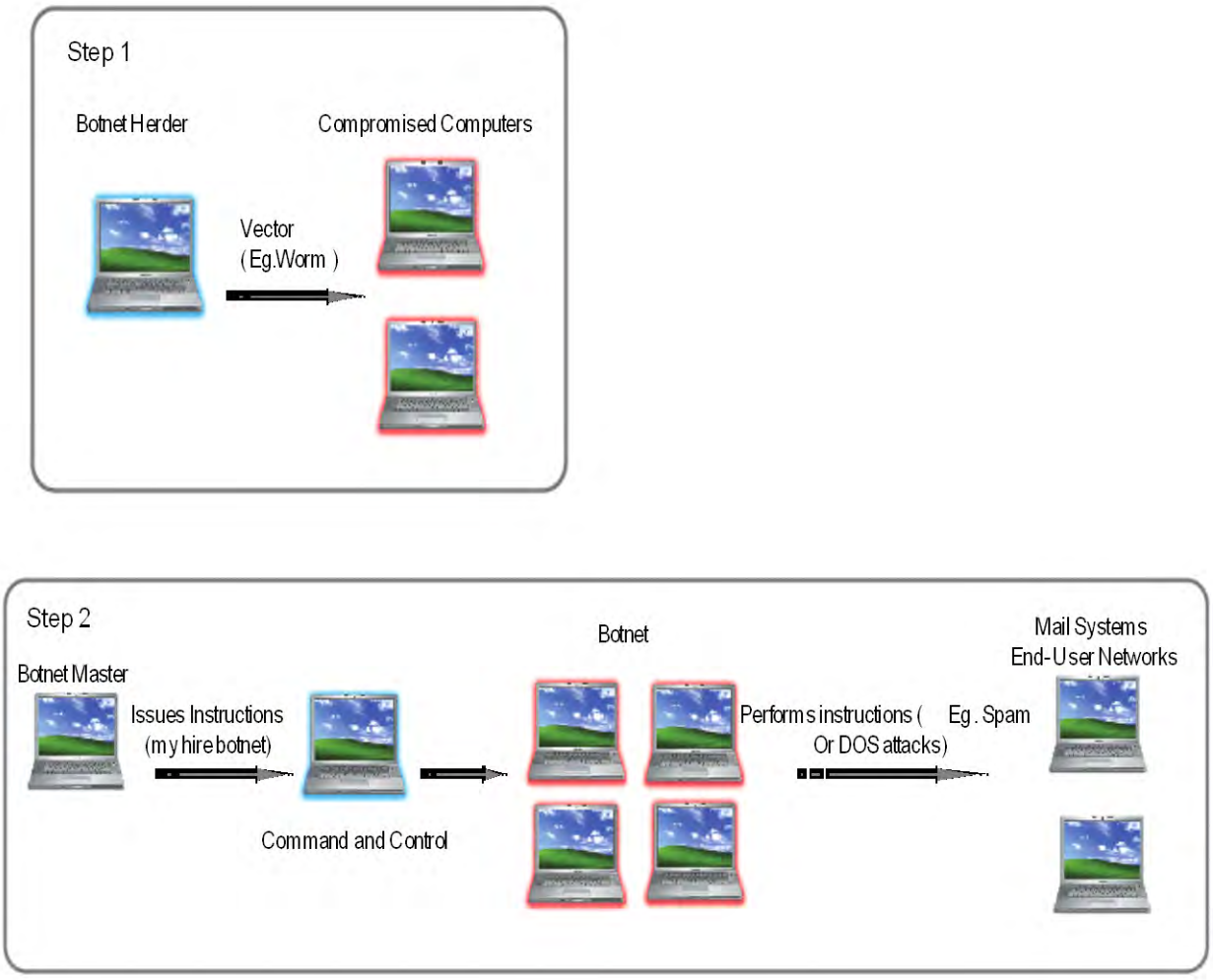
The next sections will use the terms defined in this section to examine design, motivation, use, business models and countermeasures relating to botnets.

[18] Pfleeger, note 4 above, pages 145-147.
[19] 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 (last accessed December 2011).
[20] *See generally*, Clarke, R., "Peer-to-Peer (P2P) – An Overview" (2004) available at http://rogerclarke.com/EC/P2POview.html (last accessed February 6, 2011).
[21] Oram, A. (Ed) *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (O'Reily & Associates: Sebastopol, 2001)

3.2 DESIGN: HOW TO MAKE A BOTNET

The following diagram in **Figure 3(A)** explains a botnet.

Figure 3(A): Steps in Procuring and Using a Botnet



In Step 1, the botnet herder needs to install bots on computers and thereby acquire compromised computers in order to build his/her botnet.

In Step 2, the botnet master then makes content available to the bots, which causes them to perform actions. The botnet master may or may not be the botnet herder who builds the botnet. The botnet master could, for example, hire the use of the botnet.

3.2.1 Step 1: Building a Botnet

There are a number of methods to compromise a computer to become part of a botnet. This process will be referred to as "building a botnet". Worms are the predominant form of delivery mechanism for acquiring bots. Worms are self-replicating and may spread through a number of methods. The principal methods are through exploiting operating system vulnerabilities, drive-by download and through social engineering techniques such as malicious weblinks and spam. With a system vulnerability or drive by download no action is required by the victim. The computer is compromised through an automated process. With social engineering, however, the user is tricked into clicking on a link which then executes malware onto the user's computer. These methods can be linked with a worm. Worms, however, are linked to the spread of the bots and not to botnet communication once a computer is compromised.[22] These bot acquisition methods are systematically considered below.

The methods used to install bots often target software, hardware, and operating system vulnerabilities.[23] Many vulnerable computers are those that are unpatched[24], use Windows and do not have a firewall.[25] Vulnerable computers are commonly identified through port scans.[26] Some commonly used ports are port 80 HTTP (not Microsoft-specific) and several related to Windows: port 42 WINS (host name server), port 445 Microsoft –DS-Service, port 1025 (Windows Messenger), 1433 (Microsoft-SQL-Server).[27]

Botnet masters are increasingly resorting to new techniques to build a botnet. Drive-by-downloads are becoming a more common method.[28] The term drive-by-download is used in many ways. For our purpose, a drive-by-download is a technique whereby malware is

---

[22] Dagon, D., Grizzard, J., Sharma, V., Nunnery, C., and ByungHoon Kang, B., "Peer-to-peer Botnets: Overview and Case Study" (2007) Hotbots Conference available at http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard_html/#uniq (last accessed June 30, 2010).

[23] A vulnerability is a feature or weakness that gives rise to vulnerabilities making a computer or computer network susceptible to attack.

[24] Operating system vendors issue patches to fix vulnerabilities. A patch is a set of computer code that purports to fix a vulnerability. Updating anti-virus and anti-spyware is a form of a patch. A threat is called a zero day exploit when there is no security patch available to fix the vulnerability.

[25] 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), pages 171-191. *See* also Clarke, R. and Maurushat, A., "The Feasibility of Consumer Device Security" (2009) UNSW Law Review Series " 5

[26] A port scan is a process whereby requests are sent to networked computer ports in order to see which ports are open on a target computer.

[27] 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)

[28] Provos, N., McNamee, D., Mavrommatis, P., Wang, K., and Modadugu, N., "The Ghost in the Browser: Analysis of Web-based Malware" (2007) HotBots07 Conference, Cambridge Massachusetts, USENIX.

downloaded to a computer as a result of a browser issuing a request for a web-page, but such that the browser's user is unaware that he or she is triggering the download. The user is probably also unaware during the download that he or she has triggered it. The malware in this instance could be software that compromises a computer, making it part of a botnet. The Torpig and Mebroot botnets, for example, discussed in **section 2.6** utilised a drive-by-download technique. This is explained by Mebroot and Torpig researchers:

> "Victims are infected through drive-by-download attacks. In these attacks, web pages on legitimate but vulnerable web sites are modified with the inclusion of HTML tags that cause the victim's browser to request JavaScript code from a web site ... under control of the attackers. This JavaScript code launches a number of exploits against the browser or some of its components, such as ActiveX controls and plugins. If any exploit is successful, an executable is downloaded from the drive-by-download server to the victim machine, and it is executed. The downloaded executable acts as an installer for Mebroot. The installer injects a DLL into the file manager process (explorer.exe), and execution continues in the file manager's context. This makes all subsequent actions appear as if they were performed by a legitimate system process."[29]

There are many bot vectors designed to compromise the computer. The principal vectors for bot infiltration are operating system vulnerabilities, drive-by-downloads and through social engineering techniques such as malicious weblinks, phishing[30] and spam[31]. Often, many malicious programs are installed all at once. This could be adware, spyware[32], Trojans[33] and spyware (which often includes keystroke loggers to steal usernames and passwords).[34] The installations, therefore, can be multi-purpose. Now that the botnet has been built, the compromised computer queries the command and control source. Instructions in the form of bots are issued to the compromised computer.

---

[29] 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).

[30] Phishing refers to the process of tricking recipients into sharing sensitive information with an unknown party. Typically, the user will receive an email that appears to come from a reputable organisation such as a bank. The Email includes what appears to be a link to the organisation's website. However, if you follow the link, you are connected to a replica of the website. Any details you enter, such as account numbers, PINS or passwords. These can be stolen and used by miscreants. See The Anti-Phishing Working Group at http://www.antiphishing.org/index.html (last accessed June 30, 2010).

[31] SPAM is unsolicited bulk email. See SPAM available at http://en.wikipedia.org/wiki/E-mail_spam (last accessed June 30, 2010).

[32] 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.
Spyware is "software that surreptitiously gathers data within a device, and makes it available to one or more other parties". *See* Clarke, note 6 above. One category of spyware is software that tracks a user's web-usage. The collection of this data may be used for behavioural marketing or for more nefarious purposes such as fraud and identity theft. The collected data is uses for those purposes whether or not the collection is consensual.
Some software may be classified as both adware and spyware.

[33] Software that purports to perform a useful function (and may do so), but does perform one or more malicious functions, and reaches the device as a result of a social engineering exploit. *See* Clarke, note 6 above.

[34] Software that surreptitiously records the keystrokes that are entered on a device. *See* Clarke, note 6 above.

3.2.2 Step 2: Establish Command and Control and Send Instructions

The bot includes functionality that retrieves updates from the C&C source of the botnet. The C&C source may be located in a webpage (a file that is accessed by means of a URL, including a pathname, e.g. http://www.isinwack3456.com/Soucre/Commands- 1000909.txt), in the Internet Relay Chat (IRC) channel, in peer-to-peer (P2P) channels, or by passing an unusual set of search terms to a search engine such as Google. The creation of a botnet may be subject to some controls. For instance, a botnet master may be able to specify over which range of IP addresses the botnet should spread.[35] In a typical botnet, there will be several C&C source locations to retrieve instructions, and these may be changed, perhaps quite frequently.

Compromised computers may be taken over by other botnet masters or the computers may be remedied such that they are no longer compromised. Botnet masters, therefore, need to acquire more compromised computers to replace those that are no longer part of the botnet. One of the ways to do this is to use the remaining compromised computers to send out messages to other addresses in order to install more bots.

Many botnets use a worm to propagate. As computer worms are self-replicating, they propagate for as long as computers can be found that have the vulnerability that the vector exploits. If one compromised computer infects seven other computers per day thereby compromising them and adding them into the botnet and then each of the newly infected computers also infects seven more computers, then one has a botnet that acquires compromised computers at 7^7 per day.[36] Botnet propagation may also be done through what is known as seed botnets, where a one botnet creates a new botnet, which may then be used for upgrades such as the Torpig and Mebroot botnets as will be described in **section 2.6**.

---

[35] Dunham, note 7 above, page 55.

[36] Dagon, D., Zou, C., and Lee, W. "Modeling Botnet Propagation Using Time Zones" (2006) Proceedings of the 13th Network and Distributed System Security Symposium (NDSS). I have used a very straight forward propagation mechanism of 7^7 for an example of propagation. Computer scientists use much more sophisticated mathematical formulas. Dagon et al., for example, use a worm propagation diurnal model:

$$\frac{dI(t)}{dt} = \beta\ \alpha\ (t)I(t)[N(t)-I(t)-R(t)]-\gamma\ \alpha\ (t)I(t)$$

3.3 USE: BOTNET USAGE AND BUSINESS MODELS

The botnet master may issue commands or he/she may hire out the botnet to third parties for illicit purposes such as to send spam, click fraud, install Trojans to steal usernames and passwords later used for fraud and identity theft, or to launch a distributed denial of service attack. Each of these is explained below.

3.3.1 Distributed Denial of Service Attack (DDoS)

A denial of service attack attempts to overload or shut down a computer, server, or service on the Internet such that legitimate users can no longer access it. Most DoS attacks target the hosts that run web servers and aim to make these websites unavailable. No data is stolen or compromised though a criminal may launch a DoS attack on a company's website to divert attention from the fact that they are hacking illegally into a corporation or organisations' files to steal information.

A naïve DoS attack can be undertaken by even small numbers of individuals sending packets to a target at the same time. This has the disadvantage for the attackers that the attacks are more readily traced, and hence the attack can be countered, and the individuals responsible can be themselves targeted.[37]

A Distributed Denial of Service Attack (DDoS) overcomes these weaknesses. 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) [38]. Distributed denial of service attacks are often performed with a botnet with several of the compromised computers sending packets to the target computer simultaneously. A DoS attack may also be distributed by use of peer-to-peer nodes[39].

---

[37] When a denial of service is caused by too many individual queries to a network it is usually unintentional. When a website spikes in popularity and received too much traffic all at once the website is overwhelmed thereby creating the same effect as a DoS attack. For example, it was reported that when Michael Jackson died in 2009, a number of websites reporting on the issue crashed due to overwhelming Internet traffic. *See* Denial-of-service attack available at http://www.en.wikipedia.org/wiki/Denial-of-service_attack#Unintentional_denial_of _service (last accessed June 30, 2010).

[38] Denial of Service Attack is well defined on http://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack (last accessed June 30, 2010).

[39] There are several documented instances where a DoS attack was launched through p2p. Athanasopoulos, E., Anagnostakis, K., and Markatos, E., "Misusing Unstructured P2P Systems to Perform DoS attacks: The Network

There are many documented instances where botnets are used to perform denial of service attacks on a website for personal reasons. Disgruntled employees who have been fired from their position may use a botnet to attack their former employee's website or a DoS attack is performed for some form of personal reason.[40] In another instance, a group of protesters known as "Anonymous" launched a denial of service attack against the Australian Parliament House website. The operation became known as "Operation Titstorm". The group infiltrated the website by sending network traffic of up to 7.5 million requests per second and sent pornographic images (predominantly of "tits") to Parliamentary websites. The attack was launched in protest to the proposed mandatory Internet filter[41]. Due to the volume of network traffic a botnet would have been required for the task.

3.3.2 Acquisition of Data to Enable Financial Fraud

Building a botnet often involves the installation of several computer programs onto a user's system without his or her knowledge. One piece of software compromises the computer and directs it to repeatedly query the C&C source. The inserted programs may track, collect and transfer information to the botnet master. This may include usernames and passwords, banking credentials, credit card information and copies of other identification information. This information is then used to steal money from bank accounts and to fraudulently use the captured credit card details or create cards that can be used to perform fraudulent transactions. The Mariposa and Torpig botnets in **section 2.6** were all used to steal money, commit mass fraud, and to commit identity theft.

---

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/. *See also* 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).

[40] In *R v. Caffrey* (2006) a botnet master performed a denial of service attack on the Port of Houston and interfered with shipping logistics. He claims to have done so due to a personal dispute with a girlfriend and the company in question. Reference to *R v. Caffrey* may be found 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 (last accessed April 27, 2010). Some details of the case are also described in Grabosky, P., *Electronic Crime* (Prentice Hall, 2007) page 80-81 and by Brenner, S., Carrier, B. and Henninger, J., "The Trojan Horse Defense in Cyber-Crime Cases" (November, 2004) Santa Clara Computer and High Tech Law Journal Vol. 21.

[41] For an excellent account of the incident *see* Hardy, K., "Operation Titstorm: Hacktivism or Terrorist Act?" (2010) University of New South Wales Law Journal 16:1.

3.3.3 Click Fraud

Many Internet businesses such as Google operate on a click fee basis. An advertiser or corporation pays a company a set fee based on the number of users that click on its link or advertisement. Click fraud then involves the use of a computer program that imitates a legitimate user of a web browser by clicking on a pay per click online advertisement.[42] Bots may be instructed to commit click fraud.

3.3.4 Spam

Botnets are frequently used to send spam. These are known as spam botnets. Mariposa, as will be examined in **section 2.6**, is a spam botnet targeting Microsoft hotmail customers. A spam botnet utilises user accounts whose details were acquired from compromised computers to send out emails to other Internet user's email accounts. There is anecdotal evidence that spam has become the driving force behind the economics of botnets during 2004-2011.[43]

3.3.5 Curiosity

Some botnet masters are not motivated by financial gain but merely out of curiosity. They establish their botnets as an experiment in acquiring computer skills. As will be seen in the AKILL botnet in **section 2.6**, amateur Owen Walker established and used his botnet primarily out of a curiosity. In particular, he attempted to launch a denial of service attack against the University of Pennsylvania without any other motivation than to see if it was possible.

3.3.6 Affiliate Employment

Some botnet masters finance their operations through unlawful installation of adware or spyware onto third party systems. Adware companies pay these so-called "affiliates". Dollarrevenue (DR Company) is an example of a Dutch adware company that uses the "affiliate model" to have

---

[42] Wilbur, KC, and Zhu, R., "Click Fraud" (March, 2009) ACM Marketing Science Volume 28, Issue 2. Gandhi, M., and Jakobssen, M., "Bad Advertisements: Stealthy Click-Fraudwith Unwitting Accessories" (2006) Journal of Digital Forensics Practice, Volume 1 available at http://www.informaworld.com/smpp/content~db=all ~content=a762491449 (last accessed July 1, 2010). *See also* Click Fraud available at http://en.wikipedia.org/wiki/Click_fraud (last accessed June 30, 2010)

[43] Ramachandran,A. and Feamster, N., "Understanding the Network-Level Behaviour of Spammers" (2006) SIGCOMM.

their software (DR software) installed onto third party computers. DollarRevenue is explained in detail below as adware companies are perceived as legitimate businesses in many jurisdictions, while other jurisdictions such as Australia, do not have a regulatory agency with the mandate to handle adware, spyware and unwanted software installation.

DR Company claims to be a legitimate advertising company, which displays third-party advertising on computers. The company claims to install its software with proper consent and notice. The company's website is no longer available on the Internet. Documents relating to DRCompany's business model are likewise not provided for public disclosure with the investigations into the company. Fortunately, the Internet Wayback Machine was able to reproduce the DRCompany website along with its payment terms, and terms of use. Captured below is the publicly displayed business model of DR Company as of Nov. 9, 2006, using the Internet Wayback Machine.

Figure 3(B) Wayback Machine Screen Shot of www.dollarrevenue.com **'Home Page' as it Stood on Nov. 9, 2006**

The company uses an affiliate business model whereby third parties sign-up to DR Company and agree to deploy DR Software through ActiveX and software bundling. Active payouts in North America average $.25 cents per installation as seen above. DR Company is structured like many spyware companies from a legal perspective – there is an attempt to transfer liability to third-party affiliates through an online contract. The 'Affiliate Agreement' is displayed in its entirety in **Appendix A** (found at the end of this chapter). Important terms are highlighted in **Figure 2(C)** below.

Figure 3(C) Key 'Content from 'Affiliate Agreement' Tab from Wayback Machine: Query 'www.dollarrevenue.com' Nov. 9, 2006

> "The action of sending any hits from any URLs which contain and/or promote the following content: warez, MP3s, ROMs, EMUs, newsgroup postings, SPAM e-mails, or any other site which contains content or promotes activities which are illegal in the United States of America will result in the immediate cancellation of the account from which the hits were sent and the forfeiture of any funds owed to that account.
>
> Affiliate who wishes to install DollarRevenue by use of an executable file (bundled or attached to his own program) must abide by DollarRevenue's Distribution Code of Conduct Agreement:
>
> **Affiliate agrees to notify users about the installation of DollarRevenue's product before installing the application on the end user's computer and to give such end user an effective method of avoiding installation. DollarRevenue reserves the right to approve final wording of this notification and to require periodic changes as necessitated by changes to DollarRevenue's product or for other business reasons."**

Each installation of DollarRevenue product by Affiliate must include and be subject to DollarRevenue product End User License Agreement (EULA), and Affiliate must obtain the informed consent from the end user to such EULA prior to installation. Our EULA is located at www.DollarRevenue.com/eula.asp...

Affiliate may not install DollarRevenue by any type of automatic installs, browser exploits, viruses, bots or by any other means not previously approved by DollarRevenue. Affiliate may not promote any competing programs at the same time as promoting DollarRevenue and using its Tools."[44]

[44] Affiliate Agreement retrieved using the Internet Archive machine (Nov. 9, 2006) www.dollarrevenue.com/affiliateagreement.asp

DR Company is a joint venture of three Dutch enterprises (E.C.S. International B.V., WorldToStart B.V. and Media Highway International B.V.).[45] These three enterprises along with their managing directors, whose identities remain undisclosed due to pending criminal investigation, were issued fines of one million Euros by the Dutch Telecom Regulator, OPTA, for installing unsolicited software onto over 22 million computers worldwide.[46] According to the OPTA press release of the decision, two companies were fined 300,000 EUR each while the third company was fined 200,000 EUR. The joint venture in question essentially involves three individuals: a director, a programmer and an investor – some of whom are under current criminal investigation for ties to organized crime[47]. One director was fined an additional 300,000 EUR while another was fined 200,000 EUR. The amount of 300,000 is the maximum that OPTA may impose for failure to adequately inform users of the purpose and functions of software installation as well as for failure to provide a method of reverse installation under the *Dutch Telecommunications Act 2004*.

In its decision, OPTA cites the following reasons for issuing the fine:

> **"These illegally-installed programs unleashed a flood of popup windows containing advertisements for all kinds of products and services. Unsolicited search toolbars were also installed, nested in the toolbars of Windows XP and Microsoft Internet Explorer, where they displayed 'alternative search results'.**
>
> **As the software did not include uninstall functions, it could only be removed with expert assistance."[48]**

Similar activities of DR Company have been reported on stopbadware.org, sunbelt-software and spamlaw.com. The OPTA report, however, fails to mention that DollarRevenue is also involved with malicious spam, iframe injections, and Trojan downloads, which initialize information-capturing software (such as passwords and browser histories). Stopbadware.org claims that the Trojan horse drsmartloader.exe was detectable after installing DR software. This Trojan then allowed the additional installation of adware components including SurfSideKick, Webhancer,

---

[45] OPTA, "Fact Sheet: Decision to Impose Fine on Dollarrevenue" (December, 2007) available at http://www.cytrap.eu/files/ReguStand/2007/pdf/2007-12-18-DollarRevenue-largestSpywareFineEurope-NL-OPTA.pdf sed session cybercrime workshop with law enforcement agents.

[46] Above.

[47] Many notorious Russian botnet herders with ties to organized crime were paid to distribute DR software. The money trail leads to a number of organized crime units operating in Eastern Europe. One director of DR Company in particular is being investigated for more formal ties with such organized groups. This information was parted under Chatham House Rules at a closed session on cybercrme workshop with law enforcement agents and former law enforcement agents who now work for private security research companies.

[48] OPTA, note 50 above.

NewDotNet and Command Service.[49] Spamlaws reports that additional adware and Trojan files are downloaded, including a DollarRevenue Trojan, along with, for example, Adware-DCToolbar, Adware-Zeno, and Uploader-R.[50] Some of the Trojan horse applications made available through other bundled adware programs with DR Software (such as iframedollars) collected usernames and passwords for Internet banking and e-commerce websites. Sunbelt Malware Research Labs provides a screen capture list and video of over 2000 additional adware/spyware programs downloaded in a single DR Software application.[51] Of these programs, several hundred are executable, Trojan style programs.

A conditional penalty was also imposed prohibiting the directors of DR Company from further distribution of unwanted software. The OPTA issued fine was appealed by DR Company. On June 18, 2008, the OPTA Commission dismissed DR Company's objections.[52] DR Company lodged an appeal against the Commission's decision to the Rotterdam District Court on July 29, 2008.

Following the investigation of Dollarrevenue, payment details of affiliates were tracked where possible which led to the prosecution of two botnet masters, Robert Bently and Owen Walker. There may have been more prosecutions of botnet masters who worked for Dollarrevenue. Bentley and Walker, however, are the only two reported arrests and prosecutions in the media and in caselaw databases. These prosecutions are considered in detail in **Chapter 5** as is the possibility of mandating the Australian Communications and Media Authority (ACMA) the task of investigating and prosecuting distributors of unwanted software installation.

3.4.7 Hire Out Botnet

Some botnet masters hire out their botnet for third party use. The Mariposa botnet had been partitioned for third party hire as will be seen in **section 2.6.** A botnet may be hired out like a rental car or it may be hired out accompanied with services. The latter is more akin to hiring a limousine or taxi. When a botnet is hired out with services, the botnet master will perform tasks

---

[49] *See* http://www.stopbadware.org/rports/reportdisplay?reportname=dollarrenvue
[50] More adware and Trojan files are included on the website. *See* the Spamlaws website at http://www.spamlaws.com/Dollarrevenue-adware.html
[51] Sunbelt list and video transmission of over 2000 unsolicited software available at http://www.sunbelt-software.com/ihs/alex/deskwizzclickfraud542006.pdf.
[52] OPTA "Decision on objection concerning fines for distributing unsolicited software (DollarRevenue)" available at http://www.opta.nl/asp/en/publications/document.asp?id=2724

for which the client pays. This could involve any of the categories described earlier in this section.

3.4 MOTIVATION: WHAT MOTIVATES BOTNET MASTERS?

While there have not been any specific studies that have examined the specific motivation of botnet masters, there have been studies that address hacker motivation. One recent study by the United Nations Interregional Crime and Justice Research Institute is of particular importance. The study is known as the Hackers Profiling Project and is run by former hackers. The UNICRI researchers collected data over 36 months relating to hackers. Detailed online surveys were distributed to hacker forums around the globe with 216 hackers responding form over 20 countries. Hackers classified themselves as "wannabe lamer", "script-kiddies", "crackers", "ethical hacker", "cyber warrior", "industrial spy", "government agent" or "military hacker" with hackers from each category responding to the questionnaire. Motivation for hackers included:

- "it's the in thing to do",
- to vent anger and grab media attention,
- to prove their power and get media attention,
- out of curiosity, to learn, for unselfish reasons, to improve working skills
- out of curiosity to learn but also out of pure selfishness
- for financial gain
- professionally (espionage/counter-espionage, vulnerability test, activity monitoring)
- professionally and for a cause (controlling and damaging systems)[53]

All hackers that complete the survey indicated that they were aware that their actions were illegal. Some considered their actions morally acceptable but felt guilty, other had no scruples, and others did not respond to the question. Additionally, all those interviewed believed that they would never be caught by law enforcement.[54] The survey ignores two key motivation factors: cyberwarfare and for a political cause. The motivation of botnet masters is relevant for assessing

[53] 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) ages 239 - 241
[54] Above, page 240.

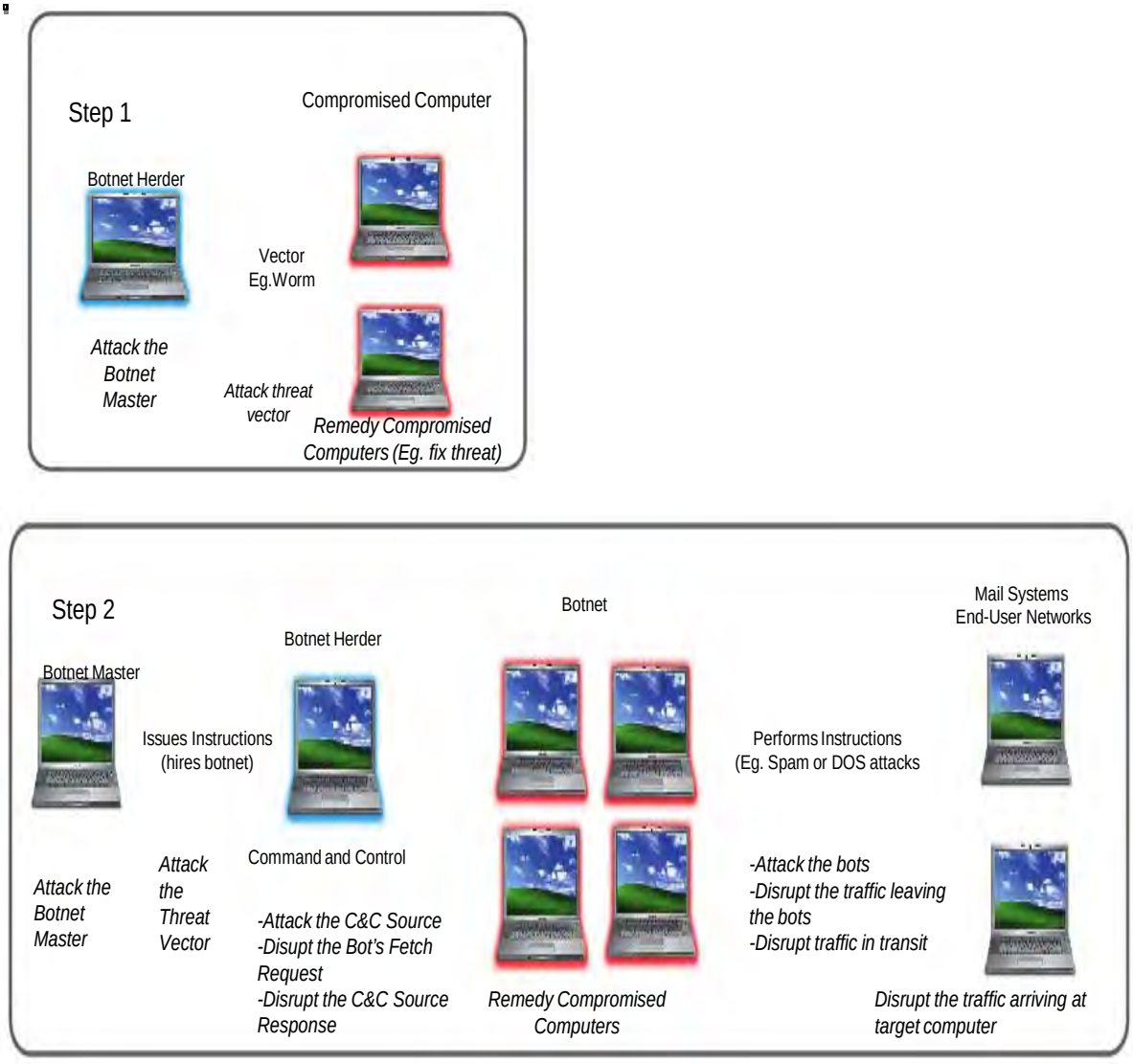
under what conditions the law may act as a deterrent and in determining appropriate charges and sentencing.

3.5 BOTNET COUNTERMEASURES

3.5.1 Introduction

Combating botnets through technical methods broadly includes prevention, detection, investigation and countermeasures. **Figure 3(D)** on the following page offers a range of theoretical countermeasure options. This chapter will concentrate on countermeasures that have appeared in the literature.

Figure 3(D) Botnet Countermeasures



3.5.2 Prevention

Many vulnerabilities and threats are well-known, and antidotes exist. The most basic approach to prevention involves methods to prevent a computer from becoming compromised. This depends on awareness, education and training of users, the installation of security software such as firewalls and anti-malware tools, the ongoing use of those tools, and the ongoing updating of them to deal with newly-emerged vulnerabilities and threats.

New vulnerabilities are continually being discovered, and new ones arise as software is modified and as new software is distributed. As new threats arise, new attacks are devised in order to take advantage of vulnerabilities. There is always a delay from the time a new vulnerability-threat combination arises until an antidote is available. Hence, vital though it is to stop the problem as it first occurs through preventative measures, it is impossible for prevention alone to be a sufficient countermeasure. Remedying compromised computers and ISP education of customers will be discussed in **Chapter 7.**

A secondary approach is to prevent a botnet from causing harm. This is discussed in subsequent sub-sections.

3.5.3 Intelligence Gathering

Intelligence gathering refers to passively observing and recording information about a botnet. The most common methods are traffic observation traffic (on IRC channels, or in other protocols such as HTTP, on P2P networks), honeynets, reverse engineering and collection of information in hacker forums and chatrooms.

Much intelligence gathering is performed using honeynets. Honeynets are information gathering places where an entity deliberately allows the computer to become infected. In doing so, information is collected as to how the computer becomes compromised, what types of malware are installed, and it allows the researcher to observe the computer code of the bots to ascertain the nature of how the botnet works and what in particular the compromised computer is being asked to do. If the botnet's instructions are encrypted, then the operator of the honeynet may

need to decrypt the instructions. The data and/or executable code may be encrypted on arrival, but it has to be decrypted by the bot before use. It is therefore accessible to the investigator in the computer's main memory, through the use of a debugging tool that enables programs to be run step-by-step and memory inspected at each step.

Reverse engineering is the study of a finished object or software, and its behaviour, to determine how it works. This may include the observation of the code while it is running to learn the behaviour of the software when processing different input. In a non-computer context this could be the equivalent of taking apart a car's motor, studying it then putting it back together to see how it is made up, and driving it in order to find out how it works. In a computer context, reverse engineering refers to the examination of the available code, and exercise of it, to determine how the software works. Reverse engineering can be categorised as passive and active. Passive reverse engineering involves the mere examination of source code. Many programs, however, do not display the source code of the product making passive reverse engineering impossible. Where the source code is not available or where it is encrypted, active reverse engineering techniques are required. A common active reverse engineering technique uses auditing of binary code often done through decompilation or disassembly.[55] Decompilation is the process of taking executable code and turning it into high level language source code such as Java. Disassembly is similar to decompilation only it involves turning executable code into assembly language. Assembly language is not as easy to analyse as high level language source code, but the conversion process is far more reliable. In advanced reverse engineering, techniques such as debugging, fuzzing, proxies and decryption are used.[56] Active reverse engineering techniques involve the use of specific software tools to perform reverse engineering; they cannot be performed through the naked eye observing source code. Advanced reverse engineering techniques, especially when used to decrypt ciphertext[57], may require significant time, effort and large quantities of data. Not all encrypted algorithms are possible to decrypt.[58] Honeynets provide some of the richest information on botnets including C&C sources, mutation routes (e.g. instructions received from webinex.com for two months then becomes webinex.biz then webinex.tv and so forth), commonly utilised ports, bots connected to the botnet, types of

[55] Harris, S., Harper, A., Eagle, C. and Ness, J. *Gray Hat Hacking: The Ethical Hacker's Handbook* (McGraw Hill 2008), pages 277 to 307.
[56] Above, pages 336-358.
[57] Ciphertext is computer code that is encrypted. The goal of decryption is to convert the ciphertext to plaintext which can then be understood. See Pfleeger, note 19 above. C. *See generally* Anderson, R., *Security Engineering: A Guide to Building Dependable Distributed Systems 2nd ed* (Wiley 2008) Chapters 5 Cryptography and 6 Distributed Systems for excellent discussion on cryptography, encryption and decryption, pages 129-213.
[58] Above.

malicious activities (e.g. Trojans or denial of service), patterns of replication (e.g. how a worm is spreading), and potentially information about the botnet master.[59] This information has benefit to security vendors in developing better anti-virus and anti-spyware software. The information is equally valuable to corporations and organisations in providing information about vulnerabilities in their network. Internet service providers use the information to develop spam filters, to identify vulnerable points in their networks, to identify customers at risk and so forth (ISPs are examined in **Chapter 7**). In other instances, a bot can be an invariant file, in which case other instances of it are easily recognisable in other devices, e.g. by checking for the presence of a segment of the file (a 'signature'), or by running a hash algorithm on the file and comparing the resulting hash with that of the captive copy. This in turn presents the opportunity to the owner of the compromised machine to be notified. Virtual honeynets may also provide present evidence which is later used in the prosecution of a botnet master. This is explored in **Chapters 4 and 6**.

Information gathering may also be done by observing hacking forums and chatrooms. There are many chatrooms, carder forums and blogs that openly discuss exploits, how to set up botnets, where to acquire stolen credit card numbers, the selling of stolen identity documents and credit card numbers, and other matters related to cybercrime. [60]

3.5.4 Disruption

Disruption is referred to in two senses. The first is in a technical sense while the second is more general. Disruption of botnet activities may be seen as a technical effort to subvert a botnet, or mitigate harm caused by a botnet. An example of subversion would be to redirect traffic from the C&C to a sinkhole.

One particular technique is called a 'DNS sinkhole', which is described by the SANS Institute as follows:

> "A DNS sinkhole works by 'spoofing' the authoritative DNS servers for malicious and unwanted hosted and domains. An administrator configures the DNS forwarder for outbound Internet traffic to return false IP addresses for these known hosts and domains. When a client requests to resolve the address of such a host or domain, the sinkhole returns a non-routable address; or any address except the real address.

[59] *See* Provos, note 8 above.
[60] Poulsen, K., *Kingpin: The True Story of Max Butler, the Master Hacker Who Ran a Billion Dollar Cyber Crime Network* (Hachette, 2011).

> When a new domain is added to the list, the domain falls under the direct control of the sinkhole administrator. After this moment, it is no longer possible to access the original host or domain. "[61]

Sinkholes were used to disrupt and takedown Waledac, Mariposa and Mega-D botnets as will be seen in **section 2.6** and later again in **Chapter 8**.

Other technical measures may involve efforts to stop the spread of the propagation method (often a worm). In a more general sense, disruption may refer to any effort to curtail the botnet. This may mean legal efforts pursued against botnet masters or spammers who contract botnet services as explored in **Chapters 4, 5 and 8**. It may also involve attempts to make a botnet less profitable by injecting or removing compromised computers from a botnet rendering it less effective. Disruption may also coincide with counter-attacks and detection measures. An organisation may launch a denial of service attack to known C&C servers where they are located on domain name pages. An organisation may also deploy a honeynet which not only detects attackers but may also run programs that implement protective security strategies upon attack.

3.5.5 Counter-Attack

Counter-attack involves engaging the botnet master in a form of a hacking attack. This may include attempts by the 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.[62] 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).[63] 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%. Unfortunately, the survey did not ask how many organisations were engaged in strikeback. Legal issues in strikeback are explored in **Chapters 4.**

---

[61] 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).
[62] *See* Smith, B., "Hacking, Poaching and Counterattacking: Digital Counterstrikes adn the Contours of Self-Help" (2005) 1 Journal of Law, Economics and Policy 185.
[63] Hutchinson, W. and Warren, M., "Attitudes of Australian Information System Managers Against Online Attackers" (2001) 9(3) Information Management & Computer Security 106.

3.5.6 Take-Down Methods

The first part of any botnet takedown necessarily involves botnet analysis and intelligence gathering. This is often done through a virtual honeynet. As described by two of the most authoritative experts on honeynets and botnets, Provos and Holz, "a honeynet is a closely monitored computing resource that we want to be probed, attacked, or compromised. More precisely, a honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource."[64] Researchers will commence by finding malware and botnets, often done in virtual honeynets. They will observe the botnet name, locations of C&C, control mechanisms, propagation method, which computers connect to the C&C, and its uses. Intelligence may be used afterwards to take down the botnet. The method of takedown will depend on the structure of the botnet. Broadly speaking, four methods are apparent in the technical literature, which I will refer to as:

1) ISP and/or domain name service (DNS) provider disconnection ,

2) Infiltration and disruption of the C&C in IRC or P2P channels (typically by self-organised security communities and researchers),

3) Prosecution of the botnet master(s), and

4) Bot remediation where the vulnerability of compromised computers is fixed.

Each of these takedown methods is explored below.

3.5.6.1 ISP and/or DNS Provider Disconnection

The first method involves contacting the DNS or ISP provider inform it that it has clients using their services to run botnets. Contacting the provider is sometimes performed by law enforcement or security organisations. Where a botnet is programmed to receive its instructions (C&C) from a website, a request may be made for disconnection of service or the ISP may blacklist the range of unique Internet Protocol Addresses the botnet is using to run its C&C. The DNS provider may also be contacted with a request to remove the domain name from its

[64] Provos, note 8 above, page 8.

register. This can be an effective route but requires the person to know the webpages to which the botnet is connecting to receive its instructions (C&C), the DNS/IP address of the IRC server, port and nickname of the bot, and most importantly, it requires desire on the ISP or DNS provider to take action.

As will be seen in detail in **Chapters 7**, there is no legal obligation for ISPs and DNS providers to take any action to disconnect the webpage or remove the domain name. That said, many DNS providers and ISPs do not tolerate abuse of their service and will take measures to stop the botnet by blacklisting the IP addresses where the C&C receives its instruction or termination of their connection contracts. This approach, however, is not always possible for a number of reasons. The service provider may have legal obligations that restrict its ability to disconnect or blacklist to situations where the terms of use is violated, or they may have to notify the owner before disconnection which is discussed in **Chapter 7**.[65] This is not always easy to prove with botnets. The diversification of IP addresses and webpages across multiple ISPs and DNS providers and often jurisdictions may make this approach unfeasible. For example, where a botnet has multiple channels where it receives its instructions, several hundred ISPs may need to be contacted across different jurisdictions. Any action taken would require disconnection by ISPs at the same time otherwise the botnet merely selects another channel to receive its instructions (C&C). Botnets could set up C&C in multiple channels: webpages, search engine keywords, IRC, and P2P.

Where the C&C is located in a P2P channel, ISPs will generally not be prepared to play a role in disrupting . This is because it is highly unlikely that their customer is actively performing the function of botnet-master. Rather, their customer's machine has been (probably quite briefly) harnessed by some other party to perform that function. The ISP will not disconnect their customer, though it may be in a good position to contact and inform them that their computer is being used as part of a botnet (and, hopefully, what they can do about it).

The role of ISPs is examined in the context of warrants in **Chapter 6**, of procedural obligations under the *Cybercrime Convention* in **Chapter 5**, and **Chapter 7** is devoted to ISP and DNS providers removal of C&C webpages, and bot remediation.

[65] Many domain name service providers must notify the domain name registrant prior to removal of a domain as per the contractual terms. This will be examined in **Chapter 7.**

3.5.6.3 Infiltration and Disruption of the C&C in IRC or P2P Channels

In the second method security researchers[66] run interference with the C&C of the botnet. This can be done by a number of means. If a botnet uses centralised communication whereby the C&C is located on a webpage or in an IRC channel, it may be possible to convince the ISP that operates the authoritative domain-name server to change the DNS entry in order to redirect traffic to a sinkhole. It may also be possible to remove the domain-name from the DNS completely, by convincing the relevant domain-name registrar to delete or at least suspend the entry in the register. This was done with the Torpig botnet as will be seen in **section 2.6**.

It is also possible to perform a denial of service attack on the host of the web-server where the C&C is located, thereby preventing any effective communication from occurring between the C&C and compromised computers. This approach, however, involves collateral damage, because other processes running on that host are affected, as are processes running on computers elsewhere on the same sub-net and nearby sub-nets. The technique also requires continual observation and attention by the individual or organisation disrupting the botnet. It does not permanently shut down the botnet. Furthermore, it would quite likely constitute a computer offence of /illegal access, interception or interference to a computer or data held in a computer.[67] Self-defence would likewise not apply in this situation as botnet activists are often not defending their own property but, rather, the property of third parties. These legal issues are explored in **Chapter 4**.

Where the C&C is in the open IRC space, it is unprotected and anyone can modify the functioning of the C&C Host. Where the C&C is decentralised such as in P2P, it is possible to inject false commands, thereby "polluting" the communications amongst compromised computers. A further possible technique is described by Krogoth as follows:

> "It could also be interesting to use the automatic patching system of the botnet where the existing communication infrastructure is used to distribute patches to the client. It could be tried to inject an "insurgent" update into the botnet. The bots would then automatically patch themselves and the botnet would cease to exist.
>
> "There are many ethical and legal aspects in this strategy for obvious reasons. Such an update can fail and leave the computer unoperateable [sic]. Since the update would be run without the users consent

[66] The term 'security researchers' is used broadly here. This may include security organisations, security experts, individual researchers, security companies or simply hacker activists.
[67] The *Council of Europe Convention on Cybercrime* uses the language in Articles 4-6 of illegal access and interference whereas in Australia, for example, the terminology is one of unauthorised access, modification or impairment as found in section 476 of the *Criminal Code 1995 (Cth)*.

> it could lead to legal actions against the person injecting the update into the botnet. Even when it was done with reputable motives."[68]

The ethical and legal implications of patching compromised computers through the injection of "insurgent" code will be explored in **Chapters 4 and 8**. Researchers of the Torpig botnet contemplated using this technique but rejected it for the reasons of unpredictability and legal liability as will be described in **section 3.6**.

Other infiltration methods have been suggested that would damage the reputation of the botnet to effectively discredit it as a commercial product for hire. This method of reputation damage is created by disrupting the botnet-herder's business model.[69] Where the motivation is financial, botnet products and services are offered, promised and delivered for a price that reflects the market. Botnet masters compete for market share.

For example, a specific botnet may be hired out for its ability to deliver a million spam messages per day to active email accounts. If researchers flooded the spam database with bad email addresses, the spam response rate would be lowered, thereby lowering the reliability of the botnet to deliver a product. This might drive customers to another botnet or lower the price for the services provided. On the other hand, experience with spam generally has shown that spammers have little interest in the proportion of email-addresses that are valid, or indeed duplicates. They are more interested in high-volumes. In the situation where a botnet has been hired to perform a DDOS attack, disruption of the attack or poor performance could also discredit the reputation of the botnet master. For example, if I contract a botnet master to perform a DDOS attack for 48 hours on a website, and that website is only attacked for a mere 2 hours, the reliability of the service is undermined. In this instance, the customer is better able to gauge the effectiveness of a DDOS attack on the target, and hence negative reputational impacts have a better chance of arising.

---

[68] Krogoth, "Botnet Construction, Control and Concealment: Looking into the Current Technology and Analysing Tendencies and Future Trends" (2008), page 50. The authors claims that the paper was submitted as part of the requirements for the award of the MSc in Information Security, but the university is not declared. The version of this paper was modified for the ShadowServer website. ShadowServer is a group of voluntary security researchers who track and document information on malware and botnets. The paper is available at http://www.shadowserver.org/wiki/uploads/Information/thesis_botnet_krogoth_2008_final.pdf (last accessed July 5, 2010).

[69] Liao, Q., Striegel, A., and Li, Z., "Botnet Economics: Uncertainty Matters" (2008) paper presented at WEIS Conference. The paper is available online at http://www.weis2008.econinfosec.org/papers/Liao.pdf (last accessed July 5, 2010).

Another method similar to adding bad email addresses is to add bad compromised computers into a botnet through what is known as a Sybil attack.[70] In a Sybil attack, fake compromised computers are added into the botnet. Once these fake compromised computers join the network, they will connect to the command and control where they will receive their instructions. Instead of following instructions, however, the fake compromised computers will fake their engagement but actually do nothing. This method attempts to destroy the reputation and market the botnet master seeks to engage in.

3.5.6.4 Prosecution of Botnet-Herder or Botnet-Master

In order to prosecute a botnet herder or botnet master, they must first be identified. This is an extremely difficult task. There are three general ways to identify a botnet-herder and the one or more botnet masters. The first involves traceback through technical means to the source. Identification of a botnet master through traceback is a difficult task, as botnet masters often use obfuscation tools that make their communications anonymous and extremely difficult to traceback. Another method of identification is to monitor botnet and malware chatrooms and blogs for information that assists in identifying the person. Many amateur botnet masters will pose questions about botnets and brag about their conquests in chatrooms and blogs.[71] Finally, if one botnet master is caught, a plea bargain can be made for the identification of other botnet masters. This was the case with a botnet master in the US who later identified Owen Walker of New Zealand. The prosecution and decided outcome against Owen Walker will be examined in **Chapter 4**. Botnet masters make money by payouts from adware companies, hiring out their botnets, and by committing fraud such as stealing banking details and credit cards. It is, therefore, possible in some instances to follow the money trail. Identification of a botnet master by following the money trail is considered, albeit briefly, in **Chapter 4**. Once a botnet master is identified prosecution is then possible providing there is sufficient evidence.

3.5.6.5 Bot Remediation

The bot remediation approach involves remedying the compromised computers over which the botnet has control. Bot remediation involves the identification of compromised computers,

---

[70] Krogoth, note 68 above, page 51-52.

[71] Many researchers have noted based on the questions asked and descriptions of botnets that those hanging out in chatrooms and blogs are amateurs. Professional botnet masters typically do not hang around in cyber cooridors gossiping and bragging about their conquests *See* Provos, note 8 above. *See* Poulsen, note 60 above. *See also* Chiesa, note 58 above.

possibly notification to the owner of such computers, and action, either voluntary or mandatory, which provides a remedy to the problem. To remedy a compromised computer means to install and run software that will remove or otherwise nullify the bot. Alternatively, the loading of the software, and perhaps also the invocation of it, may be performed over the Internet. A further possible approach is to disconnect the compromised computer from the Internet. Bot remediation differs from the other methods in an important way – it denies the botnet-master the use of that computer and hence permanently reduces the size of the botnet.

The first two methods (ISP and/or domain name service (DNS) provider disconnection and infiltration and disruption of the C&C in IRC or P2P channels), only puts off the botnet herder for a period of time. The botnet herder can still set up new C&C channels, and write new bots (malicious software programs) to communicate with the compromised computers. The takedown of the botnet is, therefore, only temporary as most botnets use self-replicating worms. This means that stopping the C&C of the botnet does not necessarily prevent the botnet from continuing to spread and thus acquiring new compromised computers. It also does not prevent a botnet from spreading new bots once a new C&C is established. Prosecuting the botnet herder also is not an absolute solution as the botnet is highly susceptible to being taken over by another botnet herder. Moreover, the compromised computers sit dormant awaiting new instructions. Only the last method, bot remediation, potentially removes the compromised computers from the equation. To use an analogy to war, one can disrupt an army by interfering with its communications systems, and one can kill the General but there will always be more Generals willing to step up, and ways of re-establishing communications. But if there are no soldiers, the General has no one to carry out the orders in his command.

The most effective takedowns of botnets include a combination of these methods such that the C&C is taken out, the botnet master is identified and prosecuted, and compromised machines are remedied. No botnet operations to date have performed all three.

3.6 SAMPLE BOTNETS

3.6.1 Introduction

This section presents several short vignettes that provide an initial empirical base for the remainder of the dissertation. The explanations apply the model and terms presented in the

earlier parts of this chapter. Some of these cases are discussed in greater detail in later chapters. An amateur botnet master is explored first followed by more sophisticated botnets, some of which are linked to organised crime: these are Torpig, Kraken and Mebroot.

3.6.2 AKILL's botnet

AKILL is the hacker nickname of amateur botnet master, Owen Walker from New Zealand. AKILL's botnet was active in the early 2000s. It may be still be active as will be explored below (taken over by another botnet master). Walker's botnet does not itself have a name. Walker was arrested for his botnet activities following an investigation by the FBI and the Dutch telecommunications regulator OPTA (see ***R. v. Walker*** in **Chapter 4** for a detailed examination of the case against Walker). It is difficult to find accurate information on AKILL's botnet, as law enforcement claim it to be an advanced bot programme[72], while computer security researchers disagree, claiming the bot to be primitive and five years behind being state-of-the–art.[73]

AKILL's bot code was a derivative of an existing bot code known as Akbot. Walker added some new code to modify Akbot. AKILL's botnet used a centralised command and control on an IRC channel. The bot programs were not encrypted. There was no fallback if the attempt to use that IRC channel to fetch instructions was unsuccessful. Walker's modified code allowed his botnet to remove other bots on the compromised computer. His bots removed any pre-existing bots on a machine and thus took over the compromised computer from the former botnet master. There can be any number of different bots installed. It may be desirable to remove other bots (malicious code) at the same time (e.g. for professional jealousy reasons, or to avoid a separate low-grade bot attracting unwanted attention to the compromised computer resulting in it being remediated; but it is not necessary to remove other bots. Akbot had not previously been used for bot removal. Bot removal in this situation meant that a rival botnet master rewrote the instructions to the botnet and was, therefore, able to take over the botnet from the original botnet master. That said, the tactic of destroying rival malicious code to take-over another botnet is often done.[74]

---

[72] *R. v. Walker*, HC HAM CRI2008-0750711 [2008] NZHC 1114.
[73] *See for example*, interview with University of Auckland Computer Security Professor, Peter Gutmann. ComputerWorld, "Akill Evaluated: Crime Lord or Script Kiddie?" (2008) available at http://computerworld.co.nz.new.nsf/scrt/8965613190D60231CC257431007FCDA0 (last accessed June 24, 2010.558-352-5/09/11.
[74] Above.

AKILL found the Akbot code on the Internet, modified it, ran the botnet and conducted his own transactions. No reports have been found of efforts to take down AKILL's botnet. It may have been taken over by another botnet master and it is probably that the botnet will continue to grow as there is a self-replicating mechanism built into the program. AKILL's botnet will be used in this thesis to distinguish between amateur botnets and those run by professionals as will be seen in the Torpig, Waledac and Mariposa botnets. As will be seen in **Chapter 4**, Walker operated this botnet primarily out of curiosity.

3.6.3 Torpig

The Torpig botnet appears to have originated in Eastern Europe in 2005 and is thought to be a portion of the larger Storm Botnet. In 2009, a group of university researchers at the University of California, Santa Barbara (UCSB) infiltrated the Torpig botnet to gather intelligence as to the botnets inner workings.[75] They used a virtual honeypot[76] to record the commands the bot receives, monitor the malicious activities, and determine which computers had been compromised. The aim of the researchers was not to take the botnet down, but to merely gather intelligence on the botnet and share this information with law enforcement, CERTs, and other security researchers.

The UCSB research team was able to take over the C&C source of the Torpig botnet for 10 days. During this time they discovered that there were two C&C methods through a reverse engineering of the domain generation algorithm. The first C&C used encrypted HTTP protocol linking to domain names. The bot was not detected by any anti-virus or anti-spyware programs**.** The backup C&C was located in a separate botnet known as Mebroot**.** Mebroot was obscured from view by means of a rootkit. The domain name C&C generated a weekly domain name, thereby moving the C&C to a new location each week. When the C&C was not functioning properly by rotating through a fast-flux each week, Torpig then began to generate a new C&C every day, and if every day did not work, the botnet switched C&C through a rapid fast-flux of every 20 minutes.[77]

---

[75] Stone-Gross, B., Cavallaro, L., Gilbert, B., Sydlowski, M., Kemmerer, R., Kruegel, C., and Vigna, G., "Your Botnet is My Botnet: Analysis of a Botnet Takeover" (2009) CCS, ACM 978-1-60

[76] "A honeynet is a closely monitored computing resource that we want to be probed, attacked, or compromised" *see* Provos, note 8 above.

[77] Kemmer, note 29 above.

The UCSB team recorded 180 000 unique hosts making up the botnet. During the 10 days, they observed message flowing from the bots back to the botnet master containing banking details from over 8 310 accounts in 410 financial institutions, together with 1 660 sets of credit card details. The researchers describe how the banking information was obtained as follows:

> "Torpig uses phishing attacks to actively elicit additional, sensitive information from its victims, which, otherwise, may not be observed during the passive monitoring it normally performs. These attacks occur in two steps. First, whenever the infected machine visits one of the domains specified in the configuration file (typically, a banking web site), Torpig issues a request to an injection server. The server's response specifies a page on the target domain where the attack should be triggered (we call this page the trigger page, and it is typically set to the login page of a site), a URL on the injection server that contains the phishing content (the injection URL), and a number of parameters that are used to fine tune the attack (e.g., whether the attack is active and the maximum number of times it can be launched). The second step occurs when the user visits the trigger page. At that time, Torpig requests the injection URL from the injection server and injects the returned content into the user's browser. This content typically consists of an HTML form that asks the user for sensitive information, for example, credit card numbers and social security numbers. These phishing attacks are very difficult to detect, even for attentive users. In fact, the injected content carefully reproduces the style and look-and-feel of the target web site. Furthermore, the injection mechanism defies all phishing indicators included in modern browsers. For example, the SSL configuration appears correct, and so does the URL displayed in the address bar. An example screen-shot of a Torpig phishing page for Wells Fargo Bank i shown in Figure 2. Notice that the URL correctly point to https://online.wellsfargo.com/signon, the SSL certificate has been validated, and the address bar displays a padlock. Also, the page has the same style as the original web site."[78]

The researchers recorded the phishing scams noting that 14% related to jobs/resumes, 7% were money making proposals, 6% sports fans, 5% exams and websites on worrying about grades, and 4% were related to sex.[79] The researchers reported that the banking information collected was sold to multiple parties in the underground economy. Symantec also followed the Torpig botnet, noting that credit card details were fetching a rate between $.10 and $25, while bank accounts were worth between $10-$100, with total profit estimates from anywhere of $830 000 thousand to $8.3 million.[80] It is reasonable to infer that Torpig's botnet master(s) were motivated by financial gain.

The researchers expressed concern at the risk of being pursued by law enforcement as well as potential retribution victims. They have openly expressed a strong belief that the Torpig botnet originated in Eastern Europe and may be linked to organised criminal groups.[81] The researchers contacted the FBI during the time-frame within which the researchers had infiltrated the botnet. Once notified, the FBI sent the data and sent it to the National Cyber-Forensics and Training

---

[78] Kemmer, note 29 above.
[79] Above.
[80] 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).
[81] Kemmer, note 29 above.

Alliance, a not-for-profit security corporation.[82] The FBI made requests to registrars to de-register the domain names of the documented C&C he researchers note that on the day that the FBI was notified, the C&C migrated from domain names to the encrypted rootkit. Mebroot As the researchers note, this is likely not a coincidence.[83] The Mebroot botnet is encrypted. No researcher at the time was able to crack Mebroot's encryption. The Torpig botnet will be further discussed in **Chapters 4, 8** and **9.**

3.6.4 Waledac

The Waledac botnet was established in 2009 by compromising computers through social engineering techniques such as links within a spam message. Waledac was then used to send spam to email-addresses held in the address-books associated with Hotmail accounts. Microsoft claimed that in 2009 the Waledac botnet was responsible for the sending of 651 million spam messages from Hotmail email accounts.[84]

Waledac messages were encrypted.[85] The Waledac botnet had a sophisticated hierarchical C&C structure which used HTTP (and did so in an original manner, between P2P nodes), DNS and DCE/RPC protocols.[86] The reason why Waledac is said to be hierarchical is that it used an intermediate layer of proxy bots as well as the usual worker bots. The layer of proxy bots was responsible for relaying information from the C&C source back to the worker bots.

The primary C&C of Waledac was embedded in webpages, which fluxed through 273 locations. This was backed up by a double fast-flux for the P2P communications.[87] Waledac is believed to have been either a derivative of the STORM botnet and/or a sold-off partition of the STORM botnet.[88] STORM was the first known botnet to use P2P for the C&C and is considered to be

---

[82] *See* Poulsen, note 60 above.
[83] Kemmer, note 29 above.
[84] *See* "Waledac Questions Answered" available at http://www.lavasoft.com/mylavasoft/company/blog/waledac-questions-answered
[85] Balatazar, J., Costoya, J. And Flores, R., "Infiltrating WALEDAC Botnet's Covert Operations", (2009)TREND MICRO.
[86] Jang, D., Kim, M., Jung, H-C, N, B-N, "Analysis of HTTP@P Botnet: Case Study Waledac" (2009) Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, page 410.
[87] Schneier, B. "The Storm Worm" (October 4, 2007) Schneier on Security http://www.schneier.com/blog/archives/2007/10/the_storm_worm.html (last accessed June 24, 2010).
[88] Naraine, R. "Storm Worm Botnet Partitions For Sale" (2007) available at http://www.zdnet.com/blog/security/storm-worm-botnet-partitions-for-sale/592. Interview with Joe Stewart, a computer security researcher with SecureWorks.

the most sophisticated botnet of its generation.[89] The STORM botnet is believed to come from an organised criminal group in Eastern Europe.[90]

All of the domains were within the .com top level domain. In February 2010 Microsoft's Digital Crimes Unit sought a temporary restraining order to order the registrar, in all cases Verisign, to de-register the domains of Waledac's C&C. A federal judge granted Microsoft a temporary restraining order against the domain owners. The court order is filed as sealed and is therefore not publicly available. The document, however, has been leaked on the Internet and is available on security blogs.[91]

The C&Cs have to be neutralised at the same point in time if the botnet is to be dismantled, because otherwise the botnet-master has enough time to update the bots and migrate the C&C Host to another location. The DNS entries for the C&C domains were removed from the authoritative domain-name servers at the same time. There were 20 other domains that were registered in China. With the assistance of the China CERT (CNCERT), the DNS entries for those 20 domains were removed from the authoritative domain-name servers. CNCERT and the Chinese ISPs were not legally obligated to do so, but presumably had the discretion to do so, and did so on a voluntary basis.

At the same time that Verisign and CNCERT removed the 273 domain names of the C&C of Waledac, security researchers performed an attack on the back-up of the C&C in the P2P channel. Microsoft partnered with Shadowserver Foundation (a self-organised security community that tracks botnets), the Vienna University of Technology, University of Mannheim, University of Bonn, and the University of Washington to coordinate the takedown of the P2P channels. The operation was known as Operation b49. However, those whose computers were compromised were not notified and presumably, not remedied. Bots continue to make requests to the pre-programmed locations, get no response, and consequently do not anything more. The Waledac botnet master may, however, set up new C&Cs for the botnet, and then issue new instructions to the compromised computers.

---

[89] Stewart, J. "Protocols and Encryption of the Storm Botnet" Blackhat Computer Security Conference available at https://www.blackhat.com/.../BH_US_08_Stewart_Protocols_of_the_Storm.pdg (last accessed June 25, 2010).
[90] Russian Business Network "New and Improved Storm Botnet for 2008" available at http://rbnexploit.blogspot.com/.../rbn-new-and-improved-storm-botnet-for.html (last accessed June 25, 2010). *See also* Vamosi, R. "FBI Warns of New Storm Worm Variant" (2008) available at http://new.cnet.com/8301-1009_3-10002760-83.html (last accessed June 24, 2010).
[91] *Microsoft Corporation v. John Does 1027*, Controlling a Computer Botnet Thereby Injuring Microsoft and Its Customers, (Feb. 22, 2010) United States District Court for the State of Victoria, Civil Action 1:10 cv 156 (LMB/JFA).

3.6.5 Mariposa

The Mariposa botnet was used to send spam and to steal username and passwords for financial institutions. The Mariposa botnet was investigated by the Mariposa Working Group (MWG) which comprised security researchers from universities, private corporations (Defence Intelligence, Georgia Tech Information Security Center, and Panda Labs Security), and the relevant DNS providers and ISPs. [92]

The researchers used honeypots to collect information about the botnet. Once this information had been compiled, the researchers' goals were to infiltrate the botnet, gain control and identify the botnet master(s).

The Mariposa botnet ran its C&C from domain name pages in a fast flux rotation in a similar fashion to Torpig and Waledac. Unlike Torpig and Waledac, there were no P2P or rootkit alternatives for the C&C. MWG was able to infiltrate and take over the botnet and changed the DNS records such that the botnet was unable to connect to the C&C. The botnet masters used virtual private network services (VPN) to prevent traceback. This allowed the botnet masters to remain anonymous. On one occasion, however, the main botnet master, Netkairo from Spain, accessed the botnet without using VPN. This one slipup enabled MWG to provide sufficient information to law enforcement agencies in the US who contacted their colleagues in Spain, which were able to identify and arrest Netkairo.

It was revealed that the Mariposa botnet connected to 12 million compromised computers. Parts of Mariposa were rented to other criminals for theft of confidential credentials, for adware, and click fraud. Financial gain was the motive behind the use of Mariposa. Law enforcement agency investigations revealed that several botnet master(s) were involved forming a criminal gang known as Días de Pesadilla Team (DDP team).[93] Three botnet masters were arrested in February, 2010 by the Spanish Civil Guard.

MWG found the DDP team had data relating to over 800 000 users spread over 180 countries. In addition to installing adware for an affiliate fee, the Mariposa botnet was programmed to steal credit card information which was then sold to other criminals. The DDP team also stole directly from bank accounts. The money was laundered through online poker activities and by

[92] Quarterly Report PandaLabs (January-March 2010) available at http://www.pandasecurity.com/img/enc/Quarterly_Report_Pandalabs_Q1_2010.pdf (last accessed June 24, 2010).
[93] In English this translates to Nightmare Days.

using money mules. It is estimated that fraud losses and damages were in the millions. Several counts of fraud charges were brought against the members of DDP. These botnet masters will not, however, be charged with any form of unauthorized access or modification of a computer because Spain, although a signatory to the *Cybercrime Convention*, has yet to ratify it. The *Cybercrime Convention* will be considered in **Chapter 5**.

As at the end of June 2010, the investigation of the DDP was ongoing and there have been claims that the botnet has resumed its functions.[94]

3.6.6 Mega-D

The Mega-D botnet is reported to be a spam botnet.[95] The structural composition of the Mega-D botnet is not as sophisticated as the Torpig, Waledac, and Mariposa botnets by virtue of the fact that its C&C servers depended entirely on the HTTP protocol and did not contain any fall-back channels.[96]

However, like the other previously examined botnets, Mega-D utilized many C&C servers which were rotated through IP addresses and domain names and contained pre-generated domains embedded into the bot code.[97] If the primary C&C server failed (e.g. because the registry entry was removed by the domain name registrar), Mega-D was capable of generating one new C&C domain location per day. As with many botnets, botnet masters do not register all of the domain names that are embedded into their programs perhaps as a cost-reduction method. They only register new domains when necessary. Once researchers at FireEye had identified the 32 unregistered domain names embedded into the botnet, they were therefore able to effectively block their use by the botnet-master by registering each of the names themselves.[98]

The researchers also identified the active domain names that had been previously registered by the botnet master and were able to contact the relevant Internet service providers and domain name providers requesting that they de-register the domain names and IP addresses. All of the

---

[94] 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).
[95] M86 Security Labs, "Mega-D Accounts for 32% of Spam" (2008) available at http://www.m86security.com/TRACE/traceitem.asp?article=510 (last accessed December 12, 2010).
[96] Stewart, J., "Mega-D/Mega-D Trojan Analysis," (2008) Secure Works available at http://www.secureworks.com/research/threats/Mega-D/ (last accessed December 12, 2010).
[97] Lin, P., "Anatomy of the Mega-D Takedown" (December, 2009) Network Security, pages 4-7.
[98] A list of the domain names of migrating C&C servers is provided by FireEye including many domain names ending in .net, .com, .kz, .biz, .net, and .org. Lin, note 102 above, page 5.

C&C servers had to be taken down at the same time in order to prevent the botnet from recovering.[99] Once all of the known botnet-master registered domain names were removed, and all of the known botnet-master related IP-addresses were disconnected, each bot would continue to go through its pre-programmed list of fall-back C&C sources, eventually coming to a domain name that the botnet master had not registered. As FireEye had registered such domains all Mega-D botnet traffic could then be directed to the Shadowserver sinkhole server.

3.7 THEORETICAL FRAMEWORK

Not only do the liberal features of the Internet make it vulnerable to use by the government and commercial parties as seen in **Chapter 2**, but also to that of organized crime. Cybercriminals are not merely aided by the features and technologies of the Internet, cybercriminals control a substantial part of the Internet's architecture through botnets. This control of the Internet raises an interesting question within Lessig's model in terms that the role of law. The law could directly regulate individual behaviour through enacting of criminal provisions followed by successful investigations and prosecutions of botnet masters. As will be demonstrated in the next three chapters, this approach will prove ineffective. The more effective approach as will be seen in **Chapters 7 and 8** will be to indirectly regulate the architecture, whether this is through legislative provisions or a more soft law approach as seen in self-regulated industry codes of conduct. The end goal is not to merely disrupt the model of distribution but the more difficult task of stripping control of the architecture away from cybercriminals. The only successful way to assert control over the architecture will involve a complex strategy drawing on connectivity enablers, financial markets, law enforcement, security experts, universities, governments, key industry stakeholders and self-help security communities. This is elaborated further in **Chapters 8 and 9**.

3.8 CONCLUDING REMARKS

This chapter explored key components of botnets and the botnet industry. It was demonstrated that botnet masters exploit vulnerabilities on networks and web browsers in order to compromise computers. It was additionally seen that security products such as anti-virus, anti-spyware and firewalls, no matter how up-to-date, cannot provide an entirely reliable shield

[99] There were four C & C servers, however, that were not removed in a timely fashion as of December, 2009. FireEye lists them as 98.126.17.114, 64.202.189.170, 98.126.44.146, and 62.90.134.24. As of November 12, 2010 these servers have been removed from the Internet.

against bot acquisition, because they cannot detect bots that utilise as-yet undetected vulnerabilities. This brings into question the ability of technology to act as a deterrent to a botnet master. Many botnets are used to perform acts that have a detrimental effect on organisations and individuals, and, in particular, to launch denial of service attacks, send spam and to assist in the performance of financial fraud, identity fraud and in extreme cases identity theft.. While not all botnet masters are motivated by financial gain, the more advanced botnet structures such as those seen with Torpig, Waledac and Mariposa are operated by professionals motivated by financial gain.[100]

The remaining chapters in this thesis will continually refer to the concepts articulated in this chapter. For this reason, this chapter forms the foundation for all subsequent chapters.

[100] Ianelli, N. and Hackworth, A., "Botnets as a Vehicle of Online Crime" Ddec. 1 2005 US CERT

Chapter 4

THE AUSTRALIAN CRIMINAL LAW LANDSCAPE FOR BOTNET-RELATED PROSECUTIONS

Table of Contents

4.0 AIMS OF CHAPTER

This chapter further elaborates on the legal limitations of investigating and prosecuting botnet masters. The chapter *assumes* that the generic legal and technical challenges as will be demonstrated in **Chapter 6** have been overcome and that prosecution of a botnet master is possible. This chapter, therefore, analyses the national criminal law framework in Australia relevant to botnets. While there are many other types of offences that could conceivably fall within the Australian criminal framework, only the offences that an accused would mostly likely be charged with will be considered. The most relevant offences include: unauthorised access, modification or impairment to data or electronic communications; dishonest use of a computer; conspiracy (to defraud); fraud and aiding and abetting. It will be argued that the current state of Australian criminal law is sufficient to prosecute a botnet master. The real challenge as seen in **Chapter 3** and as will be seen in **Chapter 6** stems from generic challenges and obfuscation crime tools.

The legal analysis is limited to relevant Commonwealth provisions and does not include an assessment of the criminal provisions found in each of the Australian State's criminal statutes[1]. This is due to the fact that the Commonwealth provisions related to cybercrime are the direct result of the promulgation of the Model Criminal Code (Model Code). The Model Code contains a series of chapters dedicated to specific topics in need of legal reform and harmonisation between States. Chapter 4 of the Model Code, for example, covers damages and computer offences. Typically, the Model Code suggests reforms to the law which is often, but not always, later adopted by the States and Territories. After a Model Code is introduced, Commonwealth and State provisions are often either introduced or amended in order to harmonise the law between States. Thus, in many situations, the Commonwealth provisions are substantially similar to those provisions from those of an individual state. Following the analysis of the national criminal legal framework, one of the few publicly available cases where a botnet master was tried on criminal charges, *R. v. Walker*, is used as a case study to better understand applicable Australian provisions and to reveal deficiencies in prosecution. The last section

[1] Most states have authoritative textbooks and materials related to each territory. For instance, a good examination of the criminal laws of New South Wales is found in Brown, D., Farrier, D., Egger, S., McNamara, L. and Steele, A., *Criminal Laws: Materials and Commentary on Criminal Law and Process of New South Wales 4th ed.* (The Federation Press: 2006).

examines the lack of exemptions to computer offences that hinder security research and provides a series of recommendations for law reform.

While suggestions are made to improve the effectiveness of law enforcement, this chapter highlights the overall proposition of this thesis that the law will play a limited role in the fight against botnets and the malware industry. Suggestions for legal reform to improve the ability to combat botnets will be made. **Chapters 7 and 8** examine methods which will likely have a greater impact in combating botnets and the resulting harms. The international criminal legal framework will be considered in **Chapter 5**.

4.1 PRE-BOTNET AND POST-BOTNET CRIMES

As a federation, the Australian framework is complicated with both federal and state / territory criminal legislation in the area. In an attempt to harmonize existing computer crimes offences, the Attorney-General issued a *Model Criminal Code* (Model Code). This Model Code led to the passing of a number of amendments to the *Crimes Act 1914 (Cth)*. New South Wales, the Australian Capital Territory, Victoria, the Northern Territory and South Australia all contain similar provisions based on the Model Code. Tasmania, Queensland, and Western Australia remain the only states to yet implement the Model Code.[2]

The *Cybercrime Act 2001 (Cth) r*epresents the foremost change to the law regarding computer related offences. This federal legislation amended the *Criminal Code Act 1995 (Cth)*, the *Crimes Act 1914 (Cth)* and the *Customs Act 1901 (Cth)*. The most relevant parts of the federal *Criminal Code Act* are found in Part 10.6 which looks at offences committed through telecommunication services, Part 10.7 which broadly addresses computer offences, Part 7.3 which deals with fraudulent conduct, and Part 10.8 which deals expressly with financial information offences. Relevant provisions from both the *Criminal Code 1995(Cth)*[3] as well as those found in many State criminal codes address actions which could be categorised broadly as computer offences. Such actions might include unauthorised access, impairment and modification of data or electronic communications, and dishonest use of personal information. Whether an offence is committed generally depends on whether the person had the intent to commit an offence or to cause harm, but in some cases recklessness is sufficient. This is examined in greater detail in the sections that follow.

---

[2] *Criminal Code 1922* (Tasmania), *Criminal Code 1899* (Queensland), *Criminal Code 1902* (Western Australia)
[3] Hereinafter referred to as the *CC*.

As seen in **Chapters 1** and **3**, a botnet may be used to commit a variety of crimes such as financial fraud, click fraud (general fraud), distribution of child pornography, identity theft, unauthorised access and modification of data, spam and denial of service attacks. This does not mean, however, that the botnet herder is necessarily the perpetrator of such crimes. In the Mariposa botnet investigation as seen in **Chapter 3**, the botnet herders perpetrated a number of crimes through the use of their botnet. The Spanish authorities, however, will likely only charge the botnet herders with fraud as Spain has not passed legislation that prohibits unauthorised use of computers. In the Mariposa instance, the botnet herders used their botnets to commit fraud, steal identities, and to send spam. Here the botnet herders *directly* committed a number of crimes. Many botnet herders, however, merely rent their botnets out to others. In the latter instance, customers use the botnet to commit crimes such as steal banking passwords to commit fraud, to launch a DDoS, or to send spam containing links to the sale of illegal drugs and child pornography. Depending on the circumstance, a botnet herder could be charged with a number of crimes for hiring out a botnet.

Many botnet herders are likely to commit a common offence – unauthorised access and/or modification to a computer system. There are, however, a few instances where one could have a botnet and conceivably not commit an offence. This will be examined in **section 4.4)**. Procuring a computer to become part of a botnet most likely involves unauthorised access and modification to a computer, and could potentially involve dishonest use of a computer as well as misleading and deceptive conduct. Subsequent acts resulting from the use of a botnet, such as a DDoS attack on a website, will attract related penalties that address unauthorised modification or impairment of data or electronic communications. Applicable criminal provisions relate to the establishment of a botnet by acquiring zombie computers, and provisions that might apply once the botnet is established and used to commit subsequent crimes. I will refer to these as pre-botnet crimes and post-botnet crimes as explored below.[4]

Pre-botnet crimes refer to the process (where criminal) of acquiring bots to become part of a botnet. How to build a botnet was explored in **Chapter 3** where it was seen that bot acquisition often involves a form of deceptive behaviour and/or unauthorised access to a user's computer which is criminalised as will be seen below. **Post-botnet crimes** refer to criminal acts performed with a botnet.

[4] This is my own categorisation of botnet-related crimes.

Pre-botnet crimes are examined first and potentially entail unauthorised access of a computer system or data; producing, supplying or obtaining data with intent to commit an offence, as well as misleading and deceptive conduct. The New Zealand court decision against botnet master, Owen Walker, is explored in **section 4.5.** The case of *R. v. Walker* highlights a number of issues surrounding prosecution of a botnet master and provides a useful context for which to consider the legal framework applicable to botnets.

Last, post-botnet crimes are considered. Spam botnets may be used to sell illegal drugs, provide links to child pornography and link to other types of illegal activities. Trojans may be installed via a botnet which then steals usernames and passwords in order to perpetrate financial fraud and identity theft. Botnets are also used to disseminate child pornography. Botnets are also used to commit click-fraud. While these activities are illegal, the potential list of post-botnet crimes is practically endless. While botnets are used to commit such crimes, they are often rented out for this purpose. The botnet master himself or herself is often not the main perpetrator of the crime, but merely assists with its commission. For this reason, the analysis of post-botnet crimes will be limited to the most prevalent forms which include unauthorised modification or impairment to data or electronic communications, fraud, conspiracy (to defraud) and 'aiding and abetting' in a crime. **Figure 4(A)** on the following page maps out pre-botnet and post-botnet offences.

Figure 4(A): Table Outlining Pre-Botnet and Post-Botnet Offences

PRE-BOTNET OFFENCES **(How to Build a Botnet)**	**POST-BOTNET OFFENCES** **(What are Botnets Used For)**
Unauthorised Access and/or Modification of Data (s.477.1, s.477.2, s.478.1 of *CC*)	**Unauthorised Modification to Data or Impairment of Electronic Communications (s.477.1, s.477.2, s.477.3, s. 478.1, s.478.2, and s. 478.3 of *CC*).**
	Fraud (Divisions 133, 134 and 135 *CC*) and Conspiracy to Defraud (s.135.4 *CC*)
Misleading and Deceptive Conduct ***s.52 Trades Practices Act***	**Aiding and Abetting in the Commission of a Crime (s.11.2 CC) and Conspiracy to Commit an Offence (s.11.5 *CC*)**
Producing, supplying or obtaining data with intent to commit an offence (s. 478.4 *CC*).	**Other offences not considered in this chapter: unsolicited emails, distribution of child pornography, illicit sale of drugs, illicit sale of counterfeit goods, trespass, fraud, identity theft, click-fraud, trade secret theft, and espionage.**

4.2 PRE-BOTNET CRIMES

4.2.1 Unauthorised Access, Modification or Impairment to Data

The user of computer offences to capture the actions of a botnet master is not fully evident either in a reading of the legislation, the Model Code notes, the bills, or subsequent caselaw interpreting the provisions (as no botnet masters have been prosecuted in Australia). I will examine each of the provisions relevant to bot acquisition (pre-botnet crime). There may be some overlap with post-botnet crimes in this section in order to fully explicate the importance of criminalising bot acquisition. The following analysis explains the provisions in the table.

The Commonwealth provisions make it illegal to access or modify data, or impair electronic communications without authorisation. These are referred to as computer offences which are outlined in Part 10.7 of the *Criminal Code 1995 (Cth)*. The CC is divided into serious computer offences which attract a penalty of up to 10 years imprisonment (Division 477.1 "Serious Computer Offences"), and other computer offences which attract a penalty of up to 2 years imprisonment (Division 477.2 "Unauthorised Modification of Data to Cause Impairment", Division 477.3 "Unauthorised Impairment of Electronic Communication", and Divisions 478 "Other Computer Offences").

Serious computer offences in s.477.1 require three elements to be met. First, a carriage service must be used in the commission of the offence (Eg. the Internet). Second, the person must knowingly access, modify or impair data in an unauthorised manner. Accidental access or modification of data would not be caught under this provision. Third, there must be intent to commit a serious offence. "Serious offence" is defined in s.477.1(9) as "punishable by imprisonment for life or a period of 5 or more years." As the Model Code notes, "It is, essentially a specialised offence of attempt." [5] The use of a botnet to capture usernames and passwords which are then used to obtain credit card numbers or to transfer funds fraudulently. Obtaining credit card numbers with the intent to later use them in a fraudulent matter would be caught under s.480.4 which addresses dishonestly obtaining or dealing in personal financial information. This attracts a penalty of 5 years. Mere possession or control of financial

[5] *Model Criminal Code*, Chapter 4 (January 2001), page 104.

information (Eg. credit card numbers) through dishonest means where the information had *not* been used to commit a crime only attracts a penalty of 3 years (s.480.5). In this latter instance, if a botnet master accidently obtained bank account numbers and credit card details through a keylogging program (Eg. was really searching for World of Witchcraft passwords) with no intent of using the banking details, there would be no serious offence. In the case of a fraudulent transfer of funds from a user's bank account to an unauthorised account, Divisions 134 and 135 which deal with fraud, would apply and attract a penalty in most instances ranging from 5 to 10 years. This activity would be a serious offence. Where banking details or credit card numbers are captured with an intent to use them in a fraudulent manner, s.477.1 is triggered. Section 477.1 offences attract a penalty that does not exceed the penalty of the serious offence (s.4.77.1(6)). For example, if the fraudulent activity conducted through the use of a botnet attracted 10 years of imprisonment, the court could not add 2 more years to the sentence for having modified data in an unauthorised manner. The facilitation of the commission of a serious offence through accessing, modifying or impairing data is also caught under s.477.1(4)(c). Where a botnet master knowingly rents a botnet to someone who will use the botnet to fraudulently steal bank funds, this could be construed as facilitation in the commission of a serious offence. As will be seen later, this could also be construed more generally as conspiracy to defraud or aiding and abetting in the commission of a crime.

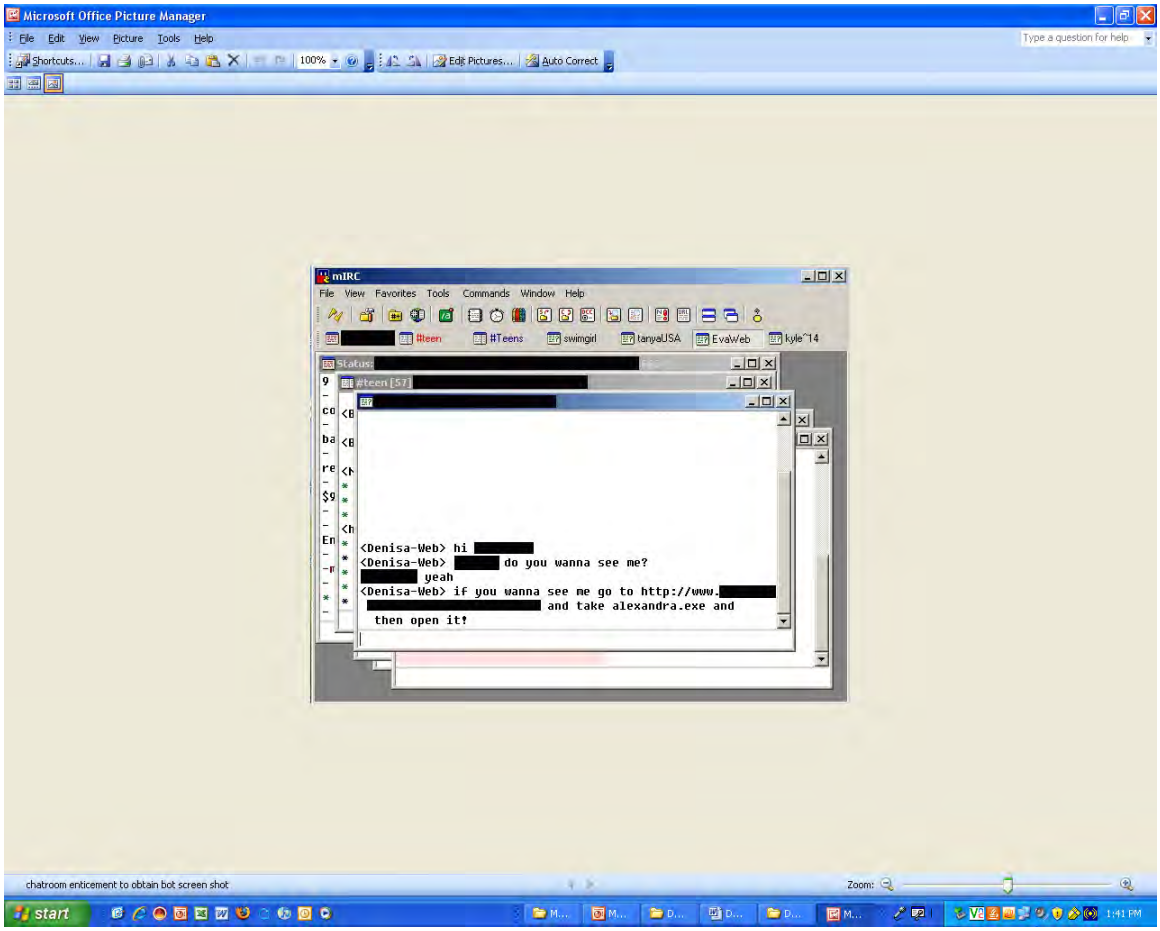
Sections 477.2 ("unauthorised modification of data to cause impairment") and 477.3 ("unauthorised impairment to electronic communications") involve situations where there is no intent to commit a serious offence. Section 477.3, however, is aimed at the use of a botnet to perform a denial of service attack and is, therefore, considered a post-botnet crime (**section 4.3.1**). These sections differ from the "serious offence" provision in several ways. First, there is no need to demonstrate intent to commit a serious offence. The provisions apply to a person who knowingly or recklessly causes modification to data which, in turn, impairs access to, or the reliability, security or operation of a Commonwealth computer or electronic communication or uses a carriage service to do so. In acquiring a bot to form part of a botnet, an unwanted software program is downloaded onto the user's computer. This would most likely constitute unauthorised access and modification but would not necessarily impair the data. Impairment of data (s.477.2) or impairment of an electronic communication (s.477.3) is required for these provisions to apply. It is not helpful that "unauthorised access, modification or impairment" is defined in s.476.2 in a manner which merely repeats the use of the terms "modification" and "impairment" without defining these terms. There is no reported case in Australia of

unauthorised access, modification or impairment to data or electronic communications. The *Model Criminal Code* provides some assistance by explaining that the impairment to electronic communications provision is meant to apply to a denial of service attack.[6] Where a botnet master uses their botnet to perform a denial of service attack, s.477.3 would apply. Where a botnet master rents their botnet to someone, the provision is not triggered. In this instance, the prosecution could use s.477.1(4)(d) where there is facilitation to commit a serious offence, or a more general provision of aiding and abetting a crime which will be explored in **section 4.3.4.**

Most of these provisions could be considered, depending on the context, as offences that could apply to pre-botnet crimes, and in some instances as will be seen in **section 4.3**, post-botnet crimes as well. The provisions are perhaps best considered in the context of an example. **Chapter 3** demonstrated many methods of how a computer becomes part of a botnet such as a user clicking on a link which they believe to be related to a news story, only to trigger a software program (or several software programs) that infect his computer rendering it compromised. One common method is to create a fictitious person in a chatroom. The fictitious person is really just a computer program (robot) which will respond in a set pattern of language and will eventually ask if the other person would like to see a photo of himself or herself, and if so, click here. The user clicks on the link (Eg. Often an .exe file) to retrieve a photo and a number of software programs are installed onto the user's system. The fictitious person (robot) typically is a worm programmed to initiate chat sessions with many people infecting machines one after another. Once the worm starts to infect a machine and make it part of a botnet it keeps on going and infecting more machines. Worms perpetually self-propagate. The botnet, therefore, continues to grow in size and requires minimal effort to build. Some researchers have noted that it takes only two days to build a botnet.[7] Below in **Figure 4(B)** is an example of a thread of conversation in a chatroom where the link is designed for bot acquisition.

[6] MCC, note 5 above.
[7] 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.htmlhttp://blog.spywareguide.com/2006/06/building_a_botnet_empire_in_tw_1.html (last accessed May 31, 2010). *See* note 10 below.

Figure 4(B) Executable Code in Chatroom Triggering Bot[8]



The screen is paraphrased as follows:

> Denisa> hi
>
> Denisa> do you wanna see me?
>
> Victime> yeah
>
> Denisa> if you waana see me to go http://www_____ and take Alexandra.exe and then open it!

Using the above example of chatroom initiated bot acquisition, the first question to answer is whether there has been any form of *unauthorised* access, modification or impairment. The *Criminal Code* does not define what is meant by "unauthorised". There is no caselaw on what is meant by unauthorised access, modification or impairment of data in *this type of context*. The

[8] 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

caselaw on unauthorised computer offences is dominated by unlawful employee access to databases while there is little caselaw where "hackers" were involved. For example, in *Johnston v Commissioner of Police*[9] addresses the misconduct of junior police officers accessing an information system without authorisation. In *Regan Gerard Gilmour v Director of Public Prosecutions (Commonwealth)*[10] an employee inserted data into a Commonwealth computer without authorisation. The decision of *Salter v DPP*[11] also involved unauthorised access of an employee to a police database. Justice Hulme referred to the 1993 decision of *Gilmour v Director of Public Prosecutions*[12] where Hayne J stated, "In the case of a hacker it will be clear that he has no authority to enter the system". *R v Stevens*[13] is one of the few publicly available decisions where an employee has not been involved. In this case the accused hacked into the ISP Ausnet, registered a fake account, and obtained credit card information of some of Ausnet's clients. Stevens made public his hack (including a few credit card numbers) to demonstrate the severe lack of security with Ausnet servers and forwarded the information to a journalist. He did not use the credit cards that he obtained; again, the purpose of the hack was to expose lackadaisical security practices. Some customers later complained that their credit cards were used abroad without authorisation. The decision does not, however, explore whether such credit cards were used abroad due to Steven's disclosure of the numbers or due to someone else having obtained such numbers as the result of Ausnet's insecure data storage practices. No botnets, worms, viruses, Trojan or any modern crime tools were used in any of the Australian cases involving unauthorised access, modification or impairment to data or electronic communications.

The lack of prosecutions of botnet masters for bot acquisition activities is not due to loopholes in the *Criminal Code* but is likely as the result of some of the generic challenges as will be explored in **Chapter 6:** lack of police resources and training, traceback issues, digital forensics, volatility of evidence, and jurisdiction. Other reasons may include lack of political will to tackle this area of cybercrime and an underreporting of unauthorised incidents to police. There is potentially, however, one exception to the "computer offences" where prosecution may not be possible. In the chatroom example, the user will click on 'alexandra.exe' and as a result many software programs will be unknowingly installed onto the user's computer. The computer has been compromised. The user was certainly not notified ahead of time of what would happen to their computer if they clicked on the link; while a photo of "Alexandra" may have been opened, the

[9] [2007] NSWIR Comm 73.
[10] [1996] NSWSC 55.
[11] [2008]NSWSC 1325.
[12] (1995) 43 NSWLR 243.
[13] [1999] NSWCCA 69.

installation of unwanted and unknown software was deceptive and misleading.[14] The issue of consent and informed consent is examined further in **sections 4.4** and **4.7.4.**

4.2.2 Possession, Control or Supply of Data

Mere possession, control or supply of data with intent to commit a computer offence such as that found in s.478.3 and s.478.4 (supply) of the *CC* is prohibited. For example, if a botnet herder in Australia had collected usernames and passwords from third party computers with intent to use them in future fraudulent activity, they would be caught under s.478.3 of the *CC*. This is more along the lines of a pre-meditated post-botnet crime. It remains entirely uncertain as to whether this or any provision would prohibit the development and possession of a computer worm which would be used to acquire bots without the person charged actually having used the worm. The provision applies irrespective of whether the data has been used in an illegal manner such as fraud. There is no caselaw on s.478.3 or s.478.4 of the *CC*.[15]

The provision could also potentially apply to a botnet master who rents out their botnet for illegal use whereby the botnet herder supplies someone with a botnet . There are several provisions which could apply to a botnet master who hires out his botnet for use. Conspiracy and aiding and abetting could apply to the hiring out of a botnets. Much would be fact dependent. Botnets may be hired out to others for use in the same fashion that a person rents a car. The salesperson at the rental car company would not know the customer's planned use of the car. It could be for use in an armed robbery or a tourist destination. The same cannot be said for a botnet master. It is difficult to envisage a situation whereby a botnet is hired out for legal use. The possibility of legal use of a botnet, *albeit quite remote*, is explored in **section 4.4**. By and large, botnets are designed and used for crime. It would be difficult to prove, therefore, why possession, control of supply of data provisions (s.478.3 and 478.4) should not apply to a botnet master even in the event where the botnet master does not have actual knowledge that the customer intends to commit a crime. With the rental car salesman, there is only a small possibility that a car will be used in the commission of a crime. The primary use of most rental cars is not for crime. The primary use of botnets is for illicit activity. In the case of hiring out a botnet, it is *probable* that the botnet will be used in the facilitation of a crime. This is more a case

[14] It would be possible, however, to imagine a scenario where the user must consent to a set of terms and conditions which explained that certain software programs would be downloaded onto their computer and where their computer would become part of a botnet. This, however, would be a rare example.
[15] Databases from AustLII , LexisNexis Australia, and FirstPoint were used.

of wilful blindness. Wilful blindness should not inhibit a successful prosecution for the supply of a botnet but, as there are no precedents applying wilful blindness to botnets, the outcome could be different if there were a court case on point.

Where a botnet is hired out and a criminal act is committed with the botnet, this is more likely to be in the area of conspiracy and aiding and abetting in the commission of a crime. To use another comparison, a customer hires a limousine complete with driver, hops into the car with a disguise and a visible gun. The limousine driver then takes the customer to the bank, and waits for the customer to commit armed robbery, and drives the customer knowingly to his next location. Here, we are into the territory of aiding and abetting in the commission of a crime. In parallel, where a botnet master hires out the use of the botnet and then assists the customer in its illicit usage such as performing a denial of service attack or stealing financial information, a crime is clearly committed. Post-botnet crimes such as conspiracy to commit a crime, fraud, conspiracy to defraud, and aiding and abetting are explored in **sections 4.3**.

4.2.3 Misleading and Deceptive Conduct

The methods used to acquire bots often involve practices that are both misleading and deceptive. Untruthful and misleading emails might be sent luring the user to click on an attachment or link. When the user does so, a number of programs are automatically downloaded onto their computer. **Figure 4(B)** above displayed an example of such chatroom dialogue where the bot posed as someone interested in starting up a romance with the end-user. The end-user was provided with a link that was alleged to provide a photo of the interested party. When the end-user clicked on the link a number of adware and spyware applications were unknowingly downloaded onto the user's system (Eg. Dollarrevenue). One of these applications compromised the user's computer rendering it part of a botnet.

The *Fair Trading Act 1987* (NSW)[16] and the *Trade Practices Act 1974* (Cth)[17] prohibit misleading and deceptive conduct.[18] On January 1, 2011 the *TPA* was renamed the *Competition and Consumers Act 2010* (Cth).[19] For the purpose of the analysis below, reference will be made to the *TPA* and caselaw referring to the *TPA*. Section 52 of the *TPA* prohibits misleading and deceptive

[16] Hereinafter *FTA*.
[17] Hereinafter *TPA*.
[18] For a comprehensive overview of the FTA and TPA *see* Corones, S and Clarke, P. *Consumer Protection and Product Liability Law 3rd3ed* (Thomson Lawbook, 2008).
[19] Hereinafter *CCA*.

conduct of corporations engaged in trade and commerce whereas an individual's conduct is generally thought of as falling under State legislation such as the *FTA*. The *TPA* extends to individuals where the conduct involves the "use of postal, telegraphic or telephonic services"(s.6(3)). The full federal court of appeal in *ACCC v. Henry Kayes*[20] extended the scope of the act to include conduct of individuals using the radio and Internet. That a botnet master is not a corporation is, therefore, not a factor in applying the *TPA* (or *FTA*) providing the Internet or telephone is used. For the purpose of this thesis, only provisions and caselaw from the *TPA* will be examined.

In order for s52 to apply, a person's actions must to considered to be "in trade or commerce", must give rise to financial gain or profit and be misleading or deceptive to a consumer.[21] The High Court of Australia in *Concrete Constructions (NSW) v. Nelson*[22] interpreted "in trade and commerce" broadly stating that "trade or commerce are not terms of art but are terms of common knowledge of the widest import."[23] In subsequent caselaw the Australian courts have interpreted "in trade and commerce" to apply to a wide variety of contexts, including individuals on television programs promoting millionaire services[24] and personal websites and blogs.[25] Providing that there is financial gain or where the individual or corporation has profited in some manner, the trade and commerce component is easily met.[26]

Misleading and deceptive practice has been given a broad construction. Section 52 can be applied:

- "By business to protect their commercial interests, as well as by consumers;
- By individuals in relation to commercial transaction, as well as in relation to consumer transaction;
- In relation to private communications, as well as communications directed towards the public;

---

[20] *ACCC v. Henry Kaye* [2004] FCA 1363.
[21] False representations are also prohibited under s.53 of the *TPA* where goods or services are falsely represented to be of a certain quality or quantity. The same elements must be proven s.53 as for s.52 with the only difference being one of false representation versus misleading and deceptive conduct.
[22] Mason, Deane, Dawson and Gaudron JJ in *Concrete Constructions (NSW) Pty Ltd v. Nelson* [1990] HCA 17 at 6.
[23] Above.
[24] *ACCC v. Channel 7 Brisbane* [HCA] 19
[25] *Seven Network Ltd. V. News Interactive Pty Ltd* [2004] FCA 1047
[26] *Pilmer v Roberts* (1997) 80 FCR 303. This case involved deceptive statements in a public lecture by a Christian Minister, Professor Pilmer. Because the audience members could purchase a copy of the lecture, the court ruled that Professor Pilmer had profited (however meagre the amount) from the sale of the lecture and his conduct could, therefore, be said to fall within "trade and commerce".

- To protect the public interest as well as the interests of private individuals;
- By individuals, or businesses, who suffer no loss or damage as a result of misleading conduct as well as by those who do;
- In private proceedings as well as in proceedings brought by the ACCC."[27]

The *TPA* would apply to conduct where a botnet master uses false representations or uses methods that are misleading and deceptive such as seen in **Figure 4(B) above**. The fact that a botnet master is not a corporation and is not engaged in online business transactions does not bar the application of the *TPA*.

4.3 POST-BOTNET CRIMES

4.3.1 Unauthorised Access, Modification or Impairment

Pre-botnet crimes were concerned with unauthorised access. Post-botnet crimes are concerned with modification and impairment of data and electronic communications. For example, a denial of service attack would be an impairment to electronic communications under s.477.3 of the *CC*. Causing a Trojan or worm to be installed onto a computer would constitute unauthorised modification to data, and possibly impairment as well if the functionality of the computer or data was compromised.

The computer offences provisions are sufficiently broad so as to capture post-botnet crimes. In spite of this, there is no caselaw that addresses modification or impairment of data (s. 477.1 or 477.2) or impairment of electronic communications (s.477.3). According to the Australian High Tech Crime Centre, we know that in 2005 denial of service attacks constituted 22% of cybercrime cases costing $8.9 million and over 63% of cybercrime cases fell in the category of virus/worm/Trojan costing $2.7 million.[28] Again, the lack of caselaw may be due to most cases being settled or it may be the case that there simply have not been any successful investigations of botnet masters.

[27] Corones and Clarke, note 18 above.
[28] 2005 Australian Computer Crime and Security Survey. The survey included questioning of 110 organisations in Australia. It is available at http://www.aic.gov.au/statistics/hightech/cybercrime.aspx (last accessed May 24, 2010).

4.3.2 Aiding and Abetting in the Commission of a Crime

Both conspiracy and aiding and abetting are considered to fall within the doctrine of "law of extended common purpose liability" which is considered below. The doctrine considers in what circumstances and to what extent should those involved in a crime be held accountable inspite of the fact that they were not the actual person to commit the crime. For example, the driver of a car in an armed robbery or the person who held down the victim while another person raped or murdered the victim could be prosecuted under the extended common purpose liability.

The High Court of Australia has on several occasions considered the law of extended common purpose liability and has given specific scope to what is meant of s11.2 of the *CC* which makes it an offence to aid or abet the commission of a crime. The High Court of Australia in *Clayton v. R*[29] confirmed the decisions of *McAuliffe*[30] and *Gillard* [31]stating that, "If a party to a joint criminal enterprise foresees the possibility that another might be assaulted with intention to kill or cause really serious injury to that person, and despite that foresight, continues to participate in the venture, the criminal culpability lies in the continued participation in the join enterprise with the necessary foresight." The High Court of Australia places emphasis on continuing to play a role in a crime once it is foreseeable that a crime will be committed. *Clayton, McAuliffe* and *Gillard* were cases that all involved murders where the accused played a role in the murders such as drove the getaway vehicle but did not actually kill the victim.

In *Gillard* the accused stole and drove a van at the request of a man named Preston. Preston entered the van in disguise and had a gun. Preston had the accused phone a shop where the intended victim worked to see if he was indeed there. The accused drove Preston to the shop, watched Preston enter the shop, Preston then shot two men and injured another, and the accused drove Preston to another destination. After the incident the accused disposed of the van. The court found the accused guilty of murder by his complicit and continued cooperation with the accused due to the foreseeability that Preston would kill the individuals at the shop. The court stated that, "The accused is held criminally responsible for his or her *continued* participation in a joint enterprise, despite having foreseen the possibility of events turning out as in fact they did. It does not depend upon identifying a coincidence between the wish or

[29] *Clayton v R* [2006] HCA 58
[30] *McAuliffe v The Queen* [1995] 183 CLR 108
[31] *Gillard v R* [2003] HCA 64

agreement of A that an act be done by B and B's doing of that act. The relevant conduct is that of A – in continuing to participate in the venture despite foresight of what may be done by B."[32]

In the botnet instance, where the botnet master hires out a botnet and aids the customer to commit a crime, it is difficult to see why the doctrine of law of extended common purpose liability should not apply. The botnet master has aided and abetted in the commission of a crime. That crime could be fraud, unauthorised access or impairment to a computer, and may even entail distribution of child pornography materials where a botnet is used for this purpose. Many botnets as seen in **Chapter 3** are used to send illegal spam. Often the spam may be selling prescription drugs, pornography and in some instances, child pornography. In this situation, it is somewhat more difficult to ascertain the appropriate scope for aiding and abetting. Certainly the botnet master could be seen as aiding and abetting in the sending of spam, but it would more difficult to stretch this doctrine to a situation where it is foreseeable that the spam is advertising the sale of something that is otherwise illegal such as Viagra without a prescription. The foreseeability of criminal use, however, should address whether there is continual cooperation once someone discovers that the spam is being used to advertise an illegal drug.

4.3.3 Conspiracy to Commit an Offence

Section 11.5 of the *CC* refers to situations where there is conspiracy to commit an offence (punishable by imprisonment for more than 12 months or by a fine of 200 penalty units). Conspiracy will only be relevant to a botnet master in a few instances. Conspiracy requires that there must be an agreement between two or more persons, that the agreement must include intent to commit an offence, and that one of the persons must have committed an overt act that was part of the agreement. For instance, where a botnet master hires out his botnet and services, and there is an agreement that he will technically assist the client in launching a denial of service attack, the first two requirements of conspiracy will have been met. There is no conspiracy, however, where the botnet master hires out the botnet merely with knowledge of the likelihood of criminal use. The denial of service attack must then have been performed by either the client or botnet master to satisfy the third requirement. Conspiracy to defraud is covered by a separate provision, s.135.4 of the *CC* and is explored in **section 4.3.5**.

[32] *Gillard*, note 31 above, paras 117 and 118.

4.3.4 Fraud

Part 7.2 of the CC deals with fraud and is comprised of three divisions: Division 133 (Preliminary), Division 134 (Obtaining property or a financial advantage by deception) and Division 135 (Other offences involving fraudulent conduct). The provisions apply where property or financial advantage is obtained by deception or dishonest means from another person. The definition of 'deception' specifically includes situations where computers or electronic devices are involved.[33] "Dishonesty" is defined as "dishonest according to the standards of ordinary people and known by the defendant to be dishonest according to the standards of original people."[34] Deception and dishonesty are the core mental elements in fraud offences.[35]

Botnet masters often use a botnet to download Trojans onto computers which capture usernames, passwords and credit card details which the botnet master might then use to purchase goods, steal money, or might use details of someone's identity to apply for services (ie. identity theft). The provisions on fraud are sufficiently broad so as to include situations where botnet masters obtain credit card details or usernames and passwords to steal funds.

4.3.5 Conspiracy to Defraud

Conspiracy to defraud under s.135.4 of the *CC* is a separate provision from the generic conspiracy provision found in s.11.5. Conspiracy to defraud has similar elements where a person must conspire with one or more person with the intent to commit an offence In this case the offence is specific – intention of dishonestly obtaining a gain or causing a loss to a third person. Absent is the requirement that the offence be carried out by one of the parties which is dissimilar to the generic offence found in s. 11.5. The penalty for conspiracy to defraud is 10 years.

A botnet master who conspires with another person to install a Trojan which will steal banking details (usernames, passwords, and banking information) in order to steal money from an

---

[33] S. 133.1 *CC* "deception" means an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes:
(a) A deception as to the intentions of the person using the deception or any other person; and
(b) Conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.

[34] S. 133.1 *CC*.

[35] *See* Steele, A., "New Fraud and Identity-Related Crimes in New South Wales" (2010) Judicial Officers Bulletin 22.3, pages 18-22. *See also* Steel, A., "The Meaning of Dishonesty in Theft" (2009) Common Law World Review; 38(2).

account will be caught by s.135.4 regardless of whether the Trojan was installed and money stolen. An agreement to merely install Trojans which capture keylogging strokes without reference to absconding funds from a third party, however, may not appear to satisfy the requirements of conspiracy to defraud. The High Court of Australia in *The Queen v LK; The Queen v RK*[36] was asked to interpret whether mere recklessness as opposed to an agreement with intent to commit an offence would satisfy the requirements of conspiracy under s.11.5 of the *CC*. The court held the fault element for conspiracy was intention and not recklessness. Under this line of reasoning it would seem that a botnet master would require intent to commit the offence; mere recklessness would not suffice. An agreement to use a botnet to install keylogging Trojans which unbeknownst to the botnet master would be used to commit fraud would likely not satisfy the definition of conspiracy, as the botnet master would have merely been reckless. That said, the installation of a Trojan would still be an offence under the CC (unauthorised access and modification of data). Here intent to commit an offence would easily be met.

4.4 NOT ALL BOTNETS WOULD BE ILLEGAL

Under both the *Convention* and the *CC*, it remains ambiguous whether a person could lawfully build and use a botnet. Most acquisitions of compromised computers are through unauthorised access, dishonest intent, or in a misleading and deceptive fashion. That said, it is possible that a consumer could consent to become part of a botnet. A user may use a website service which requires user consent through agreeing to terms of use. Users do not generally read Terms of Use Agreements. The user clicks on the "I Agree" button only to find several software programs downloaded onto their system. Some of these programs may be malicious in nature, and may include a program that compromises their machine and makes it part of a botnet. The terms of use are almost always worded vaguely and in a confusing matter such that a user would not know that their systems had been compromised and were part of a botnet. Provisions in online terms of use must not use false representations, or be misleading or deceptive.[37] Silence or non-disclosure of terms may lead to misleading and deceptive conduct where the omission to disclose information is deliberate.[38] Even in the event that such terms were defined in detail including information that the user's computer would be used in the commission of crimes, these terms should have to be brought to the express attention of the user by the contractor in a format other than merely pressing the "I Agree" button. In an exceptional case, this could

[36] *The Queen v LK; The Queen v RK* [2010] HCA 17was
[37] *Australian Competition and Consumer Commission v Chen* (2003) 132 FCR 309
[38] *Software Integrators Pty Ltd v Roadrunner Couriers Pty Ltd* (1997) ATPR (Digest) Supreme Court of South Australia.

conceivably be in the format of a compulsory voice clip explaining the provision, or by an email or telephone call to the user to clarify the terms.

Thus if a consumer clicks the "I Agree" button, in most cases consent will be invalid. Of course, a consumer cannot consent to aid and abet in the commission of a crime or illegal act. Any subsequent use of a botnet for an illicit purpose such as sending some spam marketing illicit drugs or a DDoS attack could not be consented to. Consent, however, could be granted for a computer to become a zombie for the use of *lawful* spam distribution. Under Australian law and the *Convention* the mere possession of a botnet, if acquisition is through lawful means and consent obtained, would not criminalised.

4.5 *R V. WALKER*

The case of *R v. Walker* presents an important perspective on a prosecution of a botnet master, particularly as there are so few other examples. As the judge in the case highlights,

> "Mr. Walker developed and used software that enabled him to remotely control infected computers. Collectively, the infected computers formed a robot network, commonly referred to as a bot net. Mr. Walker installed his bot code on tens of thousands of computers. He developed his code so that it could protect itself from discovery, spread automatically and identify and destroy rival bot codes. The code automatically disabled any antivirus software on an infected computer and prevented software from being updated, but in such a way that the computer owner believed the antivirus software he or she had on his or her computer was still working and was successfully installing updates. Another bot code allowed Mr. Walker to operate through other computers as a proxy, making it harder for his activity to be traced back to him." [39]

Walker was brought up on several charges. 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.[40] 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 which is considered as part of the Autism Spectrum.

---

[39] *R. v. Walker* HC HAM CRI2008-0750711 [2008] NZHC 1114 (15 July 2008), page 4
[40] Above, page 37

The judge looked at four factors when deciding how to sentence Owen Walker. First, what was the reason for the crime? The judge accepted that Walker's criminal behavior was motivated by curiosity and an intense interest in computers rather than motivated by criminal intent or malice.[41] The fact that he earned $36 174.64 from illegal activity did not seem to be a factor in the judge's decision. This particular finding is open to criticism. If a person were to break into a shopping mall, and replace all the store signs in the mall with substituted advertisements, one could easily conceive that a person may have done the act out of mischief and curiosity. However, if a person does the same act and is paid $36 174.64 by a third party to do so, the claim of mere curiosity becomes untenable. The judge's finding that there was no criminal intent in this case can be similarly be criticised as it signals to people that breaking and entering into a computer system will be treated lightly.

Second, the judge considered whether the harm was to individuals or a business enterprise. The judge noted that harm is difficult to assess in such cases because "it frequently cannot be identified."[42] Here he acknowledges that the only identifiable harm is the damage caused to the University of Pennsylvania website from a DDoS attack. The case does not state whether Walker performed a DDoS attack against the website or whether he rented his botnet out to someone for this purpose. The judge merely notes that $13 000 of damage was caused. It would not have been unreasonable for the court to estimate damages to those victim's machines which received unwanted adware courtesy of Walker's botnet. In this case, Walker installed the adware known as Dollar Revenue onto people's computers through his botnet.[43]

The point of damages needs to be highlighted. Assessing damages of $13000 for the denial of service attack seems somewhat farcical given the levels of damage caused by DollarRevenue (DR) software (explored below). Future damage assessment should include an actuarial figure calculated by the average cost of an end user to clean his or her computer from DR software and similar programs times by the estimated amount of machines affected. Adware companies such as DR pay on average 25 NZ cents per installation. Walker earned $36 174.64 NZD. This translates to 144 698.56 unauthorised installations. An estimated cost to remove DR from user's computers required an expert at an estimated average billing cost of $50 per computer. In many cases the harddrives of the computers had to be replaced or a new computer had to be purchased. The real damage caused is likely to be:

---

[41] Note 39 above, page 37
[42] Note 39 above, page 24
[43] Walker likely installed adware other than DRsoftware onto user's systems as previously seen in **Chapter 3.**

$13000 for the denial of service attack + ($50 per machine X 144 698.56 installations)

= $7, 247, 928 NZD

The real damage and costs of Walker's curiousity with computers amounts to millions and not some trivial figure in the low thousands. A broader look at DollarRevenue Software is explored below. Australia should provide a guide on assessing damages in computer related crimes. This guide should not be based merely on what may be proven by the victim, but where there is concrete evidence that other parties were affected, a reasonable estimate based on actuarial principles is recommended.

4.5.1 DollarRevenue Software

The term 'DollarRevenue' has been used in two general fashions. The first denotes the Dutch company 'DollarRevenue'. In its second sense, the term 'DollarRevenue' indicates a type of unwanted software, displaying characteristics similar to both adware and spyware.[44] Adware is typically associated with advertisements displayed online. Malicious adware, meanwhile, typically includes pop-ups, toolbars, sliders, and desktop icons. Spyware is a broader concept, encompassing malicious forms of adware, and online behaviour-tracking methods such as those targeting browser history. DR Company's actions are best categorized as spyware. In order to avoid confusion, 'DollarRevenue' as a company will be hereinafter referred to as 'DR Company' whereas the software distributed by DR Company will be referred to as 'DR software'.

DR Company is a joint venture of three Dutch enterprises (E.C.S. International B.V., WorldToStart B.V. and Media Highway International B.V.) These three enterprises along with their managing directors, whose identities remain undisclosed due to pending criminal investigation, were issued one million Euros in fines by the Dutch Telecom Regulator, OPTA, for installing unsolicited software onto over 22 million computers worldwide. According to the OPTA press release on the decision, two companies were fined 300,000 EUR each while the third company was fined 200,000 EUR. The joint venture in question essentially involves three individuals: a director, a programmer and an investor – some of whom are under current criminal investigation for ties to organized crime[45]. One director was fined an additional 300,000

[44] *See* Maurushat, A., "Supplementary Submission 62.1" Inquiry into Cybercrime (September 2009) available at http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub62_1.pdf (last accessed February 8, 2011).
[45] Many notorious Russian botnet herders with ties to organized crime were paid to distribute DR software. The money trail leads to a number of organized crime units operating in Eastern Europe. One individual of DR

EUR while another was fined 200,000 EUR. The amount of 300,000 is the maximum that OPTA may impose for failure to adequately inform users of the purpose and functions of software installation as well as for failure to provide a method of reverse installation under the *Dutch Telecommunications Act 2004*.

In its decision, OPTA cites the following reasons for issuing the fine:

> These illegally-installed programs unleashed a flood of popup windows containing advertisements for all kinds of products and services. Unsolicited search toolbars were also installed, nested in the toolbars of Windows XP and Microsoft Internet Explorer, where they displayed 'alternative search results'.
>
> As the software did not include uninstall functions, it could only be removed with expert assistance.[46]

Similar activities of DR Company have been reported on stopbadware.org, sunbelt-software corporation and spamlaw.com. The OPTA report, however, fails to mention that DollarRevenue is also involved with malicious spam, iframe injections, and Trojan downloads, which initialize information-capturing software (such as passwords and browser histories). Stopbadware.org claims that the Trojan horse drsmartloader.exe was detectable after installing DR software. This Trojan then allowed the additional installation of adware components including SurfSideKick, Webhancer, NewDotNet and Command Service.[47] Spamlaws reports that additional adware and Trojan files are downloaded, including a DollarRevenue Trojan, along with, for example, Adware-DCToolbar, Adware-Zeno, and Uploader-R.[48] Some of the Trojan horse applications made available through other bundled adware programs with DR Software (such as iframedollars) collected usernames and passwords for banking and e-commerce websites. Sunbelt Malware Research Labs provides a screen capture list and video of over 2000 additional adware/spyware programs downloaded in a single DR Software application.[49] Of these programs, several hundred are executable, Trojan style programs.

A conditional penalty was also imposed prohibiting the directors of DR Company from further distribution of unwanted software. The OPTA issued fine was appealed by DR Company. On

---

Company in particular is being investigated for more formal ties with such organized groups. This information was parted under Chatham House Rules at a closed session cybercrime workshop with law enforcement agents.

[46] OPTA, "Fact Sheet: Decision to Impose Fine on Dollarrevenue" (December, 2007) available at http://www.cytrap.eu/files/ReguStand/2007/pdf/2007-12-18-DollarRevenue-largestSpywareFineEurope-NL-OPTA.pdf

[47] *See* http://www.stopbadware.org/rports/reportdisplay?reportname=dollarrenvue

[48] More adware and Trojan files are included on the website. *See* the Spamlaws website at http://www.spamlaws.com/Dollarrevenue-adware.html

[49] Sunbelt list and video transmission of over 2000 unsolicited software available at http://www.sunbelt-software.com/ihs/alex/deskwizzclickfraud542006.pdf.

June 18, 2008, the OPTA Commission dismissed DR Company's objections.[50] DR Company lodged an appeal against the Commission's decision to the Rotterdam District Court on July 29, 2008.

DR Company claims to be a legitimate advertising company, which displays third-party advertising on computers. The company claims to install its software with proper consent and notice. The company uses an affiliate business model where third parties sign-up to DR Company and agree to deploy DR Software through ActiveX and software bundling. Active payouts in North America average 25 cents per installation as seen above. DR Company is structured like many spyware companies from a legal perspective – there is an attempt to transfer liability to third-part affiliates through an online contract. DR software is installed by unauthorized third party installations onto a user's computer through deception and dishonesty, the chief method of which is botnets.

DR software is often classified as an adware program, though it also has properties akin to spyware due to some of its tracking functions. Closer examination, however, reveals that the company is more aptly categorized as an unwanted software broker or a re-distributor of adware/spyware. DR Company promotes itself as, "one of the best pay-per-install affiliate programs on the Internet. DollarRevenue provides revenue opportunities to affiliates who have entertainment/content websites, offering them an alternative to traditional advertising models."[51] What DR Company purports to do, however, contradicts the actual functions of DR Software. A number of researchers have noted that downloading DR Software results in a flurry of transmissions from advertising sites.[52]

The following represent general types of activities that DR Software performs, including detailed examples where possible. Activities are categorized as:

- unauthorized spam;
- unwanted software bundles (typically adware and spyware);
- spyware pop-up ads;

[50] OPTA "Decision on objection concerning fines for distributing unsolicited software (DollarRevenue)" available at http://www.opta.nl/asp/en/publications/document.asp?id=2724
[51] Screenshot of DollarRevenue website on Nov. 9, 2006 retrieved through the Wayback Machine Internet Archive.
[52] The most comprehensive public documentation was performed by Patrick Jordan, a researcher at Sunbelt. The following list records over 2,000 transmissions of adware which install onto a user's computer when DR Software. For a list of transmissions from this session *see* http://www.sunbelt-software.com/ihs/alex/deskwizzclickfraud542006.pdf.

- spyware banner ad injections onto third party sites;
- deceptive Anti-Virus and Anti- Spyware Removal Advertisements;
- iframe injection;
- Trojans and executable code;
- exploit-based installations onto trusted commercial websites; and/or
- botnet application.

This categorization is non-exhaustive and somewhat artificial. DR software deploys a number of techniques to trigger several different functions. For example, DR software may be bundled with other adware programs (such as Zango) which, when installed, initializes an enticing banner advertisement (landing page) that when clicked takes the user to a popular content site (malware distribution site). DR is considered one of the worst adware companies on the Internet; the damage that DR software has caused has been documented by Team Cymru but is not available as public information.[53]

Botnet herders with ties to DR company have been arrested and tried for their botnet activities. Robert Bentley, a 21 year-old male from Florida pleaded guilty to accessing a computer without authorization (known as LSDigital as his hacker name). Bentley installed an adware program known as DollarRevenue on a number of European computers using his botnet. He is currently serving a 41-month sentence and was fined $65,000 USD for his activities. While such arrests may appear promising, as investigating officer Duckin admits, "Bentley doesn't count as 'Mr. Big' in the world of cybercrime."[54] The investigation of Bentley led U.S. law enforcement to Owen Walker. The payment records of DollarRevenue to Walker confirmed Walker's affiliate activities.[55] The fact that Walker did not obscure his payment through the use of a fake identity or through money laundering channels such as PayPal suggests that he may not have thought that what he was doing was wrong or illegal, or it may suggest that he didn't care that he was breaking the law or think that he would ever be caught. Owen Walker is now employed by Telstra in Australia. Recommendations are found at the end of the chapter in **section 4.7.**

[53] Team Cymru closed session cybercrime presentation at AusCERT 2007 with Chatham House Rules.
[54] The judgment is unreported. Details from the case may be found in news articles. The quote in question is from 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
[55] Computer World, "AKILL Controlled a Botnet of 1.3 Million PCs, Says OPTA" (2007) available athttp://www.compuerworld.co.nz/new.nsf/news/64482C4D3AAB769ACC2573B7007419F7 (last accessed June 25, 2010).

4.6 DEFENDING AGAINST BOTNETS

This section covers types of defences by corporations and third parties to combat botnets. This includes self-defence mechanisms such as hackback when performed by the entity under attack, and when hackback measures are undertaken by third parties.

4.6.1 HackBack

Hackback 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. Botnets are commonly used in many types of computer offences.

Consider the example of a denial of service attack launched against a corporation's website. A botnet has been used to launch the DOS. 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 a corporation 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.[56] 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 those found in options 4 (third party), 5 (information collection and traceback) and 6 (counterstrike).[57] The legal implications of these three options are considered below.

4.6.2 Self-Defence

There are no cases that deal with defending oneself against bot acquisition or a denial of service attack. In this instance the 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-defense 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.

---

[56] Email correspondence with Ron Plescoe, Director of the National Cyber Forensics and Training Alliance (NCFTA). On file with the author. Similar points have been made by leading cyber security experts. Former Acting Direction of the National Cyber Security Division (NCSD) within the Department of Homeland Security, Andy Purdy, discusses the importance of moving from defensive to offensive protection in order to best mitigate against damage caused from unwanted intrusions and cyber attacks. *See* Purdy, A. "Fight Cybercrime Like We Mean It" AusCERT 2009 available at http://conference.auscert.org.au/conf2009/presenter.php?presenter_id=AP (last accessed June 12, 2010).

[57] *See* 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). *See also* 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; 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; Sawyer, J. "Tech Insight: The Enterprise Hacks Back!" Dark Reading available at http://darkreading.com/security/attacks/showArticle.jhtml?articleID=223100750.

> 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."[58]

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."[59] 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."[60]

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[61]. 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.[62] The MCC's response to hackback is insufficient.

However, the report came out in 2001 and the prevalence of self-help remedies may not have been the same as it is in 2010. There have been no Parliamentary statements since 2001 on hackback.

---

[58] MCC, note 5 above, page 108.
[59] MCC, note 5 above, page 109
[60] MCC, note 5 above, page 109
[61] Survey on file with the author.
[62] 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.

I agree with the MCC that the courts should not have the legislative burden to determine issues of telecommunications policy and that there should be a legislative provision which squarely deals with defensive and deterrent cyber strategies such as hackback. In its review of the law, the Western Australian Model Criminal Code Review Committee suggested, "a distinction between lawful 'protective counterattacks' and unlawful counterattacks which are designed to destroy the hacker's computer system."[63] The reality in a counterattack is that there may be unintended consequences with the design of any form of counterattack. Traceback to source as will be discussed in **Chapter 6** is very difficult to ascertain. The use of obfuscation technologies such as multiple proxies means that counterstrike attacks in many instances would be risky. Denial of service attacks are launched using IP addresses from compromised computers. Proxies are established to make it seem as though the attack is being launched by someone else. There are incidents where denial of service attacks on Australian websites have been made to look as though they are originating from China when in fact they were performed for money by a hackers in Australia.[64] It is easy, therefore, to launch a counter attack on an innocent third party.

I believe that legislation is required. Albeit difficult, such legislation would ideally apply tests of 'reasonable proportionality' and 'immediately necessary' in order to allow people under attack to protect their property. I would propose a seven step test that amalgamates ideas from the broader technical literature on counter-attacks:

Step 1: sufficient attribution of the source of attack has been achieved and verified by more than one source (this may entail more than one method such as liaising with AusCERT or NCTSI to see if other organisations have been attacked in a similar method, consulting honeynet groups and researchers at SANS or Shadowserver),

Step 2: other alternatives are ineffective. If there is sufficient attribution, other alternatives such as police enforcement would not be effective (Eg. party is located in a cybercrime haven such as in a country that has not ratified the *Cybercrime Convention*),

Step 3: minimal damage to third party systems. There is a minimal possibility of innocent third parties being seriously affected,

---

[63] MCC, note 5 above, p.109 from Judge's Committee of the Supreme and District Courts of Western Australia; Model Criminal Code Review Committee, 15 March 2000, per Justice Scott, chairman.
[64] Interview with one of Australia's leading digital forensics expert, Ajoy Gosh. Notes in research file.

Step 4: record of a data log. A data log is kept documenting each step of the counter attack inclusive of potentially affected third parties. The data log must then be kept for a minimum of 90 days,

Step 5: copy of data log is sent to AusCERT. It is vital that those organisations engaged in hackback be held accountable for any actions which deviate from lawful hackback or in those instances where damage is suffered to innocent third parties. AusCERT (or its equivalent) is in the best situation to know if a third party has suffered any damages as many corporations or organisations under attack consult and report the incidences to AusCERT. They are in the best position to know when an innocent third party has been affected. Such compulsory disclosure is necessary as an effective restraint to not overstep reasonable self defence,

Step 6: **reasonable measures.** The hackback method is limited to measures that are reasonable, proportionate and necessary to avoid damage to third party systems. This would include methods which are protective in nature and not retaliatory (designed to destroy the other party's computer system). It would be useful to have a nation-wide consultation to produce a "Code of Hackback" which would outline specific examples of what measures are reasonable, proportionate and necessary in different scenarios, and

Step 7: engagement of security expert. Where an expert third party is used to perform hackback, the entity who hired the expert is jointly responsible for any damages or losses sustained to innocent third parties. There should be a list of accepted security experts and organisations (Eg. registered computer security consultants, SANS Institute).

In all scenarios, where an innocent third party has sustained damage to their computer systems, the reacting party should be made liable for all such damages on a basis of absolute liability. This could include a private right of action, the introduction of a no-fault insurance scheme, or set amounts that apply under certain conditions.

4.6.3 Third Party

It is unknown whether the scope of self-defense would include measures where a third party is asked (by contract or otherwise) to perform hackback. What is interesting about this scenario is that many companies and organisations will not have the expertise to perform hackback within

their own companies and would explicitly need to seek help from individuals or corporations specialising in computer security.

Botnet detection is performed by security vendors, law enforcement agencies, but, more often than not, by a group of volunteers dedicated to patrolling cyberspace. The SANS Institute[65], for example, is a civil society group who perform some of the best training, certification and research in the area. Other individuals are committed to small security groups who play a crucial role in botnet detection and response. The role of self-organised security communities will be explored in **Chapter 8**.

It is recommended that the seven step reasonable proportionality test (hackback test) also apply to third parties whose services have been contracted. Hiring self-defence is a novel concept. The reality, however, as will be seen in **Chapter 8**, is that these activities are often performed by third parties such as the not-for-profit security corporation, the National Cyber-Forensics Training Alliance. Most corporations, especially small to medium size corporations, would not have the requisite expertise to perform self-defense actions.

4.7 RECOMMENDATIONS

This section will make a number of major recommendations.

4.7.1 Virtual Honeynet

Much intelligence gathering on botnets is done through virtual honeynets. As described by two of the most authoritative experts, Neil Provos and Thorsten Holz, "a honeynet is a closely monitored computing resource that we want to be probed, attacked, or compromised. More precisely, a honeypot is "an information system resource whose value lies in unauthorized or illicit use of that resource."[66] Security vendors, researchers, Internet Service Providers, banks and many other organisations often use virtual honeynets to gather information about how malware or a botnet is being used.

[65] The motto of the institute most accurately describes the organization, "SANS is the most trusted & by far the largest source for information security training, certification & research in the world."
[66] Holz, T. And Provos, N. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection* (Addison-Wesley 2008), page 8.

Honeynets provide some of the richest information on botnets including locations of the control and command (C & C), mutation routes (Eg. C & C is located on webinex.com for two months then becomes webinex.biz then webinex.tv and so forth), commonly utilised ports, bots connected to the botnet, types of malicious activities (Eg. Trojans or denial of service), patterns of replication (Eg. how a worm is spreading), and potentially information about the botnet master. This information benefits security vendors in developing better anti-virus and anti-spyware software. The information is equally valuable to corporations and organisations in providing information about vulnerabilities in their network. Internet service providers use the information to develop spam filters, to identify vulnerable points in their networks, identification of customers at risk and so forth (ISPs are examined in **Chapter 8**). A virtual honeynet may allow its operators to identify bots. This in turn presents an opportunity for the owner of the compromised machine to be notified. Virtual honeynets, for the purpose of this chapter, may also present evidence which is later used in the prosecution of a botnet master.

We saw with the Torpig botnet example in **Chapter 3** the type of information that was gleaned from Santa Clara University researchers' use of a virtual honeynet. Some of this information was shared with the FBI. Researchers not only identified compromised computers but they peered into email contents from infected machines to see how the Torpig botnet was spreading. They found out exactly what email messages and websites were behind the spread of the botnet including fake anti-virus software websites. In doing so, they broke many laws including privacy breaches and trespass. At one point in the Torpig presentation the researcher indicated that when the FBI was informed of what the researchers had done, they responded with the likes of, "We've been trying rather unsuccessfully to get approval to do this type of investigation for a long time." This presents us with two significant problems. First, law enforcement is unable to perform the type of investigation necessary to combat botnets due to legal safeguards. For example, it is not feasible to obtain (much less do so at the speed of a mutating botnet!), a thousand B-party warrants to examine the contents of bot owners computers to see how a botnet is replicating. Second, the operation of a virtual honeynet as seen in the cases of the Torpig botnet, involved breaking the law. There are no security exemptions found in the legislation.

4.7.2 Security Research Exemption

As seen in the cases of the Torpig, Waledec and Mariposa botnets in **Chapter 3**, the work of security researchers is imperative in botnet intelligence gathering and dismantling. Much of the work of security researchers and corporations is prohibited by the law as the work involves unauthorised access and modification of data and data systems. The fact that security researchers haven't been prosecuted is only a matter of lack of public will to do so. This is not a comforting fact to most security researchers.

The Australian Commonwealth *Criminal Code* and State criminal acts and codes do not include a security research exemption to computer offences. As will be explored in the next chapter, Australia will accede to the *Cybercrime Convention* which encourages member states to make security research exemptions to computer offences. The *misuse of a device* provision specifically allows nations to provide exemptions for security researchers. It cannot be stressed enough how important this exemption is. There is no discussion in the Model Code about exemptions to the proposed computer offences other than in the context of self-defense.

Security researchers, organisations, university computer science departments and technology companies are the primary forces behind tackling botnets and other forms of obfuscation crime tools such as malware. There has yet to be a single takedown of a botnet or prosecution of a botnet master that only involved law enforcement agents. In all publicly disclosed instances,[67] security researchers were involved in spite of the fact that they could have potentially been charged with a form of unauthorised access to computer data.

Law enforcement agents work with security researchers, as seen in the Waledec and Mariposa botnet investigations, through a variety of means. Researchers are key figures in information gathering on botnets, often through virtual honeynets. Security researchers may also visit known hacker chatrooms and websites to gather and collect information. It is difficult to conceive of a successful botnet prosecution without some information from security researchers. It is strongly recommended therefore that Australia adopt a security research exemption to those computer

[67] Pandalabs was heavily involved in the takedown of the Mariposa botnet. Microsoft was heavily involved in the takedown of the Waledec botnet. Law enforcement, and a number of international computer security organisations and university researchers aided Microsoft and Pandalabs in the takedown of these botnets. *See* "Waledac Questions Answered" available at http://www.lavasoft.com/mylavasoft/company/blog/waledec-questions-answered. *See* Corrons, L. "Mariposa Botnet" (March 3, 2010) available at http://pandalabs.pandasecurity.com/mariposa-botnet/

offences dealing with unauthorised access, modification or impairment of data or electronic communications. It is not recommended, however, that such security research exemptions extend to instances where government data and electronic communications are the target as this would be an open invitation for cyber espionage and information warfare.

Special attention will need to be paid to the drafting of a security research exemption such that it is not open to abuse. One mechanism may be to adopt the Queensland approach where individuals and corporations in the security industry are required to be licensed.[68] This includes computer security entities. Only those licensed security entities would be entitled to use the security exemption. An additional feature would require security entities to report their activities pre-engagement of self-help mechanisms to a designated authority such as AusCERT or its equivalent.

The government should also work with the industry to develop permissible guidelines on self-defence against cyber-attacks. The security research exemption is further explored in **Chapter 8.**

4.7.3 Public Interest Exemption

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. Two examples come to mind. The first involves a publicized identity theft for the purpose of bringing media attention to a serious problem that has been inadequately addressed (if at all) by the appropriate authorities. The second involves an American case related to an anti-spammer.

The first example involves a British comedian, Bennett Arron, who was the victim to identity theft and fraud.[69] His dealings with creditors, banks, government entities and law enforcement as a victim led him to become rather dissatisfied with the system. In an effort to publicize just how easy it is to steal an identity due to appalling and absurdly low security prevention measures, he stole the identity of Charles Clarke, the Home Secretary of the United Kingdom. He then

[68] Queensland Government Office of Fair Trading. The various types of licenses and their requirements are available at http://www.fairtrading.qld.gov.au/security-industry-licence-types.htm (last accessed March 1, 2011).
[69] For more information about Bennett Arron see http://en.wikipedia.org/wiki/Bennett_Arron (last accessed May 31, 2010).

produced a television film "How Not to Lose Your Identity" for Channel 4. Bennett was able to not only steal the Home Secretary's identity but he did so with minimal effort in only a few short weeks; he required a razor blade and Google skills. No hacking was involved. He was arrested for identity theft shortly after the release of the film and the charges were then later dropped. He became famous in the UK and was heralded by many newspapers as a hero for this documentary. His fame even included an appearance on the Australian SBS programme, INSIGHT.[70]

The US trial court decision of *Sierra v. Ritz*[71] 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.[72] 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. The criminal trial is pending.

---

[70] SBS, Insight "Stolen ID" available at http://news.sbs.com.au/insight/episode/index/id/30 (last accessed May 29, 2010).

[71] 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.

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

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."[73] 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?[74] The scope of unauthorized access in computer fraud statutes is an old question.[75] The novelty stems from looking an unauthorized access from a public interest perspective.

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

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

[73] Rash, M. "Mother, May I" available at http://www.securityfocus.com/print/columnists/463 (last accessed January 29, 2008).
[74] Original idea expressed by Paul Ohm in the cyberprof list serve.
[75] *See* Orin Kerr's seminal article on unauthorised access. Kerr, O. "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes" (2003) New York University Law Review, Vol. 78, No. 53

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 are compelling reasons in both of these two instances 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 the government.

4.7.4 Informed Consent as Standard

Consent obtained by deception or dishonest means is not valid consent. Informed consent is a centrally important aspect of medical practice and research, as well as social science and other forms of research.[76] What is meant by informed consent?

The *EU Data Protection Directives of (1995 and 2002)* provides some assistance. The EU Directives requires that a data subject gives informed consent to their information being processed, with "consent" meaning, "… *any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*" The *2002 Directive* suggests that ticking off a checkbox on a website is sufficient consent. This definition of consent ignores whether the user has comprehended the terms, whether the terms were sufficiently disclosed, and whether the user has actually read the terms.

In Australia, informed consent for online contracts involves a low threshold. If the terms of use must be checked to be agreed on, are available to be viewed, and are written in language that is not deceptive or dishonest, then consent is valid. When I state "informed consent" I am specifically referring to a set of criteria which must be met. In this instance of consent to

[76] Van der Geest, Thea., Pieterson, Willem Pieterson and de Vries Peter.: Informed Consent to Address Trust, Control, and Privacy Concerns in User Profiling, Workshop on Privacy-Enhanced Personalization, 10th International Conference on User Modeling, Edinburgh (2005). Available online: http://www.isr.uci.edu/pep05/papers/InformedConsent.PDF

become a botnet, informed consent should exist where the user will have read the Terms of Agreement, understood the terms including the fact that their computer would become a bot controlled by a botnet master for the purpose of sending legal spam (language of terms was clear and functions fully disclosed), the user agreed to these terms, and there is an opt out mechanism.[77]

It is recommended that where a consumer is involved, the higher standard of informed consent should apply. This would eliminate scenarios where an organisation through vague and ambiguous terms and conditions could acquire a consumer's computer to become part of a botnet.

4.7.5 ACMA to have Clear Mandate for Investigation into Malware and Botnets

Australia does not specially prohibit spyware or many forms of malware that wind up on user's computers via botnets. The case of *R v. Walker* illustrated the affiliate method for distribution of the software Dollarrevenue via botnets. An adware or spyware company that paid affiliates (botnet masters) to install software without informed user consent would not attract legal scrutiny in Australia. In 2005, the Senate introduced the *Spyware Bill*, however, the Senate did not pass the bill. The *Spyware Bill* would have prohibited the installation of software without proper and informed consent by the user. The Department of Broadband, Communications and the Digital Economy (DCITA) was given the task of reviewing the legislative framework on spyware and concluded that existing Australian laws were sufficient to protect Australians from spyware and malware. Specifically, the DCITA concluded that the *Criminal Code 1995 (Cth), Trade Practices Act 1974 (Cth), the Australian Securities and Investments Commissions Act 2001 (Cth), Corporations Act 2001 (Cth), Privacy Act 1988 (Cth), Criminal Law Consolidation Act 1935(SA), Telecommunications Act 1997 (Cth)* and the *Telecommunications (Interception) Act 1979 (Cth)* adequately dealt with spyware and malware. DCITA is of the view that spyware may be dealt with through technical means. The report states that:[78]

> [s]pyware can be dealt with through technical measures similar to those used to respond to other e-security threats such as spam, phishing and worms. There are a number of freely available and commercial tools that detect, remove and prevent spyware. These are accessible on the Internet

[77] Blount, S. *Electronic Contracts: Principles for the Common Law* (Australia: Reed International Books, 2009).

[78] DCITA, "Outcome of Review of the Legislative Framework on Spyware" 2004 available at http://www.dbcde.gov.au/communications_for_consumers/security/spyware/outcome

> or obtaining through retail outlets. Anti-spyware programs should be maintained and updated regularly.

From the legal perspective, charges and fines have not been made against *a single corporation or organization* for spyware, malware or botnet use in Australia. Contrast this finding to jurisdictions that have mandated an authority such as OPTA or the United States Federal Trade Commission, where over 100 fines and charges have been made against spyware and malware distribution companies such as Dollarrevenue in the United States, Canada and Europe.

Contrast the situation further with the Netherlands where installing software without user consent is a violation of the Dutch *Telecommunications Act*.[79] The *Telecommunications Act* prohibits both unsolicited electronic communications (spam) and the storing of information or gaining access to information in the equipment of end users without permission and proper information (malicious software). OPTA, the Dutch overseeing body charged with overseeing the *Telecommunications Act*, has been given wide powers to actively investigate, fine, issues penalties, and compliance notices. OPTA works with the Dutch police (KLP) to bring criminal charges where warranted.

There would be no obstacles in Australia to pressing charges against a botnet herder. Like the United States and New Zealand, Australia prohibits accessing, modifying, or impairing data of a computer system without consent.[80] The issue is one of mandate. ACMA is allowed to legislate and investigate spam but not malware. The bot remediation initiatives lead by ACMA as will be explored in **Chapter 7**, are limited to spam botnets.

ACMA is in the best position to investigate, coordinate with Internet Service Providers, and lay charges against companies that utilize botnet services, cooperate with the Australian Federal Police for additional investigations, as well as to gather intelligence related to botnet investigations. ACMA would share the intelligence gathering responsibilities with AusCERT (or with equivalent) and the Australian Federal Police.

I recommend that ACMA be given a clear mandate similar to that of the Dutch regulator, OPTA, for spam, and the installation of unwanted software. In short, ACMA needs to be given

---

[79] *Telecommunicatiewet*. The English translation of the Dutch Act was provided by the Ministry of Economic Affairs to the European Union SMART group for their country profile study of Spam and Spyware. See *Spam and Spyware Study* SMART 2008/0013 Country profile (Netherlands).
[80] *See* s.476(2) *Criminal Code 1995 (Cth)*.

powers to examine spyware and adware companies, and operations which utilize the services of botnets.

4.8 THEORETICAL FRAMEWORK

The matters discussed in this chapter would fall under the "laws" modality in Lessig's theory. Laws, according to Lessig, whether indirect or direct, are "a command backed up by the threat of a sanction."[81] While Lessig paints a landscape of how laws also express the values of the community and establish rights and regulate structures, he notes that law's primary goal is one of threat of punishment.[82] The national criminal legal framework of Australia falls directly within this latter definition – threat of punishment. This chapter builds on the work from **Chapter 3** which demonstrated how botnets use obfuscation technologies that operate to easily circumvent law enforcement. There are few prosecutions of botnet herders. In essence, this chapter and the proceeding chapter will address the criminal legal framework, and reinforce the argument that there is an absence of an *effective* 'threat of punishment' to botnet herders and malicious actors in general. As will be seen in **Chapter 6,** even where there is compelling evidence to convict, defendants have been able to successfully use the Trojan / bot defense, or have been able to escape investigation altogether through the use of a salami technique to keep damages in one jurisdiction below the 'de minimus' level. While there are criminal provisions in Australia which would operate to sanction the actions of a botnet herder, in practice such threat of punishment has proven an empty concept. As seen in *R. v. Walker*, the courts seem reluctant to impose criminal sanction, and where they do, the sentences and fines occurred do not appear to be sufficiently deterrent.

4.9 CONCLUDING REMARKS

A series of recommendations were made which would better assist Australian authorities to investigate botnets and prosecute botnet masters. They are summarised as:

1. Providing guidelines for lawful hackback including the seven step test.
2. The inclusion of a security research exemption to computer misuse provisions.
3. The inclusion of a public interest exemption to computer misuse provisions.

[81] Lessig, L., *Code: And Other Laws of Cyberspace* (Basic Books, 1999), page 235.
[82] Above.

4. That informed consent act as the standard for instances where a consumer might unknowingly agree to be part of a botnet.
5. ACMA should be given a clear mandate to investigate malware and botnets.

These recommendations address how reform to the criminal law in Australia could aid law enforcement in combating botnets. Without such reform it is difficult to see how the "law" will act as an effective catalyst for change. **Chapter 5** explores the international criminal framework including the *Cybercrime Convention*, Interpol, WHOIS Directory, and the *United Nations Convention on Transnational Crime*. It will be further demonstrated that the criminal law, whether domestic or international, is likely to play a small role in combating botnets, thus reinforcing the limited utility of the "law" modality in Lessig's theory to this problem.

Chapter 5

THE INTERNATIONAL CRIMINAL LEGAL FRAMEWORK

Table of Contents

5.0 AIMS OF CHAPTER

International agreements are necessary to assist in the investigation and prosecution of transnational crimes. This chapter will be divided into three parts: *The Council of Europe's Convention on Cybercrime (Cybercrime Convention), The United Nations Convention on Transnational Organised Crime,* and other international and regional organisations.

As the *Cybercrime Convention* is the most significant international treaty in the area more attention will be devoted to it. This chapter aims to analyse the articles of the *Convention* relevant to botnets, offering a comparative perspective with the *Criminal Code (Cth)* provisions. Both substantive and procedural elements of the *Convention* are explored. The advantages and

disadvantages of Australian signing and ratifying the *Cybercrime Convention* are discussed with a series of recommendations offered at the end of the section.

The next section discusses the *United Nations Convention on Transnational Organised Crime (UNTOC). The UNTOC,* while not specifically focused on cybercrime, remains a relevant instrument for addressing those aspects of cybercrime related to transnational organised crime.

The remainder of the chapter identifies global initiatives linked to cybercrime and security. While there are a number of international bodies and coalitions within the domestic and international spheres, the more prominent international bodies are Interpol and the United Nations (UN). Other international organisations and initiatives that play a role in cybercrime investigation but have a somewhat diminished role in the combat of botnets, will be addressed briefly.

5.1 THE *COUNCIL OF EUROPE CONVENTION ON CYBERCRIME*

The *Convention*, an agreement between member nations of the Council of Europe is the only enforceable international agreement in the area of cybercrime. It is somewhat unique in that it is open for signature by states who are not members of the Council of Europe. The United States, Canada and Japan have all signed the *Convention*, with the United States also ratifying.

The *Convention* has three key divisions: substantive law, procedural requirements and international cooperation. All signatories to the *Convention* must criminalise certain activities.

The *Convention* creates four main categories of substantive offences:

1) offences against the confidentiality, integrity and availability of computer data and systems, comprising interference and misuse of devices (**section 5.1.1.1**);
2) computer-related offences such as forgery and computer fraud (**section 5.1.1.2**);
3) content-related offences, in particular the production, dissemination and possession of child pornography (**section 5.1.1.3**); and
4) offences related to infringement of copyright (not considered).

Australia already criminalises the above four categories of conduct. Only the first three categories – offences against computer data and systems, computer-related forgery and fraud, and child pornography – are relevant to botnets.[1] A recent international gatherings in London was held to address economic cybercrime (computer offences, forgery and fraud)[2]. Only these first three categories will be considered in the analysis that follows with intellectual property crimes excluded from consideration.

The *Convention* also addresses the procedural aspects of cybercrime. The main categories here are:

1) expedited preservation of stored computer data (**section 5.1.2.1**);
2) expedited preservation and partial disclosure of traffic data (**section 5.1.2.1)**;
3) production orders (**section 5.1.2.2**);
4) search and seizure of stored computer data (**section 5.1.2.3**);
5) real-time collection of traffic data (**section 5.1.2.4**); and
6) interception of content data (**section 5.1.2.4**).

Each of the procedural requirements is of some relevance to botnets and malware investigation.

Finally, the *Convention* contains provisions relating to international cooperation. While some of these provisions are contentious, the *Convention* allows a certain amount of flexibility how a nation might negotiate some of the issues. These may broadly be categorised as:

1) extradition (**section 5.1.3.1**);
2) mutual assistance (**section 5.1.3.2**); and
3) designation of a 24/7 network contact (**section 5.1.3.3**).

Each of these international-cooperation components of the *Convention* exists to combat economic crimes. Particular attention will be paid to extradition and mutual assistance provisions as they

[1] Intellectual property has been excluded from analysis. The *Convention* mandates signatory nations to also sign a number of copyright treaties including *The Berne Convention for the Protection of Literary and Artistic Works*, opened for signature 14 July 1967, 828 UNTS 222 (entered into force 29 January 1970); *Paris Act relating to the Berne Convention for the Protection of Literary and Artistic Works*, opened for signature 24 July 1971, 1161 UNTS 30 (entered into force 15 December 1972); *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature 15 April 1994, 1867 UNTS 3 (entered into force 1 January 1995), annex 1C ('*Agreement on Trade-Related Aspects of Intellectual Property Rights*'); *World Intellectual Property Organization Copyright Treaty*, opened for signature 20 December 1996, 2186 UNTS 121 (entered into force 6 March 2002): *Convention* art 10. The *Convention* mandates the criminalisation of certain copyright acts. Australia has signed and ratified all of these instruments, and has criminalised many forms of copyright infringement.

[2] European Serious Organised Crime Conference (February 2010).

yield the greatest concerns.

5.1.1 Substantive Provisions Relevant to Botnets

Figure 5(A) below compares and contrasts the substantive provisions of the *Convention* with the *Criminal Code Act 1995* (Cth) schedule 1 ('*Criminal Code*'). The intellectual property provisions are not considered. While there are some differences between Australian law and the substantive provisions found in the *Convention*, there is significant overlap between the two. From a substantive perspective, no changes to Australian law would be required – though some changes, as will be demonstrated, would be desirable. Key differences between the *Convention* and Australian law are explored in the table on the following page.

Figure 5(A): Comparison between Substantive Provisions in the *Convention* and Provisions in the *Criminal Code*

Convention	*Criminal Code*	**Key Differences**
Article 2: Illegal Access	Section 477.1: Unauthorised Access, Modification or Impairment to Data with Intent to Commit a Serious Offence	The *Criminal Code* does not require intent where a carriage service (internet) is used thus creating strict liability. Both instruments do not require damage or harm to be shown.
Article 3: Illegal Interception	Section 477.1: Unauthorised Access, Modification or Impairment to Data with Intent to Commit a Serious Offence.	The *Convention* covers data in transmission. The *Criminal Code* is silent on this point. The *Criminal Code* does not require intent where a carriage service (internet) is used.
Article 4: Data Interference	Section 477.2: Unauthorised Modification of Data (no intent to commit serious offence).	

Article 5: System Interference	Section 477.3: Unauthorised Impairment of Electronic Communication (no intent to commit serious offence).	
Article 6: Misuse of Devices	Sections 478.3: and 478.4 Possession, Control or Supply of Data.	The *Convention* uses language of 'device' to cover physical objects and computer programs. The *Criminal Code* uses language of 'data', which may cover information and computer programs. Devices are covered in a more limited manner under the *Criminal Code* as a 'data storage device'. The *Convention* allows for an exception for security research.
Article 7: Computer-related Forgery	Division 144	Forgery is covered as a general heading. There is no specific computer-related offence.
Article 8: Computer-related Fraud	Divisions 134 and 135	Fraud is covered as a general heading. There is no specific computer-related offence.
Article 9: Child Pornography	Part 10.6 (section 474.19)	None
No equivalent	Division 480: Dishonesty in Obtaining or Dealing with Personal Financial Information.	Actual forgery or fraud does not have to be committed for this provision to apply.

There are several differences between the *Convention* and the *Criminal Code* which I will now address.

5.1.1.1 Offences Against computer Data and Systems

The *Convention*'s computer data provisions in articles 2–6 are substantially similar to those in the *Criminal Code*. The *Convention* criminalises 'illegal' access, interference or interception of computer data, whereas the *Criminal Code* addresses 'unauthorised' access, modification or impairment to data. The different wording would not result in a different outcome in the event of prosecution. The access provisions are different, however, with Australia adopting a strict liability approach to unauthorised access to data. Unlike the *Convention*, intent is not a factor under the Australian provision. No damages are required to attract sanction under either instrument.

Mere possession, control or supply of data with intent to commit a computer offence such as that found in sections 478.3 and 478.4 (supply) of the *Criminal Code* is not prohibited under the *Convention*. For example, a botnet master in Australia who had collected usernames and passwords from third party computers with the intent of their future use in fraudulent activity would be caught under section 478.3 of the *Criminal Code.* The provision applies irrespective of whether the data has been used in an illegal manner (for example fraudulently). The same conduct would not be specifically prohibited under the *Convention.* Articles 4 and 5 of the *Convention* require an illegal use of the data such as deletion or modification.

The *Convention* specifically addresses accessing data while it is in transmission in article 3. The *Criminal Code* does not contain any provisions that specifically address the transmission of data. According to the *Model Criminal Code*, the use of more specific terms such as computer network or computer system was avoided in order to adopt a very broad approach.[3] The *Criminal Code* refers to 'data',[4] 'data held in a computer',[5] and 'data storage device'.[6] There is no differentiation between dormant data such as that found in a computer versus data in transmission, which might include data being transferred from one point to another over the internet. The

[3] Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General ('MCCOC'), *Model Criminal Code Report Chapter 4: Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction* (2001) 121–5.
[4] *Criminal Code (Cth)* definition of 'data':
Data includes:
(a) information in any form; or
(b) any program (or part of a program)
[5] *Criminal Code* (*Cth)* definition of 'data held in a computer':
Data held in a computer includes:
(a) data held in any removable data storage device for the time being in the computer; or
(b) data held in a data storage device on a computer network of which the computer forms part.
[6] *Criminal Code* (*Cth)* definition of 'data held in a computer':
Data storage device means a thing (for example, a disk or file server) containing, or designed to contain, data for use by a computer.

Commonwealth definition of data, however, is sufficiently broad as to cover transmission of data over the internet. Where the data has been modified, accessed or impaired without authorisation, it is illegal. Botnets may be used to collect data in an unauthorised matter, but they are not typically used to intercept data in transition from one point to another.

The greatest difference in the computer data provisions lies in article 6, which prohibits the misuse of a device. This article of the *Convention* enjoys no parallel in the *Criminal Code*. Devices used to illegally access, intercept or interfere with data or computers are not prohibited under the *Criminal Code*. Article 6 of the *Convention* makes illegal the misuse of any device used to commit offences in articles 2–5, and also makes illegal the production, sale, distribution, or making available of such devices. Devices might include a port scanner, or credit card skimmer. There is no reference in the *Convention* as to whether a botnet would constitute a device. As the definition of device includes a computer program, there is no reason to think that a botnet would be excluded from this definition. Article 6 could, in theory, apply to the production, sale, making available (for example, for hire services) or mere possession of a botnet. Given the absence of the terms 'botnet' or 'bot' in the *Convention*, the *Model Criminal Code,* the *Cybercrime Act 2001* (Cth)*,* and *Criminal Code*, it is probable that botnets were not contemplated in the 1990s and early 2000s when these instruments were written. Any legislative changes to the *Criminal Code* should explicitly refer to botnets as a prohibited device.

The *Criminal Code* does not criminalise the misuse of a device. Devices used to commit internet crimes do not *obviously* appear to be contemplated within the legislation (I will speculate below on how I think they might be caught under Australian legislation). Where a device is contemplated in the legislation, it is usually a specific type of device with reference to it having physical qualities. For example, a 'data storage device' is the only defined device reference within the *Criminal Code,* where the definition encompasses a disk or file server. A 'tracking device', by way of another example, refers to an electronic device.[7] This definition seems to imply that the device has a physical quality, unlike the *Convention*, which also allows for a computer software program to be a device.

Under sections 478.3 and 478.4 the *Criminal Code* makes it an offence to possess, control or supply data with intent to commit a computer offence. The definition of 'data' includes computer programs. This could conceivably be used to capture the misuse of a device where

[7] *Criminal Code (Cth)* section 100.1.

such device is a computer software program such as a botnet. This provision applies irrespective of whether the data has been used in an illegal manner, such as fraud. The same conduct may not be criminalised under the *Convention* as the device, if not for sale or hire, must be used in an illegal manner.

The *misuse of a device* provision specifically allows nations to provide exemptions for security researchers. It cannot be stressed enough the importance of this type of exemption. In Australia security researchers are not exempt from the computer provisions in the *Criminal Code*. Security researchers, organisations, university computer science departments and technology companies are the primary forces behind tackling botnets and other forms of obfuscation crime tools. There has yet to be a single takedown of a botnet or prosecution of a botnet master that only involved law enforcement agents. In all publicly disclosed instances,[8] security researchers were heavily involved in spite of the fact that they could have potentially been charged with a form of unauthorised access to computer data.

5.1.1.2 Computer-Related Forgery and Fraud

The *Convention* criminalises computer-related forgery and fraud where there is dishonest or fraudulent intent and where there is damage or loss of property. The *Criminal Code* does not specifically cover computer-related forgery and fraud; instead, the *Criminal Code* prohibits forgery and fraudulent conduct as a general heading under division 144 (Forgery), division 134 (Fraudulent Conduct) and division 135 (Other Offences Involving Fraudulent Conduct). These generic headings are sufficiently broad as to cover computer-related forgery and fraud.

5.1.1.3 Content-Related Offences (Child Pornography)

The *Criminal Code* child pornography provisions fully comply with the *Convention* with no differences. Child pornographic materials include written narratives, animated cartoons (such as anime or manga), and fictional depictions of abuse. The recent decision of *McEwen v Simmons*

[8] Pandalabs was heavily involved in the takedown of the Mariposa botnet. Microsoft was heavily involved in the takedown of the Waledac botnet. Law enforcement and a number of international computer security organisations and university researchers aided Microsoft and Pandalabs in the takedown of these botnets. See Jeff Williams, '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>; Luis Corrons, 'Mariposa Botnet' on *PandaLabs Blog* (3 March 2010) <http://pandalabs.pandasecurity.com/mariposa-botnet/>. Technical blogs in the area of Internet security provide the most up-to-date information on security incidents. In this case, the blogs were written by those involved with the take-down of the botnets in question.

establishes that under New South Wales and Commonwealth law depictions of sexual acts among the child characters of the American cartoon *The Simpsons* constitute child pornography.[9] A child is defined as a person under 18 years of age for both the *Convention* and *Criminal Code*.

5.1.2 Procedural Elements

The *Convention* mandates procedural changes to law enforcement and co-opts ISPs into the law enforcement process. Under the *Convention*, ISPs must implement technical means to aid law enforcement to monitor network traffic. Generally, this requires ISPs to have facilities that allow for interception of communication, greater search and seizure powers, and for evidence to be collected in real-time. The procedural provisions are examined below, again in the context of botnets.

5.1.2.1 Expedited Preservation of Computer Data and Traffic Data (Article 16)

The *Convention* requires expeditious preservation of data by the person in possession or control of data. ISPs will often be the ones called upon to preserve data. Article 17 in particular is aimed at compelling ISPs to expeditiously preserve internet traffic data logs for a maximum period of 90 days. The *Convention,* however, does not compel ISPs to monitor and store data traffic. Most ISPs use medium packet monitoring systems such as the international standard, NetFlow, which is renowned for being one of the less privacy-invasive monitoring technologies. NetFlow collects and analyses data traffic, and signals irregularities. Using NetFlow, the data traffic is then quickly deleted. In the case of an active criminal investigation, the *Convention* obligates an ISP to preserve the data that is already collected and stored but would otherwise be deleted expeditiously. This could include preservation of what IP addresses connect to and from another IP address, or what phone numbers connect to a Voice over Internet Protocol ('VOIP') number. This may also include information about what types of protocols a customer makes use of, size and use of packets, and so forth. Data preservation remains a controversial point, particularly in its operation in conjunction with the obligation to provide mutual assistance (examined in **section 5.1.2.1**).

Currently Australian ISPs are only required to preserve evidence, monitor internet traffic and provide help to law enforcement in three contexts:

[9] (2008) 73 NSWLR 10

1) enforcing the criminal law and laws imposing pecuniary penalties;
2) protecting the public revenue; and
3) safeguarding national security.[10]

A warrant is required before an ISP is compelled to assist law enforcement or a relevant authority.[11] ISPs are obliged to cooperate with the AFP, state police, Australian Security Intelligence Organisation ('ASIO'), revenue (tax) authorities, Australian Communications and Media Authority ('ACMA'), Australian Crime Commission and the Telecommunications Industry Ombudsman.[12] Absent a warrant, the ISP has discretion as to whether it wishes to cooperate with law enforcement. Currently, there is no legal obligation for an ISP to cooperate with law enforcement internationally. The ISP has discretion in both instances. The *Convention* changes this and allows foreign law enforcement agencies to compel ISPs to cooperate.

The type of information requested in a preservation of data order depends on whether the ISP has been intercepting communications, monitoring content, and whether or not the ISP has kept any of this data. A preservation order merely compels the ISP to put aside data that it has kept. Most importantly, the *Convention* does not compel ISPs to monitor and store data traffic for all of its customers. An ISP must only store data where a request has been made by foreign or domestic law enforcement agents.

The *Convention* does not address what is to be done with the stored data after the 90 day period elapses. Australian ISPs would still be obliged to comply with data retention and destruction laws in Australia. Nonetheless, should Australia sign the *Convention*, clear language concerning data retention and destruction should accompany any provision on point. The *Convention* also does not deal with the security measures/standards necessary to prevent data breach in relation to stored data. Such storage of a large quantity of data also provides fertile ground for information theft.

Preservations of data and traffic data logs are only useful in the investigation of a botnet master where real-time evidence can be collected and communications potentially intercepted. However, real-time evidence collection and interception of communications require a warrant under

[10] *Telecommunications Act 1997* (Cth) ('*TA*') s 313.
[11] In some instances, a certificate may offerred in place of a warrant where there is 'reasonable necessity'. The ISP has discretion in this instance as to whether to cooperate with law enforcement.
[12] *TA 1997* (Cth) pt 13.

Australian law. The *Convention* does not change this fact of domestic law. The importance of real-time evidence will be canvassed in **Chapters 6 and 7.**

5.1.2.2 Production Orders

Production orders often refer to the disclosure of 'subscriber information', in particular in relation to subscription to an ISP or a DNS registrar. As seen in **Chapters 3 and 5**, private security organisations and researchers monitor malware and botnets through honeynets. The following type of information about a botnet would need to be known in order to make a production order potentially useful in combating botnets:

- DNS/IP address of the IRC server and port number (assuming that the C&C is in the IRC);
- password to connect to the IRC-server;
- nickname of a bot and identity structure;
- name of the IRC channel to join and channel password; and
- Client-to-Client Protocol version (used for IRC).[13]

As explored in **Chapter 3**, there are several methods to take down a botnet: ISP and/or DNS provider removal of IP addresses used as C&C sources; infiltration and disruption of C&Cs; bot remediation; and prosecution. Often a combination is used.[14]

In order to prosecute a botnet master, one must first identify the botnet master. This is an extremely difficult task and several factors must be present before successful execution is possible:

- the IP address of the IRC server must be known along with the port, and nicknames of the bot;
- the IP address may be traced to the ISP or DNS provider;
- the ISP or DNS registrar would have to provide subscriber information via a production order;
- the subscriber information would have to be truthful and accurate in order to correctly

[13] *See generally* Schiller, C., Binkley, J., Harley, D., Evron, G., Bradley, T., Willems, C., and Cross, M., *Botnets: The Killer Web App* (Syngress 2007).
[14] *See for example* theWaledac botnet, note 8 above.

ascertain the identity of the botnet master; and

- evidence would need to be collected before proceeding to press charges.

Production orders to produce subscriber information are only useful where the information is accurate. Many criminals do not use their real identities to subscribe to internet services, or they register the services under an empty holding company.[15] To add to this, stolen credit cards are often used as payment for many internet services. Where this is the case, a production order will not be of any use. Where dynamic DNS is used, the constant change of IP addresses makes it difficult (if not impossible) to trace to the botnet master. Where the botnet master relies on P2P for its C&C there is no subscriber information. Production orders will only be useful in prosecution when dealing with lower level botnet masters who take minimal precautions to shield their true identities.

In any event, it is much more simple and efficient to use the WHOIS protocol and server to access subscriber information than it would be to use the *Convention* to obtain a production order, assuming of course that the criminal did not use false information and faked credentials. The WHOIS protocol and server will be explored in **Chapter 6**.

5.1.2.3 Search and Seizure

The *Convention* gives law enforcement wide-reaching powers of search and seizure of data and computers in the investigation of cybercrime. The powers that extend to law enforcement in this regard do not differ from the current powers of law enforcement to search and seize computers for evidence. The goal with the search and seizure provision is similar to those of data preservation. Due to the volatility of digital evidence, measures must be taken to preserve the data and evidence expeditiously. Where search and seizure is conducted, this includes search and seizure of a computer system or stored device where data may be found, the right to make a copy of the data and maintain the integrity of the data (which involves rendering the data inaccessible to other parties). The *Convention*'s goal in this area is to ensure that domestic law enforcement cooperates with foreign law enforcement requests to search and seize a computer for an investigation abroad.

[15] iDefense, for example, documents that the holding company in Hong Kong (Absolutee Corp) is used to register many internet webpages, IP addresses and so forth for organised crime. *See* iDefense, *The Russian Business Network: The Rise and Fall of a Criminal ISP* (27 June 2007) 8, page 15.

The *Convention* and Australian law are silent on how long law enforcement may seize a computer or a computer system without laying charges. This allows for possible police abuse where confiscated computers may be kept them for several months without ever laying charges, and potentially there may be significant damages to the computers.[16] The *Convention* does not address this type of potential abuse.

5.1.3.4 Real-Time Evidence Collection and Interception Capabilities

Many commentators have expressed fears of the *Convention* establishing an Orwellian system of electronic surveillance.[17] Such fears seem genuinely unfounded given that procedural provisions of the *Convention* only apply to active criminal investigations. For example, the *Convention* does not oblige ISPs to monitor all network traffic and preserve data logs of all of their customers for 90 days in the event that the data might be needed for future investigations. Additionally, there is some level of protection of civil liberties (privacy)[18] as real-time evidence collection and interception of communications are subject to the domestic law of each party. Interception of communications, for example, must be done in Australia under a valid warrant. The Australian content warrant framework and preliminary issues in real-time evidence collection will be explored in **Chapter 6**. Deep packet inspection technology, and ISP legal obligations regarding interception, and the implications on civil liberties will be explored in **Chapter 7**.

Article 21 of the *Convention* specifies that interception capabilities are only required for serious offences as determined by domestic law. Domestic law refers to the location, for example, of the ISP. Thus, in the Australian, context, interception requests would only be required for Australian-defined serious offences: there will arise no duty to intercept a communication for law enforcement in another country where the request is repugnant to domestic law.[19] For example, a serious offence in Singapore might include a political speech against a government. The *Convention* specifically carves out exemptions where a request is in connection with a political offence or where a request would prejudice sovereignty, security or public order.[20] This

---

[16] See Bronitt, S., and Gani, M., "Shifting Boundaries in Cybercrime: From Hacking to Cyber-Terrorism" (2003) 27 Criminology Law Journal 303.
[17] Esposito, G. 'The Council of Europe Convention on Cyber-Crime: A Revolutionary Instrument?' in Broadhurst, R. (ed) (2004) *Proceedings of the 2nd Asia Cyber-Crime Summit* (Centre for Criminology, the University of Hong Kong, 2003). *See also* 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*.
[18] Reference is made within the *Convention* to the *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 302 (entered into force 23 March 1967): *Convention* Preamble, art 15.
[19] *Convention* art 34.
[20] Above arts 27(4), 29(5), 30(2).

exemption would apply to all procedural and international cooperation provisions.

5.1.3 International Cooperation

Convention member states must cooperate with investigations with other member states. The essence of the *Convention* is to ensure cooperation 'to the widest extent possible.'[21] This cooperation is divided into four categories, considered below, with particular focus on mutual assistance provisions.

5.1.3.1 Extradition

There has been much incorrect commentary surrounding the *Convention* over extradition and mutual assistance matters. This statement from Manolescu illustrates the type of misinformation that surrounds the *Convention*:

> "The Convention extradition provisions should not replace the original binding Extradition treaties between two countries, if any, because those provisions in the *Convention* are again too vague to adequately replace dedicated and elaborated Extradition Treaties. One reason Canada did not sign the [*Convention*] is that the Canadian government does not want to have extradition clauses or rules with countries with which they do not yet have an Extradition Treaty (because of their differences in legislation, democracy or human rights). The *Convention* should not serve as the only extradition treaty between two countries which have no other extradition agreements in place."[22]

The *Convention* does not supplant existing provisions in extradition treaties. It deems articles 2–11 extraditable offences in existing treaties:[23] extradition is still subject to the conditions in the existing extradition treaty. For example, if country X punishes illegal access to a computer with the death penalty and country Y does not, if there is a provision in the existing extradition treaty that bans extradition in cases where the death penalty would apply, then there is no requirement under the *Convention* that would compel extradition. Moreover, extradition treaties were often negotiated before the current cybercrime era and are rather outdated. Re-negotiating every bilateral extradition treaty to add cybercrime components would be an arduous and onerous task which would not likely be done.[24] The *Convention* conveniently allows the incorporation of

---

[21] *Convention* art 23.
[22] Manolescu, D., *Is It Possible to Regulate the Internet Globally?: A Comparative Case Study of Cybercrime Framework in Canada and Romania* (Masters Thesis, University of Alberta, 2009) 16–17.
[23] *Convention* art 24(2).
[24] Broadhurst, eg, claims that many extradition treaties are outdated: Roderic Broadhurst, 'Developments in the Global Law Enforcement of Cyber-Crime' (2006) 29(3) *Policing: An International Journal of Police Strategies and Management* 408, page 418.

cybercrimes into existing extradition treaties.

Article 24(3) of the *Convention* allows members the option to make extradition contingent on an existing extradition treaty. Where there is no extradition treaty in place (often due to differences in legislation, democracy or human rights), members have no obligation to extradite offenders. The *Convention* does not change this unless the member state deliberately decides not to make extradition contingent on an existing extradition treaty. There are compelling reasons why nations might want to cooperate with the extradition of offenders of the crimes specified in the *Convention*, especially those egregious crimes involving child pornography, fraud where large sums of money are involved or where the fraud affects a large groups of people, and any illegal use of a computer or data in order to commit serious computer attacks to critical infrastructure such as electrical grids, banking systems and hospital databases. Extradition might seem extreme in the case of copyright infringement.

The *Convention* accounts for these lower types of crimes by making extradition contingent on the offence being punishable under the laws of both parties and only in situations where there is 'deprivation of liberty for a maximum period of at least one year.' Furthermore, parties do not have to impose criminal liability for copyright related offences where there are other effective remedies in place.[25] The flexibility of the *Convention* allows parties to adhere to the *Convention* without compromising its existing domestic safeguards against extradition in unjust or insufficiently serious matter.

There is no publicly available information on whether extradition of any botnet masters has been sought anywhere in the world. In the case against Owen Walker extradition was not sought. He was tried in New Zealand despite his victim being an organisation located in the US. Much of the intelligence and evidence was collected by the FBI and handed over to New Zealand authorities as was explored in **Chapters 3, 4** and **6**.

5.1.3.2 Mutual Assistance

Much misinformation has also been written about the mutual assistance provisions of the *Convention*. Here is an example that illustrates some common misconceptions about the *Convention*:

[25] *Convention* art 10(3). This might include a system of fines for infringement.

> "It is even more shocking that a forty-eight Article Convention on Cybercrime, which was supposedly predicated on the assertion that the effective fight against cybercrime required increased, rapid and well-functioning international cooperation in criminal matters, is entirely devoid of the word privacy. … A Convention deficient of a 'dual criminality' provision is not only very worrying for civil libertarians, it could also be seen by nations as a potential source of apathy on the drafter's behalf."[26]

Yet the preamble to the *Convention* contains strong language on the importance of the needs of law enforcement with human rights and "the rights concerning the respect for privacy". One of the primary privacy complaints of the *Convention* is rooted in the false premise that the *Convention* does not allow a state to require dual criminality. The argument is that mutual assistance would enable an interception of communications or preservation of data traffic to be done outside the safeguards of domestic law. We have already noted that the collection of real-time evidence and interception of communications must be done according to domestic law. Domestic law includes the right to privacy under Australian law (the *Privacy Act 1988* (Cth), the *TIAA*, and *TA*) as will be seen in **Chapter 7**. Moreover, parties may under the *Convention* require dual criminality for mutual assistance, as will be explored below.[27]

Dual criminality is allowed under the *Convention* with the exception of the requirement of the preservation of data. Stipulation of dual criminality is not allowed in mutual assistance requests for preservation of stored computer data.[28] Preservation of data obligations, however, does not include *comprehensive* disclosure of the data, search and seizure or any other matter other than the initial preservation. A warrant is still required in order to view the data that was preserved (Australian warrants will be discussed in **Chapter 6**). In a typical warrant only *partial* data traffic is required to be disclosed in an expeditious manner. Often law enforcement is looking for information on proxy chaining.[29] Law enforcement may, for example, need to see an immediate snapshot of how the connection is routed to or from another ISP. An expedited preservation of data request in one country could provide information as to how the connection is situated within a proxy chain, connecting from one ISP to another. Once law enforcement traces back to the source-ISP, they may then compel a production order to ascertain the subscriber information.

There is no indication in the Convention as to why preservation of stored computer data is

---

[26] Bannon, A., "Cybercrime Investigation and Prosecution: Should Ireland Ratify the Cybercrime Convention?" (2007) 3 Galway Student Law Review 115, page 132.
[27] *Convention* art 25.
[28] Above art 29(3).
[29] Lovet, G., "Fighting Cybercrime: Technical, Juridical and Ethical Challenges" (Paper presented at the Virus Bulletin Conference 2009, Geneva, 23, September 2009), page 8.

treated differently from other obligations. In a cybercrime investigation, time is a critical factor. Often investigators will need to collect evidence expeditiously in order to have sufficient evidence to convict. Digital evidence is volatile. Investigators may not have worked out the full extent of crimes committed at the time of a preservation of data request. Once they have done so, it is possible that evidence will lead to the detection of crimes that are dually criminalised, thereby compelling mutual assistance to extend beyond mere preservation of data. But the data would have been preserved, and thus able to be used as evidence. More importantly, the particularly useful portion of data preservation consists in identifying connectivity points, as criminals tend to obfuscate their IP address through proxy connections. A partial look at data traffic may sometimes provide a snapshot of routing connections.

Parties may require dual criminality for all other mutual assistance requests. These include real-time evidence, search and seizure, interception of communications and production orders.

5.1.3.2 Designation of a 24/7 Network Contact

The *Convention* creates a network of national contact points available to better coordinate criminal investigations and requests for information. The network operates on a 24-hour, seven-days-a-week basis allowing for immediate assistance, and supplements more traditional channels of cooperation such as Interpol. The role of the network is more akin to a facilitator of investigations, rather than an organisation such as Interpol whose mandate is one of active criminal investigations involving transnational crimes. Each contact within the network will either facilitate or directly carry out procedural tasks under the *Convention* such as expeditious preservation of data, interception of communications and others. The international cooperation provisions such as extradition and mutual assistance are not carried out by this network contact, but by a separate authority. The network contact, however, would facilitate extradition and mutual assistance requests to the relevant authority pursuant to article 35(2)(b). The *Convention* further mandates that such network personnel must be trained and equipped.[30]

5.1.4 The Utility of the Convention in Combating Botnets

The *Cybercrime Convention* is the only international instrument of direct relevance to botnets.

[30] *Convention* art 35(3).

There is speculation as to whether Australia should sign and ratify the *Convention*.[31] There is little statistical evidence of the success of the implementation of the *Convention*. Statistics have been generated on mutual legal assistance requests[32], numbers of countries to accede or ratify[33], and number of countries to implement a 24/7 network[34]. Success of the Convention is largely measured with anecdotal evidence through the form of guidelines and best practices. For instance, the discussion paper, "The Effectiveness of International Co-operation Against Cybercrime: Examples of Good Practice"[35] posits France, Romania and Estonia as country studies for good practices. Curiously, the paper noted that many successful investigations were the result of provisions in the law allowing for "spontaneous information." This involves the disclosure of information obtained in an investigation to foreign law enforcement agencies without prior request. Such disclosure of pertinent information allows the competent authority of another State to initiate its own investigations. The notion of "spontaneous information" is not contemplated within the substantive or procedural provisions of the *Convention* and yet is attributed as a key mechanism in international cybercrime cooperation.

There is criticism of the *Convention* as being repugnant in regard to privacy protection, and in particular, to the ability to have both free and anonymous speech online.[36] These are distinct causes for concern, especially given that Australia does not have a Bill of Rights or a high level of Constitutional protection of civil liberties such as in the United States or Canada. Any *Convention* provisions adopted, for example, in Canada which may be repugnant to civil liberties may be challenged under the *Canadian Charter of Human Rights and Freedoms*. The same safeguards are not present in Australia, therefore there is an even greater need to be particularly cautious in adopting procedures which unduly impact on civil liberties. Further analysis on civil liberties in found in **Chapter 7**. It does not follow, however, that absent a Bill of Rights, that the *Convention* should not be signed and ratified.

---

[31] In February 2011, the Australian Government has issued a call for comments on Australia's Accession to the Cybercrime Convention.
[32] Council of Europe, European Committee on Crime Problems, Committee of Experts on the Operation of European Conventions on Co-Operation in Criminal Matters, "Summary of the Replies to the Questionnaire on Mutual Legal Assistance in Computer-Related Cases" February 18, 2009.
[33] Council of Europe, The Cybercrime Convention Committee, "Questionnaire for the Parties Concerning the Practical Implementation of the Convention on Cybercrime by the Parties." September 3, 2007.
[34] Council of Europe, Project on Cybercrime, Economic Crime Division, "The Functioning of 24/7 Points of Contact for Cybercrime" April 2, 2009.
[35] Council of Europe, Project on Cybercrime, Pedro Verdelho, "The Effectiveness of International Co-operation Against Cybercrime: Examples of Good Practice" March 2008.
[36] 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).

The substantive provisions in the *Convention* are similar to Australian law though some changes would need to be made. The misuse of a device provision would need to be added to the law. This, in fact, was demonstrated to likely to be one of the most important provisions for successful prosecution of a botnet master. Additionally, Australia may have to adopt specific provisions for computer-related forgery and fraud though we have seen that under the *Criminal Code (Cth)* the current provisions against forgery and fraud are sufficiently broad so as to include its computer-related counterparts.

The procedural requirements under the *Convention* do not alter Australian law from a domestic point of view. Australian ISPs already have interception and real-time evidence collection capabilities. Preservation of data, production orders and search and seizure of computer systems, as will be seen in **Chapter 6**, are already required under Australian law for the purpose of criminal investigations. The *Convention's* procedural provisions do not alter Australian law. The provisions compel law enforcement and ISPs to fulfil similar duties as they would in a local criminal investigation extended such duties to those overseas law enforcement agents who are Party to the *Convention*. Procedural tasks must be fulfilled in accordance with domestic law. For example, in the case of interception of communications, a warrant will be required. The procedural requirements potentially become contentious when applied to the corresponding international cooperation obligations.

The *Convention* allows Parties to provide extradition only where an extradition treaty between the two Parties already exists. Ratification of the *Convention*, for example, would not mean that Australia would be forced to extradite offenders to a country where no extradition treaty exists between the two nations. Dual criminality may also be specified as a condition to extradition. The *Convention*, likewise, requires the offence to contain a minimum sentence of deprivation of liberty of one year or more.

The *Convention* allows for dual criminality in order to provide mutual assistance. Where a Party to the *Convention* specifies dual criminality as a pre-condition to mutual assistance, they are able to do so in application to all procedural requirements other than expeditious preservation of data. The *Convention* does not allow dual criminality requirements for expeditious preservation of data but this does not mean that there is an obligation to disclose such preserved data to the requesting Party.

Ratification of the *Convention* would allow Australian law authorities the ability to better investigate criminal offences where part of the crime, or the criminal, is located overseas in a jurisdiction party to the *Convention*. Ratifying the *Convention* would allow law enforcement in some instances to have evidence preserved expeditiously. In doing so, proxy chains may be identified with the eventual aim of linking an IP address to the subscriber information of a botnet master. It could allow law enforcement the ability to use live forensics investigations to follow and preserve evidence of illegal bot activity.

Mutual assistance provisions are significantly diluted because countries with significant cybercrime industries are not party to the *Convention*. Russia, for example, is not party to the *Convention*. Even if nations such as Russia were to sign the *Convention*, there is scepticism that sufficient resources would be allocated to law enforcement to enable investigation. The fact is that in all nations, cybercrime and e-commerce is under-enforced. Priority inevitably goes to crimes where the victims are local. The *Convention* does not change this fact.

The popularity of botnets as a cybercrime tool did not fully emerge until 2004 where there was a shift to monetization of malware and botnets. Many of the emerging obfuscation technologies make traceback of botnet masters difficult where the likelihood of the prosecution of sophisticated botnet masters is rather unlikely. Nonetheless, the *Convention* remains of some utility to law enforcement. Where information may be gathered about a botnet master (perhaps through following the financial trail or through information trading when prosecution other malicious actors in order to strike a better deal), identification of the botnet master means that it may be possible through real-time forensics to collect evidence, including examination of encrypted documents and messages, to mount a successful prosecution. But perhaps the most important element of the *Convention* may prove to be merely compelling nations to adopt provisions making many forms of cyber crime illegal.

As seen in **Chapter 3** with the Mariposa and Waledac botnet takedowns, there is a more public and coordinated effort between the security companies, ISPs, researchers, DNS registrars, and law enforcement to both takedown botnets and prosecute botnet masters. The efforts of law enforcement in the Mariposa situation may prove somewhat fruitless at the end of the day. While Spain has signed the *Convention*, it has yet to ratify it. Spain does not have substantive provisions in its law that makes the operation of a botnet illegal. As such, Spanish authorities have the much greater burden of proving credit card fraud. The more countries that sign and

ratify this *Convention*, the less legal safe havens there will be for botnet masters to hide behind the protection of legal loopholes. From a policy perspective, it is my view that Australia should accede to the *Convention*.

The procedural requirements of ISPs under the *Convention* have attracted criticism from civil liberty groups and researchers on the grounds of privacy, freedom of expression and lack of due procedure in criminal matters.[37] The main concern has been the role of ISPs as agents of law enforcement, and with the obligation of ISPs to monitor, collect and preserve massive amount of information of its customers. These points will be explored in detail in **section 7.5 of Chapter 7, "The Role of ISPs and DNS Providers in Combating Botnets"**.

5.2 *THE UNITED NATIONS CONVENTION ON TRANSNATIONAL ORGANISED CRIME*

The *United National Convention on Transnational Organised Crime* (UNTOC), while not specifically focused on cybercrime, remains a relevant instrument for addressing those aspects of cybercrime related to transnational organised crime. Often, as seen in **Chapter 3**, botnets are used as a primary tool for organised Internet crime. Organised crime makes the most nefarious use of botnets such as fraud and distribution of child pornography.

The *UNTOC* has been signed and ratified by over 147 states including Australia, the United Kingdom, the United States, Canada, and more importantly, in states with high levels of organised Internet crime such as Russia, the Ukraine, Bulgaria, Romania, and China. The *UNTOC*'s global reach is more extensive than the *Council of Europe's Convention on Cybercrime*. The UNTOC extends to serious crime committed by organised criminal groups that is transnational in nature. 'Serious crime' is defined broadly to as to encompass an offence that is punishable with deprivation of liberty of at least four years.[38] An 'organised criminal group' is defined as a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes ... in order to obtain financial or material benefit.[39] According to Article 3(2), a crime is transnational if it is committed in more than one State, is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State, is committed in one State but involves an organised criminal

[37] *See for example* Young, note 17 above. *See also* Kerr, note 32 above.
[38] Article 2(b)
[39] Article 2(a)

group that engages in criminal activities in more than one State, or it committed in one State but has substantial effects in another State.

Most botnet activities would be transnational in nature. Not all States, however, have introduced legislation criminalising illegal access, use, interference, etc. to computers. As seen in **Chapters 3 and 4**, Spain, for example, has not yet ratified the *Cybercrime Convention* nor has it introduced cybercrime provisions. In spite of valiant efforts of security researchers and law enforcement, there is a good chance that the botnet masters of the Mariposa botnet will not be successfully prosecuted. There is some speculation that this Spanish group has ties to organised crime in Eastern Europe as seen in **Chapter 3**. The operation of a botnet in Australia would be defined as a serious crime. Whether or not a botnet is run as part of the operations of an organised criminal group is not an easy question. An organised criminal group might, for example, hire out a botnet (or several botnets) for illicit purposes. It is probable that the botnet master would not know whether they had been hired or paid by an organised crime group. Consider the case of the young New Zealand botnet master in **Chapter 4,** Owen Walker, who had been illegally installing DollarRevenue and Iframes adware onto computers. Both of these adware companies have ties to organised crime.[40] It is ambiguous under the UNTOC whether botnet masters working for organised criminal groups, whether knowingly or unknowingly, would be caught under this provision. The case is more complex where the botnet master may choose through wilful blindness to ignore signs that they were working for organised criminal groups. For example, when one is paid through known money laundering channels such as Western Union, and Paypal, and where there is much available discourse on the Internet concerning, for example, Iframes connection to organised crime, a botnet master would have to deliberately deceive themselves to believe that their activities were legitimate.

The *UNTOC* establishes categories of broad substantive offences related to organised crime. The main substantive offences are:

> Article 5: *Criminalization of Parties in an Organised Criminal Group*
>
> Article6: *Criminalization of the Laundering of Proceeds of Crime*
>
> Article 8: *Criminalization of Corruption*
>
> Article 23: *Criminalization of Obstruction to Justice*

[40] *See for example*, Santorelli, S., "The Future of Botnets" (2008) AusCERT Conference.

The international cooperation provisions could potentially play a more relevant role in botnet investigations where they are related to organised crime. The Waledac botnet, a later version of the Storm botnet, as seen in **Chapter 3,** is thought to be linked to Eastern European organised crime.[41] The *UNTOC* mandates mutual legal assistance under Article 18. Similar to the *Cybercrime Convention*, mutual assistance may be refused if the request is prohibited under domestic law, contrary to the legal system, where the request has not been made in conformity with the *UNTOC*, and where assistance would prejudice sovereignty, security, ordre public or other essential interests.[42] For example, requests by US authorities for mutual assistance in the prosecution of a notorious Ukrainian malicious author with ties to organised crime were refused. Ukrainian law enforcement refused to mutually assist (and extradite) in the investigation under the guise of threat to sovereignty and security as the young twenty-some year old Ukrainian male had apparently run for election to the Ukrainian Parliament.[43]

The *UNTOC* does not contain the same extent of procedural obligations as the *Cybercrime Convention.* The most valuable component of the *Cybercrime Convention* is its application to ISPs and DNS registrars. These entities are best positioned to offer what is often the most valuable information in a cybercrime investigation: to collect evidence in real-time, intercept communications, preserve valuable data, and disclose subscriber information. The obligations contained in the *UNTOC* do not extend to ISPs and DNS registrars. The UNTOC represents a formal process created to govern transnational evidence collection and sharing between member states. The traditional methods in the *UNTOC*, while potentially valuable for combating organised crime, remain somewhat cumbersome and ineffective in cybercrime investigations which require very quick turn-around time for evidence collection and preservation.

5.3 INTERPOL

The International Criminal Police Organization[44] (Interpol) is an international police organization that, according to its website, "facilitates cross-border police cooperation, and

[41] See iDefense, note 15 above.
[42] Article 21 *UNTOC.*
[43] Presentation by FBI (2008), AusCERT Conference.
[44] Formerly, the International Criminal Police Commission which was established after World War 2. *See generally,* Igbinovia, P., "Interpol: A Survey of Research Findings" (1984) 7 Police Studies: International Review of Police Development 112.

supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime."[45] Interpol does not launch its own investigations into criminal activity, does not have agents and does not arrest or prosecute criminals. These activities are done by national law enforcement of member countries. Interpol has 188 member countries including Australia, Canada, the United State, the United Kingdom, and Russia. The structure of Interpol includes a General Assembly (Executive Committee), Advisors, General Secretariat and National Central Bureaus. The General Secretariat who runs the day to day operations of this police organization is located in Lyons, France. The General Secretariat communicates with the member state national central bureaus, in particular through facilitating information sharing, coordinating joint operational activities, conducting research and development of databases, training, and by developing best practices.[46] The organization is bound to the provisions contained in the Interpol Constitution and General Regulations (Interpol Constitution). According to the Interpol Constitution, its aims are:

(1) To ensure and promote the widest mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights;
(2) To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes[47].

Interpol is a unique organization in that it is a full-fledged international organization that operates without an international treaty. It is an inter-governmental organisation established without a treaty. As one commentator writes, "Interpol is arguably the most discussed and least understood international police organization."[48] Interpol has listed five priorities which include drugs, terrorism, trafficking of humans, organised crime and financial and high-technology crime.[49] There is no public information available as to whether Interpol classifies botnets as part of the wider landscape of financial and high-technology crimes.

Interpol has developed an international database for credit card fraud known as the Universal Classification System for Counterfeit Payment Cards. This is a secure website that provides law

[45] *See* www.interpol.int/public/icpo.default.asp (last accessed December 1, 2011).
[46] *See* www.interpol.int./Public/icpo/Guide (last accessed December 1, 2011).
[47] Article 2 of the Interpol Constitution
[48] Deflem, M., "The Origins of Interpol" in *Policing World Society: Historial Foundations of International Police Cooperation* (Oxford Universit Press, 2004) pages 124 to 153. *See also* Garrison, O, *The Secret World of Interpol* (New York: Ralston-Pilot, 1976).
[49] Note 42 above.

enforcement a database outlining the latest trends and techniques in credit card fraud and forgery. The database contains general information along with forensics data that may be used to track fraud instances and fraudsters. It should be noted that anti-fraud departments in the payment card industry also have access to this database. The database allows for the secure sharing of up-to-date information on credit card fraud. The information sharing has allowed investigators to link previously unconnected investigations across different countries and regions.[50] The payment card database offers an example of how Interpol might be better drawn into a coordinated effort against malicious actors using botnets and botnet masters.

Assuming that Interpol does not already have a botnet database, Interpol could develop similar global botnet databases that allow law enforcement, and security experts, access to a global database with useful information for tracking botnets.

As previously shown in **Chapters 3 and 4**, law enforcement currently are limited to the type of information that they are able to collect about botnets. Combating botnets is predominantly performed by security communities, computer security companies, and increasingly by ISPs and DNS registrars as will be demonstrated in **Chapters 7 and 8**. There is currently no global database available for law enforcement to obtain useful and time-sensitive data on botnets. Such a database could potentially be useful in seeing the overall picture of botnets, how they are related to various cybercrimes, and highlight bridges between cybercrimes and money laundering. Interpol is in a good position to develop such a database as they are a well-established and trusted organisation.[51] While Interpol's current role in combating malware and botnets is non-existent, they are well-placed to play a future role in the area as a trusted point of information sharing for law enforcement purposes. Certification authorities such as US Cert and AusCERT play an important role in information sharing of computer security threats such as malware. The type of information shared, however, is typically of a technical nature with descriptions of new threats. This is not the type of information sharing as seen and in **Chapter 3** necessary for law enforcement in tracking and prosecuting botnet masters.

---

[50] Newton, J. (2004), "Interpol and the cards industry: global partnerships to deliver local solutions", in Broadhurst, R. (Ed.), note 17 above.The author describes law enforcement investigation of what appeared to be isolated attacks of ATM in Canada, which were then later linked through the Interpol database with incidents in Canada, Chile, Colombia adnthe USA with ties to organised crime in Venezeula.

[51] Others have argued for a secure global database for combating malware and botnets. *See, for example*, Allman, M., Blanton, E., Paxson, V. And Shenker, S. "Fighting Coordinated Attackers with Cross-Organizational Information Sharing" Records of the 5th Workshop on Hot Topics in Networks, Beckman Centre 2006.

5.4 INTERNATIONAL AND REGIONAL INITIATIVES

There are a number of other international organizations that have formed working parties on issues of cybercrime and transnational cybercrime, funded research, produced best practice guidelines, and established national points of contact for exchange of information for transnational organised criminal activity. These groups include the Organization for Economic and Cultural Development, the Asia-Pacific Economic Cooperation (APEC), the Council of Europe, and the G8 group of nations, the Organisation of American States (OAS), and the Association of South East Asian Nations (ASEAN). These organisations pursue international aspects of communications policy relating to e-security, critical infrastructure protection, authentication, privacy, malware and spam. The works of these organisations have been excluded from a detailed analysis as they are of a limited relevance to combating botnets.[52]

5.5 THEORETICAL FRAMEWORK

It has often been thought that international harmonisation of cybercrime laws will offer a powerful tool to combat cybercrime. While it must be recognised that accession to the *Convention on Cybercrime* will prove useful to law enforcement for investigations involving multiple jurisdictions, the utility of the Convention will in many ways be contingent on law enforcement's ability to traceback to the criminal. Harmonisation of law across jurisdictions will occasionally benefit law enforcement in the prosecution of a botnet master, such as in the take down of the Mariposa botnet, where the botnet masters were identified. Identifying botnet masters, however, is a rare occasion. The main problem for botnets is not the lack of harmonisation but the ability to identify anyone to be prosecuted in the first place. As will be seen in **Chapter 6,** this is in many instances a difficult if not impossible task. Under Lessig's paradigm, the direct regulation in the form of international criminal sanction will ultimately have a limited impact on the botnet master. Indirect regulation that offers to reconstruct the architecture facilitating botnets is imperative and will be examined in **Chapters 7 and 8**, and then revisited in **Chapter 9**.

5.6 CONCLUDING REMARKS

This chapter has compared the Australian cybercrime framework with the provisions found in the Cybercrime Convention. It has been recommended that Australia should accede to the

[52] More information about how such international and regional organisations are involved in cybercrime, *see* Broadhurst, note 17 above.

Cybercrime Convention. I have made several recommendations which include:

- Australia should include a mandatory dual criminality provision for mutual assistance.
- Clear language on data retention and disposal and security standards should be given to ISPs.
- The misuse of a device provision should be modified so as to implicitly include botnets.
- Guidelines are required as to how long law enforcement may seize a computer or a computer system without laying charges

Privacy and freedom of expression concerns of law enforcement detection, monitoring and retaining of Internet traffic data will be explored in **Chapter 7**.

The obfuscation techniques as explored in **Chapters 3 and 6** render many of the procedural aspects of the *Cybercrime Convention* of little to no utility in relation to botnets. Where cyber-criminals are unsophisticated (do not use obfuscation technologies), or where they are sophisticated but, being human, make mistakes, and where that operation is transnational, the *Convention* may aid in prosecuting botnet masters. For the reasons previously stated in Chapters 4 and 5, criminal law will play a limited role in combating botnets.

Interpol has been an underutilized organisation so far in combating botnets. Interpol is well situated to provide a secure botnet database to be used by law enforcement and security organisations to better track, mitigate and eventually prosecute botnet masters. Such a database could be useful in proactively tackling botnets. Currently, there is no publicly available information to indicate that Interpol will develop such a database or that it intends to prioritise combating botnets as one of its key focus areas.

Chapter 6

CHALLENGES IN THE INVESTIGATION AND PROSECUTION OF BOTNET MASTERS

Table of Contents

6.0 AIMS OF THE CHAPTER

The ability of law enforcement to successfully investigate a botnet is often thwarted by generic challenges arising in what are referred to as high tech crimes[1] and technology related cases. Where a botnet is involved, cybercrime may take several forms. This includes but is not limited to fraud, identity theft, and corruption of personal information (Eg. unauthorised access to data), dishonest use of a computer, unsolicited email and misleading and deceptive practice. Botnets are often used as a tool to commit these forms of cybercrime as seen in **Chapters 3 and 4**.

Law enforcement faces many significant challenges in prosecuting botnet masters. For a variety of reasons, very few botnet related cases are prosecuted. Botnet related crimes such as fraud are rarely reported. Many cybercrimes are committed by people in distant jurisdictions. International cooperation is required, but is difficult to get, and very slow. The gathering of evidence requires forensic specialists, who are in short supply. Technical complexities abound. The laws relating to digital evidence are still immature. Even if cases were mounted and won, the penalties may not

[1] The term "cybercrime" is often used inter-changeably with 'high tech crime' and "Internet crime."

act as an effective deterrent, particularly given the scale of the financial benefits yielded to cyber-criminals. This chapter examines issues in digital evidence and forensics, including some generic issues surrounding attributes of digital evidence, real-time forensics, interception and warrants, difficulty of traceback, and jurisdiction. All of these problems are explained in greater detail and are interwoven in the analysis in both this and the succeeding chapters (**Chapter 4 "National Criminal Landscape"** and **Chapter 5 "International Criminal Framework")**.

Botnets have not previously been examined in the context of challenges and obstacles to law enforcement. This thesis provides a comprehensive examination of legal issues surrounding a criminal investigation of a botnet and prosecution of a botnet master. This chapter addresses botnets within broader themes of criminal investigation and prosecution including digital evidence and forensics, the warrant framework, damages and jurisdictional issues. It explores some fundamental issues which form building blocks for the subsequent chapters that will examine the national and international criminal legal framework for botnet control.

6.1 DIGITAL EVIDENCE AND FORENSICS

High tech crimes are often the most difficult crimes to prosecute.[2] This is due to a number of concerns stemming from digital evidence and forensics. These concerns are examined below, commencing with more generic concerns and moving to issues of acute relevance in regard to botnets such as warrants, real-time forensics, damages and jurisdiction.

6.1.1 Complex Technical Dimensions

The difficulties involved in explaining the technical complexities alone are enough to sink a case.[3] Imagine presenting a case where the crimes committed are explained by, "a root access by a buffer overflow in which memory was overwritten by other instructions which allowed the attacker to copy and execute code at will and then delete the code, eliminating all traces of entry (after disabling the audit log-in, of course)." [4] While it is true that lawyers and judges are called upon to understand a wide variety of non-legal concepts, special education and training for

[2] Phair, N. *Cybercrime: The Reality of the Threat* (self-published 2007) p. 156-160.
[3] Choo, R., Smith, R. And McCusker, R. Future Directions in Technology Enabled Crime (Australian Institute of Criminology 2007-2009) page 87.
[4] Pfleeger, C. and Pfleeger, S. *Security in Computing* 4th Ed. (Prentice Hall, 2006), p. 682

judges and law enforcement is advanced by many as an imperative.[5] The High Tech Crime division of the Australian Institute of Criminology (AIC) has expressly acknowledged that there is a general lack of trained computer forensics experts in Australia which necessitates outsourcing forensics work to 'non-police'. As the AIC notes:

> "Criminal courts hearing cases involving technology-enabled crime ... have difficulties where there is often the presentation of complex and technical evidence, the heavy reliance on expert opinion in technology-enabled crime cases, the use of complex and novel arguments relating to admissibility of evidence or the exercise of discretions, difficulties of juror comprehension of offence elements and evidence, the use of novel defences and defence arguments and devising appropriate sentences for convicted offenders ."[6]

A number of issues are presented in the above passage with technical complexities only accounting for part of the problem. Issues in evidence collection (section **6.1 "Digital Evidence and Collection"**), warrants (**section 6.1.4 "Warrants"**), and novel defences (**section 6.1.3 "Integrity, Volatility of Evidence and the Trojan Horse Defense"**) are explored later in this chapter. There are many issues, however, that arise long before charges are laid and perpetrators are before a court. Such evidentiary issues are explored in **sections 6.1.3-6.1.7** of this chapter, and were previously explored within specific contexts in section ***R v. Walker*** **of Chapter 4** (prosecution of a botnet master), in **Chapter 5** (procedural provisions of the *Council of Europe's Convention on Cybercrime*), and will be explored again in **Chapter 7** (the role of Internet Service Providers),and **Chapter 8** (self-organised security communities).

The technical complexities of botnet prosecution mean that in the rare event that identification of a botnet master is discovered and evidence preserved, there is a significant chance that the botnet master will escape punishment due to the lack of understanding and training of the judges and jurors.

6.1.2 Large Volumes of Data

Often digital forensics involves the examination of large amounts of data, perhaps best illustrated by way of example:

> "The amount of information gathered during the investigation in Operation Firewall by the United States Secret Service is estimated to be approximately two terabytes – the equivalent of an average university's academic library."[7]

---

[5] *See for example*, Telstra Submission 43 for the House of Representations Communications Commission Inquiry into Cyber Crime available at http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub43.pdf (last accessed Feb. 8, 2011).
[6] Choo, note 3 above, page 87.
[7] Choo, note 3 above, p. 88.

A typical medium sized company will have at least 600 terabytes of information on its server. It would take over 4 years to analyse and image the entire server.[8] Put another way, "The difference in conducting an analysis on such a large volume,... would be equivalent to interviewing every person who lives on a block where a homicide has occurred (reasonable), versus interviewing everyone who lives in the city of the homicide victim (not reasonable)."[9] The best way from a forensics standpoint to analyse large volumes of information is by shutting the server down. This is not possible in nearly all scenarios as shutting down a server would result in severe economic loss for a corporation, organisation or Internet Service Provider (Eg. shutting down a bank's network for several days), or might entail shutting down critical services such as the electrical grid, transportation or healthcare databases. In order to reduce process time, digital forensics analysists often use examination analysis techniques such as hash filtering which impact on processing time as well as the accuracy of the results.[10] The result is that the digital evidence collected *may* not be sufficiently accurate to successfully prosecute a botnet master. It may also be the case that due to the amount of data collected, law enforcement is not able to justify the expenditure of time and resources required to sift through such large quantities, especially for a crime with low provable damages (**section 6.1.7 "Damages"**). These issues ultimately influence whether law enforcement decides to actively investigate and pursue prosecution of botnet masters.

6.1.3 Integrity, Volatility of Evidence and the Trojan Horse Defense

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

[8] 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), page 92.
[9] Reyes, note 8 above, page 93.
[10] Reyes, note 8 above, page 57.

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.[11] 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" defense, 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 botnet, it may seem odd that a "Trojan horse" defense 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.[12] 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.

---

[11] Forensics training by Nick Klein, forensics expert and former member of the Australian Federal Police, "Cybercrime, Cyber Security and Digital Law Enforcement" Sydney, March 2010.

[12] 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 (last accessed April 27, 2010). Some details of the case are also described in Grabosky, P. *Electronic Crime* (Prentice Hall, 2007) page 80-81 and by Brenner, S., Carrier, B. and Henninger, J., "The Trojan Horse Defense in Cyber-Crime Cases" (November, 2004) Santa Clara Computer and High Tech Law Journal Vol. 21.

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 the defendant's computer.[13] 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."[14]

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.[15]

6.1.4 Warrants (Content)

Evidence must be collected in compliance with the law. The investigation of a botnet requires collecting information that would be likely to be classified as content monitoring in Australia. Content monitoring refers to both the examination of communications as well as the attributes of a communication. For example, this might include looking at the text of an email or the conversation of a VOIP call, and it also includes the monitoring of communication attributes such as the examination of traffic connecting to and from a website, email box or VOIP number (which IP addresses or VOIP numbers are being connected to, what ports are used, what type of files are sent, Eg. .exe files). In nearly all instances, examination of the content of a communication requires a warrant. Issuing a warrant often requires the approval of a judge and requires specification of search content along with a number of other requirements depending on the type of warrant (the types of content warrants are examined in **Figure 6(A)**). As seen in **Chapter 3**, where a botnet is used, often real-time collection of data is imperative. This type of evidence collection typically requires evidence to be collected at the points where the command

[13] Grabosky, P. *Electronic Crime* (Prentice Hall, 2007) page 80-81.
[14] The quote is found in Brenner, S. et al., note 12 above.
[15] For a summary of forensics issues in the presentation of cases *see* 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). *See also* Smith, R., Grabosky, P., and Urbas, G. *Cyber Criminals on Trial* (Cambridge University Press, 2004).

and control is located. This may be in the IRC, in a P2P network, or within specified webpages. In the case of the Waledac botnet, as seen in **Chapter 3**, the primary command and control was linked to over 270 webpages. In order to collect evidence, often a virtual honeypot is used. Virtual honeypots were examined in **Chapters 3 and 4** and will be considered again in **Chapter 8** when looking at legal issues in security research**.** ISP cooperation was examined under the procedural provisions of the *Council of Europe Cybercrime Convention* in **Chapter 5**.

The warrant framework may be used to compel an ISP or a similar entity to collect, preserve and intercept communications. In theory, warrants could be issued to gather evidence about a botnet and the infected bots and to identify the botnet master. As will be seen in **section 6.1.6**, tracing network evidence back to an individual botnet master poses one of the greatest challenges to the prosecution. In practice, as will be illustrated further in this section, law enforcement is precluded from gathering traceback evidence in botnet investigations, with the exception of a low level botnet master with deficient technical skills and who uses amateur techniques (discussed below). Nonetheless, if a warrant is sought to monitor and collect evidence, typically this will involve what is known as content monitoring. The collection and monitoring of the content of a communication falls within the *Telecommunications (Interception and Access) Act 1979 (TIAA).* Call charge records, by contrast, are regulated by the *Telecommunications Act 1997 (TA).*[16] It is prohibited to monitor and disclose the content of communications without the customer's consent.[17] Unlawful collection and disclosure of the content of a communication attracts both civil and criminal sanction.[18] The *TIAA* and *TA* expressly authorise a range of disclosures including to specified law enforcement and revenue protection agencies.[19] The content warrant regime in Australia is inherently complex. **Figure 6(A)** on the following page maps the various types of warrants required in Australia for content monitoring and details the different requirements for each type of warrant.

[16] Part 13 of the *Telecommunications Act 1997*. *See also* Waters, N. "Government Surveillance in Australia" in Rule, J. (ed) *Privacy under Pressure* (2006), page 7-10. Paper on file.
[17] Part 2-1 section 7of the *TIAA 1979* prohibits disclosure of an interception or communications, and Part 3-1 section 108 of the *TIAA 1979* prohibits access to stored communications.
[18] Criminal offences are outlined in Part 2-9 of the *TIAA 1979* while civil remedies are outlined in Par 2-10 of the *TIAA 1979*. ISP liability for unlawful disclosure is discussed in **Chapter 7.**
[19] Waters, note 16 above, page 10.

Figure 6(A): Content Warrant Framework in Australia

TYPE OF WARRANT	LEGISLATION	REQUIREMENTS & RANGE OF BOTNET ACTIVITIES
Part 2-2 **Telecommunications Interception Warrant**	Part 2-2 *Telecommunications* *(Interception and Access) Act 1979* *(TIAA 1979)*	Issued by Attorney General (AG) under request of Director of Security (DS) or The Australian Security Intelligence Organisation (ASIO) in connection with national and foreign intelligence, in writing with specified duration, identification of suspected telecommunications system or named person, and reason (offense) warrant is required. Such warrants would be required, for example, to gather evidence of a denial of service attack of a government website or server; or any unauthorised access, modification or impairment of data where these are related to government websites or in relation to national security matters; or any type of botnet activity with ties to transnational organised crime or terrorism.
Part 2-5 **Telecommunications Interception** **Warrant**	Part 2-5 *TIAA 1979*	Not issued by the AG but by a judge or other agent nominated by the Minister. Requests are from Australian Federal Police, State Police, and a number of commissions connected with policing (Eg. Australian Criminal Commission). Required, for example, for collecting evidence of denial of service attack of non-government website or server; any unauthorised access, modification or impairment of non-government data; or offences linked to botnets such as fraud, click-fraud, spam, and distribution of child pornography.
Part 2-3 **Emergency Telecommunications Interception Warrant**	Part 2-3 *TIAA 1979*	May be request from police officer where there is likelihood of death or serious injury. For example, a botnet could result in death or serious injury where it is used to target, for example, airport traffic, hospital networks, or road system

		traffic lights.
Stored Communications Warrant	Schedule 1 of the *TIAA 1979*	Issued by AG if request is from DS or the ASIO. Issued by judge or magistrate when request from law enforcement. Application may be in writing or by telephone with respect to a telecommunications system or named person outlining grounds (offense) application is based on. May be issued to access stored communications only and does not apply to communications in transit. Required, for example, for an examination a of the content of an email – used to collect evidence once the identity of a botnet master is known.
B-Party Warrant	Schedule 2 *Telecommunications (Interception) Amendment Act 2006 (TIA 2006)*	Issued by AG if request is from DS or the ASIO (valid for 3 months). Issued by judge or magistrate when request from law enforcement (valid for 6 months). Warrants issued to intercept communications of persons who are reasonably suspected of being engaged in criminal activity where this may extend to innocent third parties indirectly engaged with crime suspects. This applies only in instances where the telecommunications service or named person linked to the criminal offense is unknown. For example, examination of compromised machines / bots to see how they connect to the Command and Control.
Equipment-based Warrant	Schedule 3 *TIA 2006*	Issued by the AG under request made by DS. Allows interception of telecommunications devices. Required, for example, for the examination of a piece of equipment, ie. computer, and image the entire content of a computer, not just the content in an email box. No indication if remote examination of the device is allowed by downloading software onto the suspect's computer.

No Warrant Required	*Telecommunications (Interception and Access) Amending Act 2010*	Carriage Service (Eg. ISP) is allowed to monitor content if done for "network protection duties." The ISP may voluntarily share information collected with law enforcement. For example, the vast majority of evidence collection for botnets is performed by security researchers and by ISPs. This includes detection and monitoring of networks and virtual honeypots. ISPs do not require a warrant. Security researchers, as seen in **Chapter 4**, operate in an ambiguous legal space; they cannot obtain a warrant, nor are they permitted to do research without a warrant, and there is no exception to the computer offences for security research purposes.

What type of warrant would law enforcement request to track and prosecute a botnet master? Before deciding on what type of warrant is required by law enforcement, a significant amount of information is required. Most investigations, as seen in **Chapter 3**, are the result of research and evidence collection from security organisations, ISPs and researchers which is then handed over to law enforcement. Law enforcement agencies are not equipped with the legal authority (and perhaps technical ability depending on the department in question)[20] to perform many of the tasks required to gather intelligence on botnets.

Let us suppose for instance that we had an amateur botnet operated by one botnet master located in Australia from a machine with a static IP address who only had one Command & Control (C&C) domain name page established. This particular botnet which we will label, Dumb Botnet, controlled 100 computers – all with IP addresses in Australia. As all the required links including the botnet master, bots, C&C, and IP addresses are all located in Australia no jurisdictional issues are present and law enforcement may use the Australian content monitoring framework without concern of involving international coordination of law enforcement and ISPs. In order to uncover more information about Dumb Botnet through content monitoring, law enforcement would initially need a piece of important information to justify a warrant. This

[20] Not all States have dedicated cyber crime or high tech crime units, while others with such specialised units may lack the resources required to properly investigate botnets.

could mean that law enforcement would require information about either the C&C, or the botnet master, or the compromised machines that form part of the botnet.

If law enforcement agencies had location information of the C&C (Eg. receiving instructions from a fictitious website www.netar.com.au[21]) of Dumb Botnet, law enforcement could request a Part 2-5 Telecommunications Interception Warrant over a 'telecommunications system' to monitor traffic connecting to and from this C&C. This is not as easy as it sounds. Knowledge of a webpage and an IP address does not provide information about subscriber information. It does not tell us the domain name service registrar where www.netar.com.au was registered. And it does not tell us which ISP is hosting www.netar.com.au. Law enforcement agents will make a request using the WHOIS protocol to access subscriber information for a domain name or IP address.[22] ISPs send subscriber information to the WHOIS servers which keep a comprehensive database of subscriber's information. This protocol allows systems administrators (and law enforcement in some instances) to obtain the subscriber's name (when a fake identity has not been used) along with contact details. The WHOIS protocol and servers are considered again in **Chapter 7**. Without the use of WHOIS, law enforcement agents can still identify the domain name service registrar and ISP but the task is more arduous and cumbersome than using the WHOIS protocol. Assuming that the C&C was known (Eg. resolving to IP address at www.netar.com.au) and that law enforcement was able to identify the appropriate ISP, a law enforcement agent could then apply for a Part 2-5 Telecommunications Interception Warrant. A warrant to monitor the traffic of www.netar.com.au (the C&C) could reveal IP traffic to and from the C&C (an IP address or possibly a range of IP addresses). These would be compromised computers, and *possibly* the IP Address of the botnet master (in our example, these entities are located in Australia so the investigation will be easily continued).

If law enforcement only had information about which computers were infected, they could request a B-Party Warrant but only where they had no information about the botnet master. Where there is information available about the perpetrator of a crime, a B-Party warrant will not be authorised. If law enforcement knew the IP address of the botnet master they could request a 'named persons' Part 2-5 Telecommunications Interception Warrant. They could then monitor

[21] This is a fictitious website name.

[22] Other protocols such as the Internet Registry Information Service (IRIS) are being developed by the IETF to eventually replace the WHOIS protocol. It is hoped that IRIS will be less privacy invasive, will reduce the use of database for marketing, will allow more efficient access by law enforcement, and will reduce the accuracy of the contents of the database. See WHOIS Task Force at http://www.gnso.icann.org/issues/whois-privacy/whois-tfl-preliminary.html#GTLDRegistriesconstituency (last accessed April 30, 2010).

all traffic of the botnet master. Law enforcement agents could also request a Stored Communications Warrant to examine the content of information, for example, in any email communications of the botnet master. With luck, law enforcement agencies, once the IP Address was identified, could obtain a warrant to search and seize the computer of the botnet master and potentially uncover further evidence linking him/her with the crime. It is possible that, in a situation like Dumb Botnet, existing content monitoring provisions are sufficient for law enforcement agencies to investigate a botnet master. The problem with this example is that even amateurs operate much more sophisticated botnets than Dumb Botnet as was seen in the examination of the amateur botnet master, Owen Walker, in **Chapter 4**. Walker's botnet, Akill, was additionally explored in **Chapter 3.**

In a *typical* botnet, there will be several C&Cs to retrieve instructions. Many botnets will change the location of the C&C every week, others every day. Webpages of C&C are typically registered with registries that are known to be lax in their practices and uncooperative with security researchers and law enforcement in either blacklisting or domain name removal. Many of these reticent domain name registrars are located in countries with no cyber crime laws – Australia is not one of these. In most instances, knowledge of the C&C will not produce information about a botnet master. Many botnet masters use a dynamic system where their IP address changes every 20 minutes. Additionally, many communications sent to the C&C are encrypted and thus not easily decipherable. Tracing back to an individual botnet master is virtually impossible. Having a valid warrant to collect information over a telecommunications system might lead to the shutting down of one C&C, but the botnet is programmed to automatically receive its instructions from a new C&C source. Many botnets contain hundreds of thousands if not millions of infected computers. A B-Party warrant would be possible in this instance for an infected computer located in Australia though not much information leading to prosecution of a botnet master may be gained from doing so.

In summary, warrants by law enforcement to investigate botnets are of limited use. Furthermore, as highlighted in the Torpig botnet example in **Chapter 3**, once law enforcement became involved in taking down the C&C sources, the C&C automatically shifted to a much more secure method using the encrypted Mebroot pathway embedded in the rootkit. The botnet masters seemed more than willing to let the security researchers of the virtual honeypot gather intelligence on its operations for a sufficient period of time to collect useful information but once law enforcement was involved, the botnet mutated within a day.

6.1.5 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. Privacy and surveillance issues are explore in the context of ISPs in **Chapter 7.**

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 (Netflow is discussed further in **Chapter 7**) 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, as will be explored in **Chapter 7** 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. 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 (Part 2-5 Telecommunications Interception Warrant).

Unlike crimes in the physical world, often there is little physical [?] evidence after a botnet-related 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.[23] 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."[24]

Without real-time evidence, there is heavy reliance on the physical memory (RAM) of a computer. As demonstrated in **Chapter 3**, 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.[25] 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, and is the main criticism of the *European CyberCrime Convention* considered in **Chapter 5**. **Chapter 7** is devoted to the role of ISPs and DNS registrars.

[23] Reyes, note 8 above.
[24] Reyes, note 8 above, page 107-108.
[25] Above, page 103.

ISPs were required by law to have interception capabilities[26], generally to be used for evidence gathering in connection with serious offences (crimes such as murder, terrorism, and child pornography).[27] This obligation of ISPs to have interception capabilities no longer exists (section 324 of the *TA* has been repealed). This is somewhat odd given that ISPs still have obligations to intercept communications but no longer have an obligation to have interception capabilities. Before section 324 was repealed, interception was limited to serious offences. A serious offence included any criminal offence which would attract a minimum of 7 years in prison. The unauthorised access, modification and impairment provisions attract a penalty of up to 10 years but do not specify a minimum sentence.[28] As there was no minimum sentence specified and no caselaw in Australia related to botnets, it was not possible to ascertain if the threshold of "serious offence" was met. The use of a botnet *could* qualify as a serious offence but this would likely only occur in a small number of instances where the unauthorised access, modification and impairment was done with intent to commit a crime. A "serious offence" would also likely occur where a botnet was used to commit identity theft or serious financial fraud. As section 324 has been repealed, there is no longer the requirement that interception only be used in the case of a serious offence. Law enforcement agents are now able to compel ISPs to intercept communications between parties regardless of whether the offence is of a serious or minor nature.

Australian ISPs are neither legally required to have the ability to collect evidence in real-time nor are they required to have interception capabilities. ISPs still have obligations to intercept communications but they do not appear to have the direct obligation to collect evidence in real-time. On the face of things, this seems counter-intuitive. Many of the technologies used in interception are similar to those used in real-time evidence collection. It is difficult to imagine therefore, that all Australian ISPs would not already have both capabilities. It is a complex area with little publicly available information as both law enforcement agents and ISPs do not disclose the specifics of the technologies used or how they are implemented.[29] My understanding of the technologies involved is that an interception tap monitors IP traffic data to and from an IP address or range of addresses (or VOIP phone number). This collection is

[26] Section 324 of the *Telecommunications Act 1997* required carriage service providers (which includes ISPs) to be able to intercept a communications passing over the network or facility in accordance with a valid warrant under the *Telecommunications (Interception and Access) Act 1979*. This provision has been repealed and amended several times. *See* amending acts No. 200, 1997, No. 35, 2004, No. 40, 2004 and No. 177, 2007.
[27] Section 5D *TA*
[28] See sections 474 generally of the *Criminal Code (Cth)*.
[29] Enquiries were made to several CIO of ISPs as well as forensics experts working for the Australian Federal Police where these entities repeatedly stated that they were not authorised by law to disclose the types of technologies used for interception and real-time evidence collection.

performed in real-time. The type of technology, however, that is required to access stored communications requires the ability to take a snap-shot of a suspect's email box (peer into the actual communication) or website. This is clearly more invasive collection of data. This is also real-time data collection.

To summarise, the *TIAA* and *TA* do not mandate interception or real-time evidence collection capabilities. The *TIAA* and *TA* do not make reference to real-time evidence. The TIAA does, however, allow for stored communications warrants. There is no argument, therefore, in Australia that ISPs would be required to substantially commit additional resources to purchase and operate interception and real-time evidence technologies; those capabilities should already exist.

Real-time evidence (also referred to as live forensics) is vital in many cybercrime investigations. In particular, the use of real-time evidence technologies allows law enforcement the ability to intercept and search information that is encrypted. This is perhaps the most distinctive advantage of the use of real-time evidence techniques. In postmortem forensics, the password (often a key) must be known for the encrypted file. The information that can be found in encrypted files using post-mortem techniques is very limited. With the use of real-time or live forensics, software could be remotely installed onto a computer system prior to an incident (Eg. Pre-Deployed Agent model) or software programs (Eg. BestCrypt or ProDiscover IR) can be initiated once a document is first opened. When the document is opened the contents are not encrypted thus the surveillance device can take a snapshot of everything on the screen. This essentially allows in many instances "the investigator to image the physical memory of the computer system and glean useful information about what files and programs the suspect may be currently using."[30] Where the entire system is encrypted, the entire content of the drive would be able to be viewed because "Simply put,... while the drive is presently being used, it is unencrypted."[31] It remains unclear whether ISPs have real-time evidence technologies capable of performing the above acts as monitoring of a suspect's computer (and not specifically the content of emails) is not contemplated with a stored communication warrant. The equipment warrant does not specify whether remote searches are allowed. In the instance of real-time data collection a file would be downloaded remotely onto a computer and the entire content of the computer is imaged.

[30] Reyes, note 8 above, page 96.
[31] Above, page 99.

The interception and examination of communications in Australia requires a warrant in most instances. Warrants, as seen in **section 6.1.4**, vary depending on the type required and the requesting party. However, interception of communications, as will be shown in **Chapter 7**, by ISPs for the purpose of network protection, does not require a warrant. The importance of real-time forensics capability is re-examined in **Chapter 7.**

6.1.6 Traceback and Identification of Perpetrators

The greatest obstacle to a botnet prosecution is identifying the botnet master(s). Traceback refers to steps taken to track the evidence from a crime backwards with the goal of identifying the perpetrator of a crime. This means tracing back to the IP address of the botnet master. With botnet related crimes, traceback is not possible in most instances. Where traceback is possible, it may still be undesirable to investigate due to intensive amount of resources and money required compared with the amount of damage suffered. This is often described as the "de minimis trap" or the "salami technique"[32]. As Wall writes, "A common characteristic of many cybercrimes is that they lead to low-impact, bulk victimizations that cause large aggregated losses which are spread globally, potentially across all known jurisdictions." In other words, you steal a little bit of money from a lot of people who are located in many countries. The minimum amount necessary to commence an investigation is not met. The capacity of law enforcement to investigate botnet related crimes, therefore, is limited.

Traceback is difficult predominantly due to the obfuscation methods deployed by malware actors – typically organised crime groups. Organized crime groups use a variety of common techniques to evade technological controls and legal sanction. Most sophisticated malware operations make detection and blocking difficult. Many different techniques exist to make botnets robust, covert, and undetectable. Such commonplace techniques include dynamic DNS/multihoming, FastFlux DNS, distributed command and control (superbotnet), encryption, obfuscation and the move from open IRC channels to closed peer-to-peer channels, and the hijacking of open wireless networks. These tactics allow the host to roam and change intermittently as required to keep a botnet functioning. Malware operators employ the same strategem to keep spam and illicit content rotating. These techniques and strategies were outlined in **Chapter 3.** These

[32] According to Security Borders Beyond, the salami technique is "A white collar fraud scheme in which small amounts of money, frequently less than a dollar in each instance, are diverted from many separate accounts and credited to an account controlled by the perpetrator, usually with the help of a computer." See http://securitybordersbeyond.org/global-security-glossary-global-security-glossary-s/ (last accessed December 10, 2010).

techniques include dynamic DNS (multi-homing), fast-flux, double fast-flux (distributed command and control), encryption, anonymising technologies, peer-to-peer communications and onion routing.

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."[33]

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. As shown in **Chapter 3**, 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.

In the event that traceback is possible jurisdictional issues may arise. Often botnet masters are located in another country. As a result of difficulties in traceback and jurisdictional issues, domestic investigation targets the 'traceable' element in the chain of fraudulent activity – the

[33] Lovet, G., "Fighting Cybercrime: Technical, Juridical and Ethical Challenges" (Paper presented at the Virus Bulletin Conference 2009, Geneva, 23, September 2009), page 2.

money mule.[34] Money mules refer to those who, often innocently and unknowingly, launder money on behalf of criminals. Law enforcement investigation of money mules was discussed under "Aiding and Abetting" in **Chapter 4.**

The use of obfuscation technologies make traceback of a botnet master unlikely, and where possible, traceback has been done effectively by security researchers and organisations as seen in **Chapter 3** with the Mariposa botnet.

6.1.7 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.[35] For identity theft related cases the amount is a pure conjecture – in the case of having a device or computer program designed to steal personal information, or for forgery, the projected amount of damage or money stolen is $35 000 in order for an arrest to be made.[36] These thresholds are determined by internal police working committees. Not all law enforcement investigation units have minimal monetary amounts. Not all jurisdictions, however, have a minimum damages rule. New South Wales, for instance, does not. A decision to launch an investigation in the case of fraud related cybercrimes is dependent on a wide range of factors which include whether the crime is serious or organised crime (as was seen in **Chapter 4**) and whether the investigation is within the capabilities of the local police. [37]

Damages cannot be aggregated. For example, if a botnet master installs Trojans that steal personal information, then uses the information to steal $100 from 100 individuals, the damages or money stolen may not be aggregated to $10 000. In some instances, investigations are not performed. This is true of State authorities but not necessarily of specialised cybercrime units in the FBI or AFP who are not restricted by monetary thresholds. In other jurisdictions such as Canada, provinces have signed Memorandum of Understanding between law enforcement

---

[34] Bruce Van Der Graf, James McCormick, AusCERT stated in conferences and confirmed in caselaw to be examined in next chapter.
[35] de Villiers, M. "Virus Ex Machine Res Ipsa Loquitor" (2003) Stanford Technology Law Review 1.
[36] INSIGHT, "Stolen ID" (December 14, 2008) available at http://news.sbs.com.au/insight/episode/index/id/30 (last accessed February 11, 2011). Law enforcement from Queensland was involved with this news program. I too was interviewed for the same program.
[37] Correspondence with Detective Van der Graf, head of the Fraud Squad, New South Wales Police. Notes are on file.

agencies in order to allow for aggregate damages or for 'de minimus' fraud thresholds to be met forcing an investigation.[38]

It is imperative that minimum thresholds be reconsidered in Australia. State police should be looking to adopt Memoranda of Understanding which would allow damages to be aggregated, and for full cooperation between State police departments for these type of "salami technique" fraud scams. It may be the case that $35000 is still an appropriate amount but this only makes sense where damages or amounts stolen may be aggregated between Australian States. The next move would see Memoranda of Understanding signed between nations to ensure that damages could also be aggregated between nations. As much cybercrime is transnational in nature with damages suffered by many victims from different nations, addressing the minimum damages threshold problem is something that requires urgent attention with an attempt to obtain cross-jurisdictional uniformity.

6.2 JURISDICTION

High tech crimes often involve parties located overseas. High tech 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 Australian police, for example, cannot obtain a warrant to wire-tap someone in Latvia and cannot they compel an ISP in Mongolia to provide data logs. This type of international policing requires the cooperation of law enforcement and courts in other

[38] See *See* United States -Canada Working Group, United States -Canada Cooperation Against Cross-Border Telemarketing Fraud (November 1997) available at http://strategis.ic.gc.ca/pics/ct/reporte.pdf (last accessed February 9, 2011).

jurisdictions. Law enforcement in Australia could contact law enforcement in the location of the botnet master 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.[39] In the case of hacking (unauthorised access) and fraud, the priorities are often disparate. This is especially true in jurisdictions without computer misuse offenses. 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. Fourth, a significant portion of the botnet industry is based in developing nations such as former Soviet satellite countries, and Brazil who have limited police resources and a relatively high level of corruption. The jurisdictional hurdles stem from practical considerations as well as a lack of criminalisation of an act across jurisdictions.

The Australian courts have taken a liberal approach to criminal jurisdiction. In *DPP v Sutcliffe*[40], the Supreme Court of Victoria interpreted the *Crimes Act 1958 (Vic)* in a way that allowed the accused to be tried where he lived. This case involved stalking and harassment over the Internet. The victim was located in Canada while the suspect was located in Victoria, Australia. Due to the high cost of extradition and the ease of dissemination of harmful material, the Supreme Court of Victoria concluded that there were compelling reasons to apply the Victorian *Crimes Act* extra-territorially.[41]

There are no reported judgments of cyber criminals being extradited to or from many hotbeds of cybercrime such as Eastern European countries, China or Brazil to Australia. This is to be expected given that Australia has not signed extradition treaties with many countries considered to be hotbeds of cyber crime though Australian has announced intention to accede to the *Cybercrime Convention* (examined in detail in **Chapter 5**). There have been no reported instances of botnet masters extradited to other jurisdictions where Australia has extradition treaties, such as Australia and countries such as the United States, the United Kingdom and Canada. The United States also does not have an extradition treaty with many former Soviet countries

[39] Wall, D., *Cybercrime: Crime and Society Series* (Polity Press, 2007), page 162.
[40] *DPP v Sutcliff* [2001] VSC 43.
[41] An excellent account of the decision is found in Fitzgerald, B., Fitzgerald, A., Middleton, G., Lim, Y. and Beale, T., *Internet and E-Commerce Law: Technology, Law and Policy* (Thomson 2007) page 111.

considered hotbeds of cybercrime. This has not prevented the United States, however, from actively pursuing and prosecuting cyber criminals located overseas as will be seen in the example below.

As a result of the law enforcement disparity between nations' police resources and a lack of formal cooperation in investigating and extraditing cyber criminals, many nations are increasingly treading in murky legal territory whereby searches are performed and evidence is gathered trans-nationally. Law enforcement agents in one jurisdiction will remotely install a keylogging program onto a suspect's computer though this is not currently a procedure performed by the Australian Federal Police.[42] Many jurisdictions such as those within the European Union have legalised overseas remote computer searches.[43] Police in some European nations have been using remote searches without a warrant for several years. The German Constitutional Court recently ruled that the practice of cyber-spying violates privacy rights.[44] German police will still be allowed to use remote searches but only in exceptional cases under the auspices of a judge. The German police have estimated that they will likely need to use remote searches approximately 10 times per year.[45] The European Union Council of Ministers will expand a statute permitting warrantless surveillance including remote searches of email, instant messaging and Internet browsing history.[46] The Home Office of the United Kingdom has also authored remote searches by police.[47] In jurisdictions such as the United States, the technique is used but it remains unclear if it is legal.

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 §

[42] Question posed to AFP at High Tech Crime Conference (2010) Sydney. Notes on file with author.
[43] Closed panel on Cybercrime at AusCERT 2008 with Chatham House Rules. Law enforcement agents from the AFP, NSW, Germany and the FBI were present.
[44] The decision was handed down by the German Constitutional Court. *See* Zitierung: BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (last accessed February 10, 2011). Salient points of the decision were translated by Isabel Sickenberg and are on file.
[45] Above.
[46] The Council of the European Union, "Strategy to Combat Cybercrime" (2010) 5957/2/10FR22.
[47] British law already allows police to remotely access computers under the *Regulation of Investigatory Powers Act 2000*.

1030 (1986), as well as 20 counts to conspire and a number of fraud counts.[48] 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.

Additionally, the Court stated that the Fourth Amendment did not apply as the defendant's computers and servers "are the property of a non-resident and located outside the US [as was] the data – at least until it was transmitted to the United States".[49] Once the FBI captured almost 250 gigabytes of data, it applied to the court for a valid warrant to search and seize the data. The Court ruled that the warrant was not required to install keylogging Trojans remotely without authorisation from the defendants or notification to Russian law enforcement or to collect data from such computers. The warrant was only required post-collection, once the data was considered to be in the US. The Court further held Russian law did not apply to the FBI's actions. There is no evidence suggesting that Australian law enforcement agents use similar controversial techniques such as remote keylogging without formal cooperation from overseas law enforcement or searching and seizing evidence without a warrant.[50]

As demonstrated throughout this chapter, the content warrant framework coupled with the use of obfuscation technologies necessarily means that law enforcement efforts to identify botnet masters through monitoring communications are unlikely to be successful. As seen in the Mariposa botnet in **Chapter 3** and as was seen in the case of *R. v. Walker* in **Chapter 4**, the mere identification of a botnet master by no means secures successful prosecution. In the case of the Mariposa botnet, this was due to the tardiness of the Spanish government to enact computer misuse offences in spite the fact that Spain ratified the Cybercrime treaty a decade ago. It remains to be seen if the evidence collected and obtained by security researchers will stand up in court or will be discarded. In the case of *R. v. Walker*, New Zealand law enforcement was given information from the FBI and authorities in the Netherlands who were investigating the DollarRevenue adware/spyware company.

If more botnet masters are to be brought to justice, and in particular the ones tied to organized

---

[48] *United States v Gorshkov* (2001) WL 1024026 (Western District Washington).
[49] Above.
[50] Direct question posed to Australian Federal Police at the 2010 High Tech Crime Conference, Sydney. Chatham House Rules. It was also noted that the Australian Federal Police would like to have this right of remote search on overseas computers. Notes on file.

crime and serious fraud, law enforcement agents will need to be given the tools that security researchers use. The role of security researchers was introduced in **Chapter 3** and will be the focus of **Chapter 8 "Self-Organised Security Communities"**. Security researchers are able to gather intelligence through virtual honeypots, infiltrate the C&C of a botnet, and in some instances where a botnet master is known, remotely install keylogging software to image the content of the botnet master's computer as well as incoming and outgoing web traffic. Law enforcement agents are not able to perform these functions.

Australia has announced that in addition to acceding to the *Cybercrime Convention*, a national working party will be formed to address cybercrime. The working party will be known as the National Cybercrime Working Group (NCWG). It is imperative that the NCWG consider whether and under what conditions law enforcement agents should be able to remotely install and search a suspect's computer. I am not convinced, however, that such a tool would have any significant impact on botnet investigations and prosecutions but it could prove essential for other instances of cybercrime. From my perspective, remote searching is a necessary tool in the fight against some perpetrators of cybercrime but such a tool should be limited to only a handful of situations involving very serious offences (Eg. terrorism, child pornography, human trafficking, murders) where evidence cannot be sufficiently gathered by other methods. Any use of a remote search should be done with a content warrant and under the supervision of a judge. A new content warrant may be required for this or the equipment warrant will need to be expanded so as to include the ability to remotely search equipment.

6.3 THEORETICAL FRAMEWORK

Lessig emphasized the modality of "code"[51] which I will refer to as "architecture'. As addressed in **Chapter 2**, it is not certain if Lessig intends a broad meaning that would include software, hardware, protocols and Internet standards. I will adopt the broader definition. This chapter extends the technical analysis from **Chapter 3** demonstrating how architecture has empowered botnet masters and, at the same time, has hampered law enforcement in its ability to successfully investigate and prosecute botnet masters. In Lessig's model, "architecture" is a constraint that regulates behaviour. As explored in **Chapter 3**, architectural features of the Internet presently serve as an enabler of criminal activity, with little to no constraints imposed on

[51] Lessig, L., *Code: And Other Laws of Cyberspace* (Basic Books, 1999), page 236.

the botnet master. It will be demonstrated in this chapter how some of the architectural features of the Internet enable cybercrime while, at the same time, hampering law enforcement.

"Law" is the core modality to be examined in this examination of digital evidence and forensics and the subsequent issues surrounding warrants and jurisdiction. The requirement of a warrant to intercept and collect evidence coupled with a lack of real-time forensic capability again restrains law enforcement in its ability to successfully investigate and prosecute botnet masters.

A legal framework communicates rights and obligations, encourages players to behave responsibly, and acts as a deterrent against irresponsible behaviour. It also creates the possibility of back-end controls, in the form of sanctions against organisations and individuals that misbehave, or at least opprobrium from `naming and shaming' but the effectiveness of this depends on norms. Hence, in theory at least, the law could be an effective safeguard for parties affected by malware and botnets. In practice, however, there are a number of legal and evidentiary issues making the law more of an obstacle to hurdle than a safeguard**.** The principle aim of this chapter has to demonstrate the limited role that law enforcement will play in the area of combating botnets. Technical obfuscation, such as fast-flux botnets, dynamic DNS and encryption, was introduced in **Chapter 1** and further elaborated in **Chapter 3.** Technical obfuscation refers to techniques which allow malicious actors to circumvent safeguards such as anti-virus and anti-spyware software as well as prevent law enforcement from being able to locate the perpetrator of a crime. This chapter further addresses technical obfuscation and looks at notions which could be said to be 'legal obfuscation'. Legal obfuscation refers to the ability to evade law enforcement through either legal loopholes or the inability of parties such as law enforcement or security organisations to combat botnets due to legal safeguards (Eg. no security research exemption for unauthorised access).

6.4 CONCLUDING REMARKS

This chapter has addressed the larger and more generic problems of investigating and prosecuting botnet masters. The chapter drew on the examples previously depicted in **Chapter 3** which discussed the Torpig, Webroot, Waledac, Mariposa and Mega-D botnets to better highlight significant challenges to law enforcement. These included issues in digital forensics, current obfuscation methods, the content warrant framework applicable to botnets, real-time evidence collection, traceback, and jurisdiction. This chapter included an examination of the

Australian content warrant framework as applied to botnets. My examination of the content warrant framework would be equally relevant to its use in combating other forms of crime committed with the use of malware.

I have concluded that amending the law to include remote searching through a content warrant would not have a significant impact on botnet investigation and prosecution. This is predominantly due to the limited role that law enforcement agents will play in the overall combating of botnets. The obfuscation methods used by botnet masters make investigations difficult and traceback extremely challenging. Where sufficient evidence has been gathered, there are a number of generic challenges that make successful prosecution unlikely including proving damages, jurisdiction issues, the volatility of digital evidence, the lack of education and training of technical matters of judges and jurors, and the possibility of the successful use of the "Trojan horse" or "Bot" defense. This chapter has highlighted some challenges to botnet investigations and prosecutions. The next chapter considers changing the architecture through indirect regulation of ISPs and DNS providers

Chapter 7

THE ROLE OF INTERNET SERVICE PROVIDERS AND DOMAIN NAME SERVICE PROVIDERS IN COMBATTING BOTNETS

Table of Contents

7.13 CONCLUDING REMARKS

7.0 AIMS OF CHAPTER

While it remains important for law enforcement to pursue botnet masters for crimes committed, such pursuance will likely only prove fruitful in few situations. As seen in **Chapters 4 to 6**, law enforcement will play a small and limited role in combating botnets. As former head of the United States National Cyber Security Division and US-CERT Andy Purdy writes:

> "the reality is that given the magnitude of the malicious activity, and reasons behind why the activity is so widespread and so successful, law enforcement is destined to play a reactive role that will have little impact on the problem....
>
> There has been too much emphasis on the difficulty of attribution and not enough on working with the reality that malicious actors need witting or unwitting enablers to gain connectivity, exploit vulnerabilities, find victims, process payments, move goods, and hide money.... Enablers include numerous categories of individuals and organizations: registrars, ISPs, web hosts, email providers, telco providers, domestic and foreign banks, check cashing services, wire funds transfer services, credit card processors, certificate authorities, and shippers (FedEx, UPS, USPS)."[1]

This chapter is concerned with the enablers who provide connectivity to the Internet, hence the term "Connectivity Enablers". Internet connectivity enablers include registrars, ISPs, web hosts, email providers, and telco providers. The role and policies of ISPs and DNS providers in combating botnets will be considered in this chapter.

Specifically, this chapter will provide details of ISP initiatives aimed at disrupting botnets. The chapter addresses the proposed Australian Internet Industry Association (IIA) Code of Practice consultation paper on "For Industry Self-Regulation in the Area of E-Security"[2] , and the Comcast initiative in the United States currently before the IETF potentially for consideration as an international standard.[3] Both initiatives involve ISP monitoring and detecting compromised computers connected to their networks, notifying customers when their computers are infected and, hence, are part of a botnet, and then assisting customers to remedy the situation. A brief re-examination of botnets is provided to expand on the commentary that follows on ISP initiatives. Comments will be made on the IIA and Comcast Schemes. Critical components of

---

[1] Purdy, A. "Proposal for Malicious Activity/Cyber Crime Initiative" 2009. A copy is on file with the author.
[2] Internet Industry Association, *Internet Service Providers Coluntary Code of Practice for Industry Self-Regulation in the Area of e-Security* (September 2009).
[3] Livingood, J., Mody, N. And O'Reirdan, M. of Comcast, Internet Enginerring Task Force Working Draft, *Recommendations for the Remediation of Bots in ISP Networks* (September 2009) [hereinafter Comcast].

each scheme will be analysed. Recommendations will be made in the areas of detecting and monitoring techniques, protection of civil liberties, and ISP liability under the *Privacy Act, Telecommunications Act* and *Telecommunications (Interception and Access) Act* for ISP detection and monitoring.

7.1 ISPS AND DNS PROVIDERS

7.1.1 Differentiating ISPs from DNS Providers

There are many types of domain name service providers, all of whom perform different functions within the overall domain name system. There are four main types of groups performing DNS functions relevant to botnets:

1) General Regulatory and Policy Functions for Overall Domain name System (ICANN),

2) Regulatory and Policy Functions for gTLDs and ccTLDs (Eg. Verisign and auDA)

3) Administration of Databases (ISPs)

4) DNS Mapping to IP Addresses (ISPs)

ICANN produces the overall regulation and policy making for the domain name system. Regulation of the gTLDs and ccTLDs is performed by organisations appointed by ICANN. Such higher-level authorities include, for example, Verisign and auDA. Registrars such as Verisign and auDA then appoint a subsidiary who is responsible for the administration of the domain-names database. In Australia the auDA appointed AusRegistry to administer the database. New and amended entries into the domain name registries are managed by ISPs and by corporations offering such services such as NetRegistry. The database that maps domain-names to IP addresses is performed by those ISPs who operate domain-name servers.[4]

[4] The Cyberspace Law and Policy Centre (Lauren Loz and Alana Maurushat) mapped out the various list of registrars and resellers relevant to the .au including contractual agreements between the various resellers and registrars with ICANN and the .auDA. This table is included in **Appendix B** at the end of the thesis.

Domain name service providers can mitigate against botnets in three main ways. The first method is largely technical and involves changes to the domain name rotation.[5] ICANN has implemented several technical changes to domain name rotation, and more specifically, to target fast-flux. The second method is through contract law. DNS providers have contractual agreements with either ICANN or the official country code level top level domain provider such as the .auDA. Where DNS providers do not comply with these contractual agreements, ICANN and an entity such as the .auDA may terminate the contract. The third and last method involves DNS provider's cooperation with the removal of domain names linked to a botnet (how IP addresses of domain names are linked to botnets was explained in **Chapter 3**). Where a DNS provider will not voluntarily remove the domain name, a court order may be sought as was successfully done by Microsoft with the take-down of the Waledac botnet as was seen in **Chapters 3** and will be seen in **Chapter 8.** The first two methods (technical and contractual) are briefly explored below. The third method of cooperation is explored in the remainder of this chapter where DNS provider is subsumed into the category of ISP. Removing C&C sources involves mapping domain names to IP addresses, the service which is performed by ISPs and not domain name registrars such as the .auDA.

7.1.2 Technical and Contractual Methods of Countering Botnets by DNS Providers

ICANN is a not-for-profit public-benefit corporation formed in 1998 with the mandate of coordinating the Internet's naming system. ICANN is considered to be a global regulatory regime as its policy decisions impact on the evolution of the Internet.[6] One of the ways ICANN coordinates the domain name system is by delegating roles through contractual agreement for general top level domains (gTLDs) and country code top level domains (ccTLDs). ICANN also provides accreditation agreements for various types of domain name registries and resellers. ICANN has formed a GNSO-Council Working Party on Fast-Flux. Fast-flux and other related terms are explained below.

Fast Flux: Fast Flux refers to rapid and repeated changes to A and/or NS resource records in a DNS zone, which have the effect of rapidly changing the location (IP address) to which the

[5] Resolution does not refer a legal matter to be solved. Resolution here refers to a technical element where the user types in a domain name which is then connected to a unique internet protocol address.
[6] *See* Mueller, M. *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Massachusetts Institute of Technology, 2002).

domain name of an Internet host (A) or name server (NS) resolves.[7] However, this is not the whole picture as "the specific distinguisher of a fast-flux attack is that the dynamic nature of the DNS is exploited so that if a website is to be suppressed then it is essential to prevent the hostname resolving, rather than attempting to stop the website being hosted."[8]

Single Flux: A variant of fast flux in which rapid updates to A records in the zone file of a subdomain (usually second-or-third level) cause the location (IP address) of Internet hosts (e.g., web sites or other content servers) to change rapidly.

Name Server Flux: A variant of fast flux in which rapid updates to NS records in the zone file of a top-level domain cause the location (IP address) or the name server(s) for one or more subdomains to change rapidly.

A Records: Records that specify IP addresses corresponding to the domain name.[9]

NS Records: Records that specify which DNS servers are used with your name.

Double Flux: A variant of fast flux in which both single flux and name server flux are employed to cause the location of both hosts and name servers to change rapidly.

Fast Flux Hosting: The practice of using fast flux techniques to disguise the location of web sites or other Internet services that host illegal activities.

Fast Flux Service Network: A network of compromised computer systems (a "botnet") with public DNS records that are constantly changing.

---

[7] Gasster, L. of the ICANN GNSO Council, "GNSO Issues Report on Fast Flux Hosting" (March 25, 2008) available at http://www.st.icann.org/m/page/gnso-council/fast_flux (last accessed July 2, 2010).
[8] 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). Richard Clayton is Profeesor at the Computer Lab, Cambridge University.
[9] Aitchison, R., "DNS Records" in *Pro DNS and BIND* (Apress Publishers, 2003).

Legitimate uses of fast-flux include mobility services**,** privacy proxies[10], and search sngine caching[11]. Botnets represent an illegitimate use of fast-flux. The use of fast-flux in botnets has the consequence of thwarting traceback to crimes, utilisation of scarce bandwidth, forces repeated re-configuration of root zone, and can sometime disconnect developing countries from the Internet for a period of time. The last point is extraordinary and, it appears to come as a surprise to many members of the ICANN working group from developed countries. As the original commenter, Bill Woodcock, states:

> "First accepting this flood of illegitimate changes poses a cost in Internet bandwidth, and ultimately money, to anyone who would spread authoritative nameservers among developing countries. It consumes a scarce resource, competing with both legitimate DNS update traffic and with all other forms of Internet use that could otherwise avail themselves of that connectivity to the rest of the world. Worse, because it floods constricted circuits, it can cause incremental zone transfer processes to fail, taking servers offline for hours or days at a time while they're resynchronized. These costs and strictures are imposed upon the poorest countries in the world, who simultaneously have the highest costs for bandwidth.
>
> Second, the price that fast-flux operators extract from registries comes in the form of Service Level Agreements, or SLAs, requiring registries to provide no service, in preference to normal non-fast-flux-supporting service, when that choice is encountered. In the past, default six-week zone expiry times ensured that those who were cut off from general Internet access, but had the forethought to prepare by equipping themselves with local authoritative servers, could at least rely upon functional DNS during the time of their disconnection. That is no longer the case. SLAs catering to the fast-flux market now promise that DNS servers will be purposely removed from service if they're unable to keep up with, or lose connectivity from, the flood of fast-flux changes. Again, the countries that suffer incidents of national disconnection are usually those already labouring under the heaviest burdens: Pakistan, Sri Lanka, and Zimbabwe, for example.
>
> These are significant degredations of the quality of service offered by the domain name system, and they disproportionately and unfairly burden those who already find themselves on the wrong side of the digital divide. Fast flux is an abuse of the domain name system, and privileges the interests of criminals over the global public welfare."[12]

The DNS can be manipulated through fast-flux rotation by criminals to evade detection by law enforcement and termination of their Internet services by ISPs and DNS registrars. The ability to fast flux domain names is one of the most powerful tools in a building a formidable botnet. ICANN has identified fast flux as the most important tool in a cybercriminal's arsenal. As such, there has been much push for "ICANN, registries and registrars ... to establish best practices to

---

[10] The ICANN Working Party on Fast-Flux identified one group that uses fast-flux to avoid Internet censorship. The group, Domain UltraReach, "offers a proxy service called UltraSurf, which it says is designed to allow web users to circumvent Internet censorship by the Chinese government: http://www.ultrareach.com/company/aboutus.htm". *See* gnso-ff-pdp-may08] case study: fluxing domains used for unusual purpose, available at http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00371.html (last accessed February 7, 2011). There are many other technologies and services that allow for effective circumvention of Internet censorship such as Tor, and Psidon which do not rely on fast-flux methods.

[11] Google takes advantage of low TTL for its search engine cache but there are other technical methods to achieve the same result. *See* Gasster, note 7 above.

[12] Woodcock, B., "Submission of Packet Clearing House on the matter of the GNSO's report on fast flux" (January 27, 2009) available at http://forum.icann.org/lists/fast-flux-initial-report/msg00001.html (last accessed December 2010). The commentary that follows Woodcock's submission is one of surprise.

mitigate fast flux hosting, and to consider whether such practices should be addressed in future accreditation agreements."[13] The Working Party on Fast-Flux has recommended a series of changes to deter fast-flux which were commenced in 2010 and will continue until fully implemented.

ICANN has recommended two broad types of new proposals.[14] The first relates to DNS providers monitoring and reporting of DNS activities. The second area involves technical implementation of monitoring DNS activities including changes to domain name rotation. The specifics of ICANNs recommendations include a proposed new reporting mechanism whereby there is an email alert system for Certs, law enforcements and contracting reporting agencies. Additionally, new contractual measures have been added to the ICANN licensing agreements requiring ccTLDs to adapt measures to deter fast flux. Part of the new contractual agreement clauses will require DNS providers to authenticate contacts before permitting changes to NS records. There will no longer be any automated NS record changes. Additionally there will be a limit to the number of name servers that can be defined for a given domain. At the more technical end, ICANN will enforce a minimum "time to live" (TTL) for name server query responses so that domain names cannot be rotated quickly. Lastly, a new protocol known as DNSSEC[15] is now used for the root zone. DNSSEC is considered to be a more secure protocol which will better serve to reduce fast-flux.

Where DNS providers are not compliant with contractual agreements with ICANN and the .auDA, their licenses may be terminated. ICANN, for example, has terminated the accreditation agreement with EstDomains for failure to comply with contractual provisions.[16] The .auda has also terminated an agreement with a reseller for failing to comply with contractual provisions. The .auda successfully terminated its agreement with Australian Style Party Ltd. who provided domain name services under the name Bottle Domains for failure to report serious security incidents to the .auDA thereby breaching the contractual agreement between the parties. Australian Style Party challenged the .auDA's right to terminate the agreement, asked for compensation and to be entitled to resume business as a domain name service provider. Both

[13] [SAC025]: Fast Flux Hosting and DNS (SAC025) (January 28, 2008) available at http://www.icann.org/committees/security/sac025.pdf (last accessed January 31, 2011).
[14] The proposals and issues surrounding fast-flux may be found in ICANN documents. *See* notes 7 and 10 above.
[15] The Domain Name System Security Extension is a protocol for the root zone. More information about the protocol may be found at http://www.dnssec.net/ (last accessed November 10, 2010).
[16] A copy of the termination notice is available at http://www.icann.org/en/correspondence/burnette-to-tsastsin-28oct08-en.pdf (last accessed December 10, 2011).

the Supreme Court of Victoria and the Victoria Court of Appeal rejected Australian Style Party's requests.[17] The termination agreement remains in force.

7.1.3 ISPs as Essential Component in Botnet Removal

As seen in **Chapters 1 and 2**, botnets and similar malicious programs operate in a distributed manner where compromised machines may be located in multiple countries.[18] Many botnets also covertly operate in channels that may be difficult to detect such as in peer to peer networks.

Chapters 3 and 8 explored the coordinated efforts of security researchers and security corporations with ISPs and domain name registrars to take down the C&C sources of botnets. When a botnet is shut down, as seen in the Waledac botnet, the effectiveness of such removal is contingent on the successful prosecution of the botmaster and, more importantly, on such compromised computers being remedied. If the compromised computers are not remedied, the botnet remains susceptible to being taken over by another botmaster. Even though Microsoft and its consortium of affiliated researchers were able to temporarily shut down the Waledac botnet through a court order to de-register the reported 277 .coms where the botnet received its instructions, the botnet is still vulnerable to subverting of instructions by the botmaster in a peer-to-peer network, or being taken over by another botnet master. As long as these computers remain infected, they are still susceptible to receiving new instructions to perform malicious activity from the botnet master though this would involve quite a bit of work to re-herd the computers, and to issue new instructions in a manner that would avoid detection.

The question then becomes how do we successfully reduce the number of compromised computers? Some alternatives look at requiring users to have a computer license before they are allowed to connect to the Internet and requiring all computers sold to have pre-installed anti-virus software before a computer may be connected to the Internet.[19] However, anti-virus software only blocks a certain percentage of malicious traffic, and is reliant on the end-user patching their systems (browser, router, hardware) on a frequent basis.[20] Once a user's machine is infected and part of a botnet, they are likely to be unaware that their computer has been

---

[17] See *Australian Style Pty Ltd v .au Domain Administration Limited* [2009] VSC 422 (25 September 2009); and *Australian Style Pty Ltd v .au Domain Administration Ltd* [2010] VSCA 184 (23 July 2010).
[18] For a general reference to botnets *see* Schiller, C., Binkley, J., Harley, D, Evron, G., Bradley, T., Willems, C. and Cross, M. *Botnets: The Killer Web App* Syngress 2007).
[19] *See for example*, 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.
[20] Clarke, R. and Maurushat, A., "Who Will Bear the Cost of Insecure Devices" (2007) 18 Journal of Law, Information and Science 8.

compromised. Where a user is aware that their computer is infected, it is extremely unlikely that they will be aware that their machine is being used to commit crimes. Further, the most sophisticated botnets are not detectable through anti-virus and similar security products as seen in **Chapter 3**. User education, therefore, is a must in any effort to better secure the Internet. There is a growing recognition that ISPs are in the best position to assist in bot removal. It has been suggested in Australia that ISPs must be active not only in the removal and remedying of their customer's compromised machines but must also play a role in educating users on safer online habits. The role of ISPs in botnet remediation is explored in the remainder of this chapter below.

Internet Service Providers have taken an increasingly active role in combating botnets and malicious activity. ISPs have typically placed a strong emphasis on filtering spam botnets. This has predominantly taken shape through sophisticated spam filters known as ingress and egress filtering. Ingress filtering refers to filtering packets as they enter into a system whereas egress filtering refers to filtering packets as they exit a network system.[21] The result is that much spam content does not arrive in one's "INBOX" but find its way to the "BULK" or "SPAM" folders. This preventative measure merely quarantines the undesired content to a place where users may still access the files. This technique, while mitigating against some malicious activity, does not address the larger problem of what needs to be done once a machine is infected and part of a botnet. Organisations and ISPs also use a technique whereby a range of internet protocol addresses are blocked. This was an effective method in blocking unwanted Internet traffic when content was hosted in a more static manner such as the user being directed to a phishing website (Eg. www.bankofcanadaa.ca). Botnets, however, use very dynamic command and control structures as was seen in **Chapter 3**. Where an ISP is aware of a range of IP addresses that will be used as a command and control as seen in the Torpig example, it would be possible to block those IP addresses thereby preventing the compromised computer from connecting to the C & C. This technique, however, will only be effective in less sophisticated botnets which do not have alternative C&C in the peer-to-peer channel. The only way to block the C&C in a peer-to-peer channel is to blocks all peer-to-peer traffic. When a C&C is located in a rootkit, there is no known way to either detect or block such an application. As most botnets incorporate multiple C&C structures, IP address blocking will not be a successful tactic to combat botnets.

[21] Note 7 above.

Many ISPs and organisations also block po rt 25. Much spam and malicious traffic is routed through port 25, therefore, it is thought that blocking this port reduces the problem of unwanted content distributed through botnets. As articulated in the ITU Botnet Mitigation Toolkit document, "attempting to combat botnets simply by blocking port 25 has been compared, colourfully (and validly) by one expert to "treating lung cancer with cough syrup"." Only a portion of malware travels through port 25 while malware actors may simply re-channel traffic through another port. Not all ISPs do any ingress and egress filtering for malicious content nor do they all block port 25.

ISPs are generally not responsible for the security of their customer's computers nor for monitoring the content that their customers place and distribute online (see **sections 7.3.2 "Co-Regulatory Model", 7.6 ISP Liability for detection and monitoring" and 7.10 "The Evolving Liability Structure for ISPs"**. ISPs are generally seen as "mere conduits" of information where they have not traditionally examined the content flowing through their networks.[22] The role of ISPs, however, is changing. The next proposed change is the role of the ISP to tackle botnets more generally as ISPs are seen as a critical player in any successful initiative in the area. The following section looks at the Comcast proposal which is then followed by the IIA e-security proposal.

7.2 COMCAST'S RECOMMENDATION FOR THE REMEDIATION OF BOTS IN ISP NETWORKS

Comcast is one of the largest ISP providers in the United States capturing over 14% of the United States market.[23] Comcast is an innovator in the remediation of bots over their network. Based on their experience with methods used to remediate bots, the company has written an informal document for consideration as an informational-Request for Comment (RFC). The document is an Internet-draft and has not at this point been placed on the Internet Engineering Task Force (IETF) standards track.[24] An Internet standard refers to "a specification produced

[22] 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).
[23] *ISP-Planet* puts Comcast in at 14.7% in quarter 3 of 2008 while *Stat-Owl* puts Comcast in at 14.26 in July 09. See http://www.isp-planet.com/index.html) and *Stat-owl* (http://www.statowl.com/network_isp_market_share.php (last accessed January 29, 2010).
[24] According to Jeremy Malcom, "the IETF, as the body responsible for the development of a large majority of such standards, it is unquestionably the Internet's pre-eminent standards development body." Malcom, J. *Multi-Stakeholder Governance andthe Internet Governance Forum* (Terminum Press 2008) page 51.

by the IETF that has progressed through its standards development process to the final stage."[25] Standards do not have the effect of a legal rule, but are generally complied with because they are of a "high-quality, are timely, widely supported, and represent a high level of technical consensus amongst a broad group of experts and users."[26] The document is being considered as an informational-RFC. An informational-RFC is a working draft which is intended to become an RFC, then a proposed standard and possibly a standard. The Comcast draft, therefore, is a highly relevant document to the discussion of bot remediation.

7.2.1 Key Components of the Comcast Recommendations (Working Draft of the Internet Engineering Task Force)

The Comcast document is best described by the contents of its abstract:

> "This document contains recommendations on how Internet Service Providers can manage the effects of computers used by their subscribers, which have been infected with malicious bots, via various remediation techniques. Internet users with infected computers are exposed to risks such as loss of personal data, as well as increased susceptibility to online fraud and/or phishing. Such computers can also become an inadvertent participant in or component of an online crime network, spam network, and/or phishing network, as well as be used as a part of a distributed denial of service attack. Mitigating the effects of and remediating the installations of malicious bots will make it more difficult for botnets to operate and could reduce the level of online crime on the Internet in general and/or a particular Internet Service Provider's network."

The Comcast document addresses many of the major points in the Australian Internet Industry Associations' (IIA's) self-regulatory e-security code (**section 7.3**). The Comcast document, however, by way of contrast is a detailed document outlining the advantages and disadvantages of ISP involvement in the remediation of bots. The authors provide rich debate on various options to consider as well as detailed analysis of detection, monitoring, notification to the user, and remediation techniques. The IIA document, by way of comparison, is silent on the potential drawbacks and advantages over various options and is deeply lacking in any relevant discussion of salient points. It may be that such discussion was meant to take shape in the form of submissions from the public to the IIA's draft guidelines. Elements of the Comcast document will be used to fill in the missing information from the IIA document. For example, issues surrounding detection and monitoring techniques are explored in details in the Comcast document, whereas the IIA document merely lists possible techniques. Points from the Comcast document will be used and supplemented when critiquing the IIA document. The Comcast recommendations are dealt with in **sections 7.5** and **7.6.**

[25] Above, page 51.
[26] Malcom, note 24 above, page 51.

7.2.2 ITU Botnet Mitigation Toolkit

There exist a number of other Best Practice guidelines for ISPs tackling botnets, the most significant of which are the International Telecommunication Union report*, ITU Botnet Mitigation Toolkit*[27] and *ITU Report Practices for a National Approach to Cybersecurity*.[28] The ITU Botnet Toolkit identifies key players both in government and industry, then explains roles that each should ideally play to best combat botnets. ISPs are addressed within the document and a detailed examination of methods are provided, and the limits to ISPs remediation of botnets is provided. These limits are explored in **section 7.9.**

7.3 AUSTRALIAN INTERNET INDUSTRY ASSOCIATION CODE OF PRACTICE: FOR INDUSTRY SELF-REGULATION IN THE AREA OF E-SECURITY

7.3.1 Australian Internet Security Initiative

The Australian Communications and Media Authority (ACMA) introduced a project in 2005 known as the Australian Internet Security Initiative (AISI) to help address the problem of botnets. AISI is run by the ACMA. According to the ACMA website, AISI collects data on compromised computers and forwards daily reports to participating Australian ISPs.[29] There are over 75 ISPs participating in the project. When an ISP receives the daily botnet report, they *may* inform their customers that their computers are compromised and they may provide advice as to how to remedy the problem. There is no obligation on the ISP to use the reported data or to inform customers where their machines are compromised. The extent of ISP involvement is completely voluntary and discretionary.

The information collected by AISI generally relates to spam botnets. The focus on spam botnets may be in part due to the jurisdictional limits of ACMA. The provisions in the *Spam Act 2003* designate ACMA as the overseer to the act with powers to investigate and press charges against spam offenders.[30] Under the *Telecommunications Act,* ACMA may appoint officers to become inspectors for the purpose of carrying out spam investigations.[31] Investigators are then able to

---

[27] *ITU Botnet Mitigation Toolkit: Background Information* (January 2008).
[28] *ITU Study Group q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts* (January 2008).
[29] The AISI project is described at http://www.acma.gov.au/aisi (last accessed January 25, 2010)
[30] The *Spam Act 2003 (Cth)*
[31] *Telecommunications Act 1997* (Cth). *See* section 533 Inspectors.

request warrants and then perform search and seizures relating to breaches of the *Spam Act*,[32] conduct searches to monitor compliance,[33] and access computer data relevant to the *Spam Act*.[34] ACMA does not have the same jurisdiction over malware, adware spyware, or botnets in general. ACMA's role was more formally explored in **Chapter 4** where it was recommended that the *Spam Act 2003* be amended to cover malware and botnets, and that the ACMA's jurisdiction be extended to include malware and botnets**.** While many botnets are used to deliver specific types of content such as spam, a botnet itself if neutral and may be used to distribute any form of content. The only information since its inception available about the AISI project is a few paragraphs on the ACMA website that outline the existence of a project.[35] There is no public information available on the specifics of the project, methodology of data collection, reliability and integrity of data, the extent of ISP participation, nor reported tangible outcomes or statistics from the project.

The AISI project, however, has inspired a number of security projects to follow suit with the International Telecommunications Union (ITU) release of the "ITU Botnet Mitigation Toolkit"[36] in January 2008, along with the Australian Internet Industry Association's (IIA) consultation document in September 2009 regarding e-security self-regulation. The IIA E-Security Code represents a formalisation of the previous voluntary initiative to that of a more formal ISP initiative.

7.3.2 Co-Regulatory Model

Australian ISPs are co-regulated. *Schedule 7* of the *Broadcasting Services Act 1992 (BSA)* introduces co-regulation between ACMA and the telecommunications industry.[37] The industry's involvement consists of the development of industry codes of practice and industry standards.[38] The industry codes have mostly dealt with classification of content, and related issues of removal of offensive content, and on educating users on the use of content services.[39] *Schedule 7* of the

---

[32] *Telecommunications Act 1997* (Cth). Division 3, sections 535-546.
[33] *Telecommunications Act 1997* (Cth). Divisions 5 and5A, sections 547-547H.
[34] *Telecommunications Act 1997* (Cth). Section 547J.
[35] http://www.acma.gov.au/spam
[36] ITU, note 27 above.
[37] *Broadcasting Service Act 1992 (Cth), Schedule 7(BSA).*
[38] Reference to industry codes and standards is made in Part 4 Industry Codes and Industry Standards in *Schedule 7* of the *BSA*. Additional reference to industry codes and standards may be found in Part 6 Industry Code and Standards in the *Telecommunications Act 1997* (Cth).
[39] *For example*: Telecommunications Consumer Protection Code, EFT Code of Conduct, Content Services Code, e-Marketing code of practice, The Internet Industry Spam code of practice, Interactive Gambling industry Code, Privacy Code, IIA Family Friendly ISP Seal, and E-Security Code for ISPs

BSA provides regulations targeted at content carriers.[40] These regulations, like those of the industry code, predominantly relate to content. Where the ACMA classifies content as prohibited, *Schedule 7* sets out obligations on ISPs to remove prohibited content when hosted on their network. The e-security consultation paper, if adopted by the IIA, will form part of an industry code to be adhered to by all ISPs. This move from an AISI initiative to a self-regulatory code is a formalisation of ISP involvement in dismantling botnets.

7.3.3 IIA E-Security Code

The IIA e-security consultation document provides an overview of objectives, principles, a summary of terminology, and references other security organisations such as AusCERT and AISA for users to consult. The core of the document relates to recommended actions for ISPs to help prevent malicious activity, in particular, botnets. The recommendations for ISPs draw on many guiding principles in the Comcast information-draft before the IETF as well as many best practice principles in OECD and ITU botnet policy documents.[41] However, the IIA E-Security Code significantly departs from both the Comcast and ITU documents in that a detailed discussion of issues and ramifications of recommendations is absent. For these reasons, much of my analysis is based on the Comcast working draft in **section 7.5** and **7.6.** The ITU Botnet Toolkit is also considered when assessing the IIA E-Security Code.

The IIA E-Security Code provides guidance to ISPs in order to perform four functions. They are:

(a) Detect malicious activity on a customer's compromised computer;

(b) Take steps to respond to the AISI reports or any other source of information that may relate to malicious activity;

(c) Inform a customer on what actions they can take to protect their computers from malicious activity; and

(d) Notify Australian authorities of a malicious activity without prejudice.

No agreement has yet been made amongst stakeholders as to what modifications, if any, will be made to the Internet Industry Code of Practice in order to achieve the objectives. The consultation document, however, provides further guidance on each of the above four points

[40] *Schedule 7* of the *BSA* was introduced in the *Communications Legislation Amendment (Content Services) Act 2007* (the 'CSA'), which came into effect on 20 January 2008.
[41] Notes 3 and 27 above.

culminating in recommended action for ISPs. The following sections are broken down into the four IIA recommendations where each is critiqued in detail. Of the four IIA recommendations, educating customers and reporting malicious activities to relevant authorities are the least contentious and, hence, will be given less attention. The recommendations of detection and monitoring, and the actions to be taken once a compromised customer is detected are more controversial. A more detailed assessment and critique of the more controversial recommendations is provided below.

7.4 DETECTION AND MONITORING OF COMPROMISED COMPUTERS

The proposed IIA code encourages ISPs to adopt one or more methods of detection and monitoring. The recommendation states:

> **Detection of Malicious Activity / Compromised Computers**
>
> ISPs can typically find out about malicious activity and compromised computers in two ways:
>
> (a) By active monitoring as part of normal network management activities; and/or
>
> (b) By notification of trusted third party sources. (Note that a list of sources is included in Schedule 2 to this Code.)
>
> ISPs are encouraged to undertake one or both of the above activities to detect compromised computers on their networks.

The lack of detection and monitoring techniques in the IIA E-Security Code is puzzling. Once an ISP moves into the area where personal information and communications are being monitored, a number of legal alarm bells go off. The *Privacy Act* restricts use of personal information. The *Telecommunications Act* restricts the use and disclosure of confidential customer records, which are generally thought of as communications (Eg. emails travelling from one point to another) and stored communications (Eg. origin of email and end-point of email where stored in server). The *Telecommunications (Interception and Access) Act* regulates the interception and examination of the content of communications (Eg. email). The type and function of the detection and monitoring techniques adopted, therefore, has great legal and civil liberty implications. The legal obligation of ISPs for detection and monitoring is examined in **section 7.6.**

7.4.1 Third Party Detection and Monitoring

One of the detection and monitoring methods involves trusted third party sources providing ISPs with monitoring information. Schedule 2 of the proposed IIA e-security code provides a list of trusted third party sources of compromised computer information including: the Australian Internet Security Initiative (AISI), Spamcop reports, SORBS reports (spam and open relay blocking system), DNSBL reports (domain name service blacklist reports), AOL reports, Hotmail reports, RBLS (Blacklist notification subscription), Internal Spamassassin scanning and reporting, and reports from organisations such as AusCERT, My Net Watchman, SpamCop, RoadRunner, JunkMail Filter, other ISPs and external individuals. The list, while not exhaustive, outlines key players in the arena. These trusted third parties are both local (such as AusCERT) and international such as (Spamcop and Hotmail reports). The use of data from trusted third parties as opposed to generating data by internal monitoring methods imposes less liability risks for ISPs. ISPs are not actively monitoring computers and, therefore, stand less of a risk of violating privacy principles. An ISP could still, however, be liable for wrongful Internet disconnection if they relied on inaccurate information from a third party. Liability issues for ISPs are examined in **sections 7.6** and **7.10.**

7.4.2 ISP Detection and Monitoring

The other detection and monitoring method looks at ISPs performing internal monitoring of traffic through a variety of methods listed in *Schedule 2 - Sources of Information Relating to Compromised Computers.* These include ingress and egress address validation and filtering, gateway IPS/IDS, internal detection systems such as firewalls that detect known TCP and UDP port numbers, reports from customers, and monitoring mail queues and network patterns for anomalies or known patterns of malicious activity. Here the ISP is the source of detection and monitoring. Implications of detection and monitoring are considered below with a detailed examination of the potential methods to be used, and potential liability issues stemming from detection and monitoring methods.

7.4.3 Detection and Monitoring Techniques

Internal detection and monitoring by ISPs may use techniques that are similar to trusted third parties. As the core botnet detection methods, tools and processes overlap, many issues regarding the use of these technologies also overlap. The detection and monitoring techniques

can be categorised broadly as: scanning IP space to detect vulnerable hosts, real-time feedback reports offered by third party threat data clearinghouses, passive network monitoring technologies searching for irregular traffic, DNS-based techniques, intelligence gathering decoys such as sandboxing[42] or honeypots[43] (most data clearinghouses use such technologies), user complaints report, and sector specific sharing of compromised hosts. The richness of detail in the Comcast IETF working draft provides necessary information for future discussion on required principles, recommendations and liability issues. These seven detection categorisations, therefore, are offered in full following this section. Curiously, deep packet inspection is mentioned in neither the Comcast document nor the IIA E-Security Code. This is a serious flaw as it is not discussed in either document. Some governments will inevitably look at deep packet inspection technologies to perform a variety of functions and such technologies pose a number of civil liberties issues which are explored in **section 7.11**. Likewise, Comcast uses deep packet inspection technologies in its operation though this appears to be limited to traffic shaping. A discussion of the mechanisms used to monitor and detect compromised computers follows below.

7.4.3.1 Port Scans

The Comcast document discusses port scans as follows:

> "Where legally permissible or otherwise an industry accepted practice in a particular market region, an ISP may in some manner "scan" their IP space in order to detect un-patched or otherwise vulnerable hosts. This may provide the ISP with the opportunity to easily identify Internet users who appear to already be or are at great risk of being infected with a bot. ISPs should note that some types of port scanning may leave network services in a hung state or render them unusable due to common frailties, and that many modern firewall and host-based intrusion detection implementations may alert the Internet user to the scan. As a result the scan may be interpreted as a malicious attack against the computer. Vulnerability scanning has a higher probability of leaving accessible network services and applications in a damaged state and will often result in a higher probability of detection by the Internet user and subsequent interpretation as a targeted attack. Depending on the vulnerability being scanned, some automated methods of vulnerability checking

[42] A sandbox, according to Melnik and Dunham, is "a dedicated computer system within a lab environment for testing malcious code. Virtual machines are common sandbox solutions." Dunham, K. and Melnick, J. *Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet* (CRC Press, 2009) page 132.

[43] Holz, T. And Provos, N. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection* (Addison-Wesley 2008). There are a wide variety of honeypots ranging from high-interaction to low-interaction, and are either physical or virtual. Most companies use a virtual honeypot. According to highly respected authors Holz and Provos:
"A high-interaction honeypot is a conventional computer system – for example, a commercial off-the-shef (COTS) computer, a router, or a switch. This system has no convention task in the network and no regularly active users. ... In contrast, low-interaction honeypots emulate services, network stakcs, or other aspects of a real machine. They allow an attacker a limited interaction with the target system and allow us to learn mainly quanntitative information about attacks. ...
Physical honeypots means that the honeypot is running on a physical machine [covering one IP address] ...
[A virtual honeypot uses] one physical computer that hosts several virtual machines that act as honeypots [so that] we can have thousands of honeypots on just one machine ... making it easier to collect data."

> may result in data being altered or created afresh on the Internet user's computer which may be a problem in many legal environments."[44]

Should an Australian ISP elect to perform port scans, any data alternation on a user's computer that leads to damage would potentially be actionable under basic tort law as seen in **Chapter 4**. A non-liability clause for port scans and similar activities in the customer's Terms of Service contract would, however, likely mitigate against a successful claim in tort. As there is no security research exemption for unauthorised access, modification or impairment to data, the ISP may equally find themselves without a defence to criminal provisions.

7.4.3.2 Feedback Loops / Real-Time Abuse Reports

The Comcast document suggests the following for feedback loops and real-time abuse reports:

> "An ISP may also communicate and share selected data, via feedback loops or other mechanisms, with various third parties. Feedback loops are consistently formatted feeds of real-time (or nearly real-time) abuse reports offered by threat data clearinghouses, security alert organizations, other ISPs, and other organizations. The data may include, but is not limited to, lists of the IP addresses computers which have or are likely to have a bot running, domain names or fully qualified domain names (FQDNs) known to host malware and/or be involved in the command and control of botnets, IP addresses know to host malware and /or be involved in the command and control of botnets, recently tested or discovered techniques or detecting or remediating bot infections, new threat vectors, and other relevant information. Good examples of this include SNDS from Microsoft, XBL and PBL from Spamhaus and the DSHIELD AS tool from the SANS Institute".[45]

As will be demonstrated in **section 7.5.5**, there are restrictions around the disclosure to third parties of personal information and the content of a communication, potentially inclusive of IP addresses.

7.4.3.3 Medium Packet Inspection Technologies

The Comcast document advocates Netflow as the detection and monitoring method. The Australian proposal is silent as to whether a passive monitoring technique such as Netflow should be used as opposed to a more invasive technology.

> "An ISP may use Netflow [RFC3954] or other similar passive network monitoring to identify network anomalies that may be indicative of botnet attacks or bot communications. For example, an ISP may be able to identify compromised hosts by identifying traffic destined to IP addresses associated with the command and control of botnets. In addition, bots can be identified when a remote host is under a DDoS attack because computers participating in the attack will likely be infected by a bot, frequently as observed at network borders."[46]

Netflow and other passive monitoring techniques are explored in greater detail in **section 7.5.2.**

---

[44] Note 3 above.
[45] Above.
[46] Comcast, note 3 above.

7.4.3.4 DNS-Based Techniques

Comcast discusses DNS based techniques as seen below:

> "An ISP may use DNS-based techniques to perform detection. For example, a given classified bot may be known to query a specific list of domain names at specific times or on specific dates (in the example of the so-called "Conficker" bot), often by matching DNS queries to a well-known list of domains associated with malware. In many cases such lists are distributed by or shared using third parties, such as threat data clearinghouses."

Sharing of domain names between ISPs does not pose a problem in the same way that the sharing of IP addresses might for the simple reason that a domain name in and of itself would only in rare circumstances be classified as personal information. This privacy matter is explored in **section 7.5.1.**

7.4.3.5 Malicious Network Traffic Customer Complaints

Comcast additionally identifies customer complaint channels as a rich source of malware information.

> User complaints: Because hosts infected by bots are frequently used to send spam or participate in DDoS attacks, the ISP servicing those hosts will normally receive complaints about the malicious network traffic. Those complaints may be sent to FRC2142-specified [RFC2142] role accounts, such as abuse@ or postmaster@ or to abuse or security addresses specified by the site as part of its WHOIS (or other) contact data.

The ability of an ISP to share such information with other organisations will depend on the scope and character of the information shared. Information which looks at the content of a communication will be restricted to use under the Telecommunications Act and Telecommunications (Interception and Access Act). These legal elements are explored in **section 7.6.**

7.4.3.6 Intelligence Sharing with ISPs, Security Researchers and Blacklist Operators

The Comcast document specifically discusses the possibility of intelligence sharing amongst ISPs. Again, intelligence sharing by law may only be permissible in certain circumstances as seen in **section 7.5.5.** The Comcast document states:

> "ISPs may also discover likely bot infected hosts located at other sites; when legally permissible or otherwise an industry accepted practice in a particular market region, it may be worthwhile for ISPS to share evidence

relating to those compromised hosts with the relevant remote ISP, with security researchers, and with blocklist operators."[47]

The privacy implications are explored in **section 7.5.1**. Effectively, the Comcast document recommends that ISPs engage in illegal self-help.

7.4.3.7 Third Party Sinkholing and Honeynets

This portion of the Comcast document relates to the IIA e-Security Code's specification of the use of third party sources.

> "ISPs may operate or subscribe to services that provide 'sinkholding' or 'honeynet' capabilities. This may enable the ISP to obtain near-real-time lists of bot infected computers as they attempt to join a larger botnet or propagate to other hosts on a network."[48]

In this instance, the ISP is not performing detection and monitoring of communications. As such the binding obligations under relevant legislation would not apply. Any third party security organisation performing sinkholing or operating honeynets would naturally have obligations under the relevant jurisdiction where they were located. Some general legal issues such as the lack of exemptions for security research were explored in **Chapters 4, 5** and **6.**

7.4.3.8 Deep Packet Inspection

Deep Packet Inspection (DPI) technologies are designed to allow network operators the ability to identify a number of attributes of a packet including its origin and final destination along with the internal content of a communication (Eg. the text of an email). DPI is used by a number of non-democratic societies to dynamically block undesirable content. This is perhaps most well-known in the People's Republic of China which deploys a variety of small, medium and DPI devices at multiple points, including at the ISP level, to censor a wide range of content.[49]

As DPI expert Chris Parson writes:

> "DPI devices are designed to determine what programs generate packets, in real-time, for hundreds of thousands of transactions each second. They are designed to scale in large networking environments. ... In some cases DPI devices cannot immediately identify the application that has produced a packet. When this occurs, ISPs can use "Deep Packet Capture" (DPC) technologies to collect packets in device memory and subsequently inspect them using DPI technologies. DPC lets network administrators perform forensic analysis of packets; packets that are captured are investigated using DPI to determine "the real causes of

[47] Comcast, note 3 above.
[48] Comcast, note 3 above, pages 9 - 11
[49] Opennet Initiative, "Report on China" (2009) available at http://opennet.net/research/profiles/china (last accessed December 2010).

network problems, identify security threats, and ensure data communications and network usage complies with outlined policies." [50]

Many DPI technologies have the ability to monitor internal content of communications, but this does not mean that ISPs will choose to use this function. One interesting component of any packet inspection technology, is that having the technology in place does not necessarily mean that any active monitoring is in place. DPI is explored in greater detail in **section 7.5.3.3 "Deep Packet Inspection".**

7.5 RECOMMENDED PRINCIPLES FOR DETECTION AND MONITORING AND CIVIL LIBERTIES IMPLICATIONS

Whether an ISP elects to used third party sources or their own internal sources, or a combination of both for gathering information relating to compromised computers, there are a number of issues which require consideration. I recommend that detection and monitoring, whether it is performed by a third party or ISP should not violate the following core set of principles:

- Privacy principles and protection of personal information should be maintained (**sections 7.5.1**);
- Freedom of expression concerns should be addressed in the form of a dispute mechanism (**section 7.12**)
- Passive monitoring methods should be use as opposed to pervasive methods such as deep packet inspection (**section 7.53**);
- Methods should be non-disruptive and should not block legitimate traffic (**section 7.5.4.**);
- Use of Multiple Point Bot Detection data points to minimize false-positive identification of computers (**section 7.5.5**);
- ISPs should err on the side of caution when a likely bot infection has taken place, and should notify a customer even in the event of a benign or dormant botnet (**section 7.5.6**);
- Time-sensitive detection methods are imperative (**section 7.5.7**); and
- Review of program to be performed periodically (**section 7.5.8**)

[50] Parsons, C. "Deep Packet Inspection in Perspective: Tracing its Lineage and Surveillance Potentials"

In spite of these principles to detect and monitor network traffic, detection and monitoring by ISPs has only been legal in limited circumstances in Australia. The collection of Internet Protocol (IP) addresses and scanning of a customer's computer to detect bots will not contravene the *Privacy Act 1988* where such actions are consented to by the customer in the Terms of Service. The use of personal information, and subsequent disclosure of it by an ISP, however, did not qualify for the privacy exceptions under the *Telecommunications Act 1997* and *Telecommunications (Interception and Access) 1979 Act,* until the recent amendments in February 2010. Before the 2010 amendments, monitoring could only occur where it was done to assist the ACMA, ACCC or the Telecommunications Industry Ombudsmen – none of whom have explicit jurisdiction over botnets or malware. In essence, monitoring and detection was only legal in the context of spam botnets. The recent amendments to the TIA, however, detection and monitoring when done in the course of "network protection duties" by a "responsible person" are legal. These issues are explored in detail in **section 7.6 "ISP Liability for Detection and Monitoring"**.

7.5.1 Protect Personal Information and Respect Privacy

Tools, methods and equipment for detection and monitoring should be utilised which maintain and respect privacy. In commenting on the IIA e-security document, the Office of the Privacy Commissioner expressed concerns over the e-Security consultation document. The OPC notes that:

> "Although not mentioned in the Code, the Office also notes that the surveillance of individual communications over a network may breach the Telecommunications (Interception and Access) Act 1979 ('TIA Act') and could also be an interference with privacy under the Privacy Act 1988 ('Privacy Act')."[51]

The OPC does not provide specifics as to how detection and monitoring methods would breach either the *TIA* or *PA*, though indicates that concern is over the monitoring of "individual communications". In other words, the OPC seems to be suggesting (albeit incorrectly) that collection and monitoring of information where it is collected without identification of an individual's communications amongst a group or larger subset of communications will likely not meet this threshold. ISPs will monitor data traffic of their customers without referencing the names, addresses and other information about their customers. ISP detection and monitoring systems for a bot remediation program will identify IP addresses where either malicious activity is occurring or where those IP addresses are compromised computers. IP addresses are

[51] Pilgrim, T. " Draft Internet Industry Association eSecurity Code of Practice" Office of the Privacy Commissioner submission to the Intenet Industry Association.

"personal information" under the NPP as will be addressed below in **section 7.5.1.1**. In this sense, therefore, the OPC's statement is incorrect.

This difference between monitoring of an individual's communication versus a groups' communications has also been explained in a different manner – dataveillance vs surveillance. Surveillance and dataveillance are explained by Clarke as "Surveillance is the systematic investigation or monitoring of the actions and communications of one or more persons. Its primary purpose is generally to collect information about him/her, their activities, or their associates."[52] Dataveillance, on the other hand is "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."[53] The purpose of dataveillance is often to identify certain persons within a group who would later become the target of surveillance at a personal level. Many detection and monitoring methods used by ISPs would be considered dataveillance. The IIA E-Security document itself states that monitoring "does not require the surveillance of individual online activity."[54] The distinction between surveillance and dataveillance from a legal perspective, however, is irrelevant. If "personal information" or a "communication" is involved, it must be collected, accessed and used according to the law. In some circumstances, this involves the requirement of a warrant. Obligations under the *Privacy Act* are discussed in **section 7.5.** The legal ramifications of detection and monitoring are considered in **section 7.6.**

7.5.1.1 Internet Protocol Addresses

The technical solutions for bot detection that are currently available are immature but will evolve over time.[55] New detection methods *should* be developed in mind of privacy protection. New technologies that move from medium packet inspection to deep packet inspection involve examining the content of communications. Examination of the content of a communication triggers many privacy and disclosure obligations (see **sections 7.6** and **Chapter 6** regarding the different warrant regimes). To do this effectively and to keep in line with newly evolving botnets, peering more deeply into packets will likely prove irresistible to many countries and organisations. DPI is used among larger ISPs but the extent to which smaller ISPs will use the technology remains to be seen as cost is a significant factor. Even if there is no move towards DPI by smaller ISPs (inevitable for larger ISPS), the collecting of Internet protocol (IP)

[52] Clarke, R. "Information Technology and Dataveillance" (1988) Communications of the ACM, Vol. 31(5), p. 499.
[53] Above, p. 499.
[54] IIA e-security code, note 2 above.
[55] ITU Botnet Toolkit, note 26 above. Comcast, note 3 above.

addresses is unavoidable in most forms of detection and monitoring. As defined in the Privacy Act, "personal information" means:

> "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."[56]

It is impossible to identify the compromised machine on a network without identifying the IP address or domain name. IP addresses might be considered as personal information. This depends on whether the potentially infringing party has not only IP address information, but also information that could link an individual to the IP address. ISPs contain subscriber information of all of their clients. It is difficult to conceive of the situation where an ISP wouldn't have the requisite information, albeit perhaps no intention, to identify an individual. Domain names are not typically personal information under the *PA* in spite of the fact that a domain name when linked to an IP address can readily identify an individual. Identification of compromised computers will require identification of an IP address. This alone will trigger privacy concerns because notification to the Internet user requires identification of the either the registrant of the domain name or the subscriber to the ISP service. [57] The Internet user in this case means the person or organisation who has entered into an Internet connection contract, or the person or organisation who has registered the domain name.

7.5.1.2 Disclosure of Data Collection and Use

Detecting and monitoring IP addresses, as seen above, may be considered 'personal information". Collection of domain names triggers the need to comply with the data protection principles where the information is later used to link back with an individual. Mere identification of a domain name (Eg. www.telstra.com.au) does not qualify as personal information. ISPs can avoid breaching data protection principles through the disclosure of bot detection methods and use of personal information in the relevant terms of service documents and in their privacy policies. An explanation of what bots are and the threats that they impose should also be included in both the terms of service and privacy policies. Comcast offers a sample text on point:

> "What is a bot? A bot is a piece of software, generally installed on your machine without your knowledge, which either sends spam or tries to steal your personal information. They can be very difficult to spot, though you may have noticed that your computer is running much more slowly than usual or you notice

[56] *Privacy Act 1988* (Cth)
[57] This may be different if the domain name was, for example, www.alanamaurushat.com.au.

> regular disk activity even when you are not doing anything. Ignoring this problem is not really an option since your personal information is currently at risk. Thus, bots need to be removed to protect your personal information."[58]

Such a statement in the terms of service and privacy policy complies with disclosure requirements under the NPPs[59] as well as serves to educate end users as well about bots. Naturally, the terms and service agreements will require wording which tells the user exactly what type of information will be gathered, how it will be gathered, how the information will then be used, and with whom that information, if any, will be shared. The use of the information collected must also correspond with the purpose of its collection. IP address lists of infected computers for the purpose of bot remediation is not the same as collection for disclosure to third parties for marketing purposes.

Collection, storage and use of IP addresses will not always lead to identification of an individual. For many of the detection and monitoring tools, lists of compromised IP addresses are generated for information sharing purposes. The lists may be used to generate blacklists for spamming purposes. These lists are often shared between organisations whether they are other ISPs, security researchers or other blacklist operators. Again, the use of IP addresses and any sharing amongst other ISPs and security researchers should be disclosed in the terms of services and privacy policies. As will be demonstrated under the February 2010 amendments to the *TIA*, ISPs will be allowed to perform content inspection in order to protect their networks but such information may not be freely disclosed to third parties (**section 7.6).**

For ISPs subject to the *PA* disclosure of personal information would be legal where it falls under one of the many exceptions. Under NPP 2.1(g) of the *PA,* disclosure of personal information may be required by law in conjunction with a warrant. ISPS may not be required to disclose information but they have discretion to disclose such information. Absent a warrant, an ISP may also at its discretion assist law enforcement or revenue agencies by disclosing information about a customer.[60] For example, if an ISP in performing detection and monitoring of traffic discovered that its users computers were bots used for the commission of an offence, they could then forward information about the communication to the relevant law enforcement agency. Depending on what the botnet was being used for, further interception of communications and disclosure to law enforcement could only be conducted with an appropriate warrant or, if

[58] Comcast, note 3 above, page 16.
[59] *Privacy Act 1988, Schedule 3*, National Privacy Principles, Section 2 Use and Disclosure.
[60] NPP 2.1(g) and (h). There are other exceptions based, for example, when dealing with health information.

monitoring related to network protection, content monitoring could be performed without a warrant. For example, spam monitoring generally requires a warrant under the *Spam Act 2003*, monitoring for the purpose of security intelligence requires a warrant issued by the Attorney General, not a warrant by a court, and interception of communications of innocent parties linked with a crime suspect are subject to yet another regime known as B-party warrants.[61] Warrant regimes were examined in **Chapter 6**. This disjointed warrant system is comprised of several regimes, and contains hundreds of exemptions.

This presents a large problem in the case of network monitoring of malware and botnets. Botnets can be multi-functional. That is, a botnet may be used initially to distribute spam, then later to disseminate Trojan programs designed to steal banking usernames and passwords, and later again to launch a denial of service attack against a nation's electrical grid. Classification of a botnet as a static item is problematic. The botnet may be used to attack critical infrastructure, but the actual communication requiring monitoring often involves innocent users (B-party warrants). Matching the collection of information on botnets to the corresponding warrant regime is fraught with difficulty.

ISP detection and monitoring of Internet traffic against botnets and malware for the purpose of protecting the network typically is not contemplated in either the *PA, TA* or *TIA* (prior to the February 2010 amendment), nor is it covered by the *Spam Act 2003*. In any event, the amendments to the *TIA* adopted in February 2010 provide clear liability exemption for ISPs examining content of communications where it is done for network protection. This is examined in **section 7.6.3.**

7.5.1.3 Small Business Exemption for ISPs from the National Privacy Principles

The OPC raised an additional concern in their submission regarding the exemption of smaller ISPs from the *National Privacy Principles*. Smaller ISPs are classified as "small business operators" who are currently exempt from obligations in the *Privacy Act*. Smaller ISPs would not have to comply with the NPPs if they elected to detect and monitor traffic internally, as opposed to gathering information from trusted third party sources. The OPC notes that the Australian Law Reform Commission (ALRC), in its review of privacy law, recommended that the "small

[61] For an overview of surveillance and warrant regimes, *see* Waters, N,. "Government Surveillance in Australia" in Rule, J. (ed) *Privacy under Pressure* (2006).

business operators" exemption be removed.[62] The Government's first stage response to the ALRC report indicates that this matter won't be considered until the second state of response. In the interim, the OPC encourages small ISPs to voluntarily opt-in to the *Privacy Act* coverage under section 6EA.[63] Small business operators were initially exempt from the NPPs due to concerns of compliance costs and the desire to foster small businesses.[64] The associated costs with internal detection and monitoring by ISPs are expensive. It is likely that smaller ISPs will either conduct their own internal monitoring and will elect instead to use trusted third party sources or use less expensive methods of detection. Where smaller ISPs decide to perform internal monitoring, it is extremely unlikely that they will use pervasive packet inspection technologies due to the very high costs of such technologies. Pervasive packet inspection technologies are discussed in the following section. Nonetheless it is recommended that smaller ISPs opt in to the *Privacy Act* as a demonstration of their commitment to privacy protection.

7.5.1.4 Data Retention and Destruction Policies

Some form of data retention will be required by ISPs in a bot remediation program. The E-Security Code is silent as to permissible retention duration. Theoretically, information related to bot remediation or information collected under the "network protection duty" as seen in **section 7.6.4**, may be collected and stored in perpetuity. It is therefore recommended that the E-Security Code and *Telecommunications Interception and Access Act* be amended to include a maximum retention period.

After the period of retention expires all data should be destroyed. For instance, under a preservation of data order an ISP is compelled to store data for a period of 90 days. The *Convention*, however, is silent on data destruction policies. Information collected for network performance duties and for bot remediation programs should also be destroyed after the agreed upon data retention period. It is therefore recommended that the E-Security Code and *Telecommunications Interception and Access Act* be amended to include a mandatory destruction of data upon expiry of the retention period.

---

62 Austraian Law Reform Commission, *Review of PrivacyLaw*, Recommendation 39-1.
63 Section 6EA *Privacy Act*.
64 In the *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000*, the Senate Legal and Constitutional Committee refers to a slightly wider rationale. Namely the imposition of an increased burden on small business during time where (presumably through other legislation) significant burdens were already placed on small business. This included, according to the Department of Employment, Workplace Relations and Small Business the *"compliance costs...of meeting its obligations under the Bill"* and an *"opportunity cost in terms of time taken away...in familiarizing itself with the obligation, preparing privacy statements and notifying customers"*.

7.5.1.5 Security Standards

Data collected with the E-Security Code and with preservation of data orders under the *Cybercrime Convention* should be subject to appropriate technical measures to protect the information from unlawful access, modification, interference or other forms of disclosure to third parties. Additionally, all ISPs should have an internal policy allowing only certain authorised personnel access to the stored data.

7.5.2 Passive Monitoring Techniques Should Be Used and Deep Packet Inspection Technologies Avoided

Privacy protection is of paramount concern when ISPs detect, monitor and store data logs. Many detection and monitoring methods involve filtering. Filtering may involve different heuristic methods. These methods are essentially algorithms developed to detect, absent human intervention, illegal or undesirable content. These methods include deep packet-inspection (eg. keyword sniffing[65] and keylogging), and shallow and medium packet inspection.[66] Heuristic methods examine information found in packets to varying extents, depending on the type of packet inspection technology. Heuristic methods may be divided into three groups: small packet inspection, medium packet inspection, and deep packet inspection.

Curiously, the IIA E-Security Code does not discuss detection and monitoring techniques, although they are arguably the most controversial topic of the proposal and certainly the area that, until the February 2010 amendments to the *TIA,* would have attracted the most legal uncertainty. The Code merely lists two broad possibilities: where ISPs perform internal monitoring or they rely on trusted third party sources. This is indeed odd given that the legality of detection and monitoring is dependent on the functions performed by a technology (see **sections 7.5.4.1** and **7.5.5**).

The Comcast document explicitly states that "An ISP may use Netflow [RFC3954] or other similar passive network monitoring". Comcast is, however, one of the few *known* ISPs that uses

---

[65] 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). "Just as dogs are used in airports to sniff through luggage in search of narcotics, web-sniffers are programmed to identify and locate specified types of information on the Internet. The software will be programmed to locate and track usage of key phrases and words through Internet communications."

[66] Parsons, C. "Deep Packet Inspection in Perspective: Tracing its Lineage and Surveillance Potentials" available at http://www.surveillanceproject.org/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf (last accessed May 25, 2009);

DPI technologies. In 2007 network engineer, Rob Topolski, conducted experiments to determine why Comcast customers were experiencing unusual peer to peer traffic performance. Topolski discovered that Comcast was using DPI technology to identify peer to peer packets, then secretly blocking those packets while other forms of packets were proceeding through the network. This was thought to be a case of network discrimination which violates the network neutrality principle.[67] The discovery of DPI technology attracted much media attention, and resulted in the Free Press, the Electronic Frontier Foundation, and other public interest organisations filing a petition with the Federal Communications Commission (FCC). The FCC ordered Comcast to stop the blocking, but it did not consider the legality of DPI technologies, nor did it establish the 'network neutrality' principle as law.[68] As a result of the FCC hearing, Comcast no longer blocks peer to peer packets through DPI and has instituted a new system. According to the Free Press, "Comcast's new system identifies neighbourhoods that are growing substantially congested, and then identifies individual users within those neighbourhoods that are using a substantial amount of bandwidth, and slow down those heavy users for a short period of time."[69] This is also known as speed throttling (see **section 7.7.2**). Comcast is challenging the jurisdiction of the FCC in the matter on appeal.[70] It remains unclear whether Comcast continues to use DPI - not for network discrimination and peer to peer packet blocking - but potentially to detect and monitor network traffic, and identify attributes such as whether an individual user's computer is infected and functioning as a bot. While DPI is not needed to perform bot detection and monitoring, it remains unclear whether DPI is currently used to perform the function, or more accurately, whether it might be used in the *future* to perform this function (DPI is examined in greater detail in **section 7.5.2.3**). This is important as it remains unclear whether bot detection and remediation will involve tools that move beyond Netflow towards tools considered to be DPI.

[67] Net neutrality refers to the non-prioritisation of certain packets or Internet protocols over the Internet. Internet founder Tim Berners-Lee describes net neutrality as "If I pay to connect to the Net with a certain quality of service, and you pay to connect with that or greater quality of service, then we can communicate at that level." *See* 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).

[68] Above.

[69] [d]packet.org, "Free Press White Paper Calls Out DPI" (2009) available at https://www.dpacket.org/blog/kyle/free-press-white-paper-calls-out-dpi-risks (last accessed December 2010).

[70] *Comcast v FCC* (2010) United States Court of Appeal for the D.C. Circuit available at http://pacer.cadc.uscourts.gov/common/opinions/201004/08-1291-1238302.pdf (last accessed December 2010).

7.5.2.1 Small Packet Inspection Techniques (Firewalls)

Virtually all home computers contain operating systems with shallow packet inspection capabilities, such as a firewall. A firewall has a pre-determined set of rules which tell the computer what to let through and what to block. This type of packet filtering, for example, may block or display a message warning the user of a malicious websites. It does not block encrypted traffic or data sent from such protocols as peer to peer.

7.5.2.2 Medium Packet Inspection Techniques (Netflow)

Medium range packet inspection technologies include devices that stand between an end-user's computer and the ISP gateway. Some corporations and many ISPs use virtual honeypots or application proxies. Here, all traffic from a network must pass through the stand between/ intermediary device. These types of packet inspection technologies differ from a mere firewall in that they use more data sets to determine whether to block a packet or allow it to pass. Application proxies examine format devices, protocols, port numbers and associated locations instead of merely analysing the URL (IP Address) as in shallow packet methods.

One commonly employed medium packet inspection technology used by ISPs is NetFlow. NetFlow is used perform statistical analysis of network traffic. ISPs use NetFlow in conjunction with a router to analyse nine packet attributes: 1) IP source addresses, 2) IP destination addresses, 3) source port, 4) destination port, 5) layer 3 protocol type, 6) class of service (whether high or low priority for traffic flow), 7) router interface, 8) the amount of data transmitted (number of packets), and 9) the date and time of the data flow.[71] This method does not collect information pertaining to email addresses of intended parties, words in the subject line, body of the message, file attachments, URLs visited (search queries), bookmarks or cookies. NetFlow also is the protocol recommended for automated network monitoring by the Internet standards organisation, IETF.[72] There seems to be a consensus among network researchers as well as some academics about the appropriateness of the design of Netflow to effectively monitor traffic without impairing the privacy of users.[73]

---

[71] Ohm, P. "The Rise and Fall of Invasive ISP Surveillance" available at http://ssrn.com/abstract+1261344 (last accessed April 15, 2009)
[72] Leinen, S. RFC 3955: Evulatuation of Candidate Protocols for IP Flow Information Export (IPFIX) Oct. 2004.
[73] *See for example*, Ohm, note 73 above, page 61.

7.5.2.3 Deep Packet Inspection Techniques

Deep packet inspection (DPI), meanwhile, involves technologies that literally peer deeper into packets. In other words, DPIs are capable of collecting information pertaining to the email addresses of intended parties, words in the subject line, words in the body of the message, file attachments, and URLs visited (search queries). Many North American ISPs employ DPI for Internet traffic shaping. This involves prioritizing certain types of traffic to better control congestion and materializes in a few different contexts. Those who pay a premium rate may, for instance, be given access to preferential accelerated traffic rates. Commercial websites may be given higher priority at peak traffic times than traffic using controversial peer-to-peer systems such as Bit Torrent. Traffic shaping is part of a larger research area on network neutrality.[74]

Most DPIs provide information about where a packet is generated in real-time, IP address destinations, ports, protocols, application types and, most importantly, packet exchange patterns. DPIs are not able to perform deep packet inspection in protocols such as Skype, proxies such as Tor and encrypted peer-to-peer programs. The initial packet exchange however of something like Tor utilizes common information patterns which could identify when a request to use the Tor proxy is being made. DPIs do not store data but look for patterns of data within packets. A common parallel is looking inside an envelope or parcel to see the contents. Just as a post office employs x-ray techniques to search for known shapes such as knives, guns, etc, DPIs look for known problematic patterns. The People's Republic of China employs pervasive DPIs, as do many Western democracies investigating terrorism. The United Kingdom, by way of example, is expected to bring forward a draft Communications Data Bill under the Intercept Modernisation Programme which will require ISPs to monitor, capture and retain Internet data for the purposes of security and anti-terrorism.[75] There seems to be consensus that this type of monitoring will require DPI technologies that snoop into the internal body of communications.[76]

ISPs do not readily employ DPI for spam and virus detection, or for general security purposes. Further, DPI is not necessary for malware analysis. For example, a security expert could analyse FastfFux botnets/attacks a variety of ways. One could employ a simple Pethon script where an

---

[74] *See, for example,* Riley, C. And Scott, B. "Deep Packet Inspection: The End of the Internet as We Know It?" March 2009 available at www.freepress.net (last accessed April 17, 2009). See also the research movement of Network Neutrality Squad (NNSquad) whose members include some of the most respected Internet experts. NNSquad documents violations of the network neutrality principle noting examples of ISP traffic shaping.
[75] Known as the 'Intercept Modernisation Programme'. See *Privy Council Review of Intercept as Evidence Report CM7324* (January 30, 2008) available at http://www.official-documents.gov.uk/document/cm73/7324/7324.pdf
[76] Clayton, R., "Phorm Analysis" (July 2008) available at http://www.unitethecows.com/digital-media-news/47406-phorm-analysis-richard-clayton-released-trials-continue.html (last accessed December 2010).

entity feeds malicious or suspicious domains and maintains a database of where those domains point, either their NS records (name server) or A records (address) or whatever else. This allows an ISP to map a FastFlux botnet based on a variety of parameters without using DPI or otherwise invading a customer's privacy.[77] Typically, medium style packet inspection methods such as a network analyzer are all that an ISP requires to track FastfFlux botnets. Inaccuracy, over-breadth and invasion of privacy render DPIs controversial.[78] One of the inventors of the World-Wide-Web, Tim Berners-Lee, describes DPI as the electronic equivalent of opening people's mail without authorisation to do so where 'what is at stake is the integrity of the Internet as a communications medium.'[79]

Many ISPs use medium range inspection methods such as NetFlow that collect IP addresses as well as other key information to perform statistical analysis of network traffic. Netflow is an example of a passive monitoring method. This method is passive as it does not collect information pertaining to email addresses of intended parties, words in the subject line, body of the message, file attachments, or URLs visited (search queries).

My conclusion from a policy perspective is that more pervasive detection and monitoring methods generally should not be used for purposes of botnet control. Deep packet inspection (DPI) involves technologies that are capable of collecting information pertaining to the email addresses of intended parties, words in the subject line, body of the message, file attachments, and URLs visited (search queries). Most DPIs provide information about where a packet is generated in real-time, IP address destinations, ports, protocols, application types and, most importantly, packet exchange patterns. As previously explored, this is the equivalent of peering into the content of a parcel and examining the content of what is contained inside. The use of DPIs pose the greatest concern from a privacy and surveillance perspective. The IETF Comcast working draft distinctly notes that passive (shallow and medium range methods) methods are preferred.[80] The IIA document is silent on preferred detection and monitoring technologies, and possible issues arising from their use but notes that detection "does not require the surveillance

[77] Correspondence with Scott McIntyre, Security Officer for XS4ALL Internet B.V., kernel-team Security Officers for KPN-CERT, and steering committee member of FIRST: The Forum of Incident Response and Security Teams.
[78] *See* Bendrath, R. "Global Technology Trends and National Regulation: Explaining Variation in the Governance of Deep Packet Inspection" International Studies Annual Conference Paper (Feb. 2009) available at http://userpage.fu-berlin.de/~bendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf (last accessed May 25, 2009).
[79] ZDnet, "Berner-Lees says no to Internet 'snooping'", March 11 2009 available at http://news.ndnet.co.uk/security/01,000000189,39625971,00.htm (last accessed April 16, 2009)
[80] Comcast, note 3 above, page 10.

of individual online activity." It is assumed, based on these comments, that the IIA is not contemplating the use of DPI technologies to achieve their objectives.

There is no guarantee that DPI is not presently used by Australian ISPs or that it will not be used in the future.[81] As disclosed in the Australian Senate Standing Committee on the Enquiry into Cyber Crime and Consumer Protection, no organisation could accurately point to what technologies ISPs currently use for communication monitoring nor could they accurately point out with certainty when and to what extent ISPs were required to cooperate with law enforcement and other agencies. Indeed this lack of transparency seems to be a problem in other jurisdictions as well. For example, prior to the Canadian Radio and Telecommunications Commission's (CRTC) enquiry into the practices of Canadian ISPs traffic management, the extent of DPI use in Canada was largely unknown.[82] After the enquiry, it came to light that the major Canadian ISPs (Bell and Rogers) had been using DPI to speed throttle peer-to-peer traffic. This is known as traffic shaping. It also became known with the CRTC enquiry that Rogers had a bot remediation program similar to the one proposed in Australia. It is unknown if DPI technologies are used by Rogers for this purpose.

In the United Kingdom, the ISP Virgin uses a DPI technology known as cview. According to the company's website, cview "applies high volume advanced analytics to anonymous ISP traffic data, and aggregates this information into a measure of the total volume of unauthorised file sharing." Virgin customers pay a set fee to have unlimited streaming and downloading of content from Universal. Cview is used to monitor those customers who are not paying the fee and who are illegally downloading copyright infringing material. There is nothing anonymous about the DPI technology as IP protocols are collected. According to Privacy International, a European privacy watchdog led by Simon Davies, the extent of anonymity is that only IP addresses are collected, not usernames. The trivial ability of an ISP to link an IP address to a username, however, makes the claim of anonymity ridiculous. Privacy International has complained to the European Union that cview is a wiretap which requires a warrant or customer consent.[83] The outcome of this review is unknown as of March 1, 2010.

---

[82] Parsons, C. blog on DPI available at www.delicious.com/caparsons/dpi (last accessed December 2010).
[83] A summary of the complaint is available from Privacy International at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-56569&als[there]=Communications%20surveillance (last accessed February 26, 2010).

Regardless of whether medium or deep packet inspection technologies are utilised, both types of methods involve the collection of IP addresses and/or domain names linked back to the person registering domain names. The point is not whether such technologies are or will inevitably be used, but what safeguards are in place to ensure that abuse does not occur. This triggers some concerns of privacy and surveillance. Privacy and other legal implications of detection and monitoring technologies are explored in **section 7.6**.

7.5.3 Methods Should be Non-Disruptive and Should Not Block Legitimate Traffic

That methods should be non-disruptive and should not block legitimate traffic is not contentious for threats that are not classified as sufficiently serious. For example, where a botnet is used in an attack on critical infrastructure such as a city's electrical grid blocking of legitimate traffic may be necessary. The CERTS as discussed in **Chapter 1** use a sliding scale to assess threats. Where a malware threat is sufficiently serious, then blocking of legitimate traffic may be necessary. It is not in the business interest of ISPs to disrupt or block legitimate traffic. Detection and monitoring methods are not fool proof. Inevitably some legitimate traffic may be blocked while some users' services may occasionally be disrupted. The blocking of legitimate traffic outside the context of prevention of a serious threat is likely to be limited to situations where there has been a false-positive identification of a compromised computer. There are methods, as discussed below, to minimise false-positive identification of computers.

7.5.4 Use of Multiple Point Bot Detection

The user of multiple point bot detection data points should minimize false-positive identification of computers where detection at one data point is cross-referenced and verified at other points. So, for example, an ISP might perform port scans, utililze Netflow packet inspection, or operate a honeynet to gather information. ISPs will also receive information from AISI, AusCERT and other trusted third party resources, along with have a list of customer generated complaints. These sources could be cross-referenced. Cross-reference of multi-data points could be done through an automated process. Where a computer is designated as compromised in only one data point, it is desirable, where possible, to confirm that the bot is indeed malicious in nature. This would likely involve a non-automated process requiring staff to verify the nature of the bot. The cost of doing so may prove infeasible for some ISPs.

7.5.5 ISPs Should Error on the Side of Caution

ISPs may elect to classify the nature of the botnet, whether it is malicious, active or dormant. Classification of a bot might include an analysis of the type and severity of the threat. Bots might be a spam bot, or a key-logging bot which steals information, file distribution bot, bot used to distribute illegitimate content, and so forth. Classification of bots is of limited use due to their transformative nature. As outlined in the Comcast IETF draft, "given the dynamic nature of botnet management and the criminal incentives to seek quick financial rewards, botnets frequently update or change their core malicious capabilities."[84] If an ISP elected to classify the nature of a botnet, this would require continuous monitoring and tracking of the botnet in real-time. Dormant botnets, in the same vein, may be benign at their time of classification, then suddenly become active. It also may not be possible in some situations to positively identify when a botnet is malicious or benign. For these reasons, Comcast recommends that an "ISP should probably err on the side of caution by communicating when a likely bot infection has take place." This also serves as a preventative measure where a client at risk will act to better protect their computers. The Comcast recommendation should be endorsed.

7.5.6 Time-Sensitive Detection Methods Are Imperative

The dynamic nature of botnets as described in **Chapters 1** and **3**, make real-time detection methods more valuable than the use of methods that are not time-sensitive. The need to identify when a computer is likely to be compromised often requires a quick response. The need for real-time detection and monitoring techniques was examined in **Chapters 4 and 6.** The more effective real-time methods necessitate ISP detection and monitoring with troubling computers being wall-gardened (examined in **section 7.7.4**) or their connectivity temporarily suspended. Early detection and notification to the user means provides a number of benefits as outlined in the Comcast document:

> "users may benefit from the deployment of client-based software protections or other software tools, which can enable rapid performance of heuristically-based detection bot activity, such as the detection of a botnet as it starts to communicate to a bot net and execute some type of command. Any bot detection systems should also be capable of learning and adapting, either via manual intervention or automatically, in order to cope with a rapidly evolving threat."[85]

Walled- gardens and suspension of accounts, however, will inconvenience a user. Where a botnet imposes a serious threat, relevant authorities will be notified. In this case, relevant

[84] Comcast, note 3 above, page 8
[85] Comcast, note 3 above, page 9.

authorities, as discussed in **section 7.7.9,** refer to AusCERT is then able to issue warnings of the threat to its members, as well as other national CERTs around the world.

7.5.7 Period and Transparent Review of Program

Monitoring and collection of information, whether performed for an ISP bot remediation program, under "network protection duties" or compelled by law enforcement under national or international obligations creates an environment where civil liberties will be diminished. As will be explored in **section 7.12** there are many civil liberty implications of ISPs performing functions traditionally associated with law enforcement. It is imperative that initiatives such as ISP bot remediation be subject to periodic and transparent review in order to determine if such monitoring and collection of data is having an impact on botnets, how have civil liberties, if at all, been affected, and whether or not there are less pervasive methods of performing similar tasks. This is equally true for ISP obligations for preservation of data orders, interception, and search and seizure. There needs to be reporting of how many times the provisions were used, whether their use led to charges being laid, and whether there were any impacts on civil liberties. In order for the reporting to be effective, it is recommended that it be done in a transparent fashion.

7.6 ISP LIABILITY FOR DETECTION AND MONITORING

According to privacy expert Nigel Waters, in Australia, "The general position is that the police and many other government agencies may request information from private sector organisations relating to customers or employees. It is then up to the recipient of that request to weigh up the public interest in co-operating against customer privacy."[86] As will be seen, Australian information privacy laws limit the type and amount of detection and monitoring by agencies in theory; in practice, however, "They serve more to ensure a minimum level of transparency and procedural fairness, as well as to require minimum standards of data quality and security."[87]

Before liability of ISPs for detection and monitoring of traffic is explored, there are a few generic points that require establishing. First, telecommunications carriers (includes ISPs) are required by law to have interception capabilities, generally to be used for evidence gathering in connection

[86] Waters, note 63 above.
[87] Above, page 5.

with serious offences (crimes such as murder, terrorism, and child pornography).[88] Second, interception and examination of communications typically requires a warrant. Warrant regimes, as seen in **Chapter 6**, vary based on the type of content to be intercepted (Eg. financial information as opposed to security intelligence as opposed to e-mail or postal communications). Third, up until February 2010, there were a number of restrictions placed on ISPs which limited their detection and monitoring capabilities under the *Privacy Act 1988 (PA*), *Telecommunications Act 1997 (TA), and Telecommunications (Interception and Access) Act 1979 (TIA).* Many of these restrictions have been lifted under the 2010 amendment to the *TIA*. ISPs are in essence shielded from liability where they are performing network protection duties. It is this last generic issue - the limits of legal ISP detection and monitoring methods - which is explored in the analysis below.

7.6.1 Liability under the *Privacy Act 1988*

ISPs are bound by the *National Privacy Principles* (NPPs). These are: Principle 1 - Collection, Principle 2 - Use and disclosure, Principle 3 - Data quality, Principle 4 - Data security, Principle 5 - Openness, Principle 6 - Access and correction, Principle 7 - Identifiers, Principle 8 - Anonymity, Principle 9 - Transborder data flows, and Principle 10 - Sensitive information. ISPs are also bound by the privacy obligations in the *Telecommunications Act 1997* and *Telecommunications (Interception and Access) Act 1979* that relate to detection and monitoring of communications, and unlawful disclosure of communications (**see sections 7.5.5.2 and 7.5.5.**

7.6.2 Liability under the *Telecommunications Act 1997*

As seen, the *PA* applies to large telecommunications providers, but small ISPs are exempt from the NPPs Small ISPs are not exempt from the disclosure and interception obligations found in the *TA* and *TIA*. Content monitoring is generally thought of as coming under the purview of the *TIA* while other types of information such call charge records are regulated by the *TA*.[89] According to Waters, information other than content of communications would be governed under Part 13 of the TA where "[t]his Part generally prohibits disclosure without the customer's consent but expressly authorises a range of disclosures including to specified law enforcement

[88] TA Part 15. A serious offence also includes any criminal offence which would attract a minimum of 7 years in prison. The unauthorised access to a computer (hacking provisions) would qualify as a serious offence as the maximum sentence is 10 years.
[89] Waters, note 63 above, pages 7-10.

and revenue protection agencies."[90] Those specified law enforcement agencies largely refer to the Australian Federal Police, State Police, ACMA, ACCC , and the Telecommunications Industry Ombudsman.[91] Part 14 of the TA addresses disclosure by warrant to the relevant law enforcement authority.[92] Part 13 establishes a certificates regime of 'reasonable necessity' where the strict procedures that normally govern warrants are substituted with a less onerous regime of certificates. This also allows an ISP to exercise discretion whether to disclose information in some situations. Detection and monitoring techniques for bot remediation may be considered as content monitoring and are accordingly governed by provisions of the *TIA*. The *TIA* is considered below.

7.6.3 Liability under the *Telecommunications (Interception and Access) Act 1979*

Interception and examination of communications is regulated under the ***Telecommunications (Interception and Access) Act 1979*** ***('TIA')***. The TIA regulates both 'communications' (information such as an email as it passes over the Internet from one point to another) and 'stored communications' (communications when they are not passing over a telecommunications system and where they are held by a carrier, such as an ISP that stores the email content).[93] The *TIA*, as Waters note, has been subject to continuous and frequent amendments over the past 15 years.[94] Prior to the February 2010 amendment to the *TIA*, ISPs could not legally monitor and examine the content of communications unless expressly authorised to do so under the law. This meant that a warrant was required to examine such communications in the course of compliance with law enforcement. As seen in **Chapter 6** and in previous sections of this chapter, there are several warrant regimes depending on the type of content being examined (Eg. security intelligence, related to serious offence, b-party, spam and so forth).[95] Medium and deep packet inspection technologies examine, to varying degrees, attributes of packets that travel over the Internet. The extent of which the content of communications is examined depends on what attributes of the packets are inspected. It has been argued by the United Kingdom watchdog, Privacy International that technologies which collect information about IP addresses violate

[90] Waters, note 63 above page 10.
[91] *TA,* s. .279-299
[92] TA , Part 14.
[93] TIA, s. 5 Interpretation.
[94] Waters, note 63 above.
[95] Above.

privacy law and require warrants under European law though this watchdog appears to be the only entity to publicly embrace this position.[96]

The ability of an ISP to protect their networks and customers from security risks requires detection and monitoring of Internet traffic, whether this is done by the ISP itself or by a third party. It is unclear under the *TA* and *TLA* whether a warrant is required to monitor content for network security purposes. The uncertainly is present regardless of whether medium or deep packet inspection technologies are used. For this reason, the *TLA* was amended in February 2010 to clarify "the basis on which communications can be accessed for the purposes of protecting a computer network."[97] The *TIA* Act currently includes an interim exemption for ISPs to perform network protection activities but these provisions were not intended to be permanent. The network protection exemption ceased to have effect after December 12, 2009. The 2010 February amending act formalised the scope of exemption for network protection. The main components of the amendments are considered below.

7.6.4 *Telecommunications (Interception and Access) Amending Act 2010*

The Explanatory Memoranda (EM) of the 2009 bill succinctly summarises the main points of the recent amendment to the *TIA* as follows:

> The amendments contained in the Bill will:
>
> - enable all owners and operators of computer networks to undertake activities to operate, maintain and protect their networks
> - enable Commonwealth agencies, security authorities and eligible State authorities to ensure that their computer network is appropriately used by employees, office holders or contractors of the agency or authority
> - limit disclosure of secondary use and disclosure of network protection activities to:
>   a. network protection activities
>   b. undertaking disciplinary action against an employee, office holder or contractor of a Commonwealth agency, security authority and eligible authority of a State who has been given access to a network, and
>   c. reporting illegal behaviour that attracts a minimum of three years' imprisonment penalty threshold to the relevant authorities
>
> - require the destruction of records obtained by undertaking network protection activities when the information is no longer required for those purposes.

The 2010 amending act sets out a concrete definition of network protection duties, establishes who is entitled to perform such duties, sets limits to third party disclosure, and places limits and

[96] Note 86 above.
[97] Explanatory Memoranda, *Telecommunications (Interception and Access) Bill 2009*.

penalties against unlawful use of the data collected by government agencies. The 2010 amendments to the TIA define 'network protection duties' as "in relation to a computer network, means duties relating to: (a) the operation, protection or maintenance of the network". Network protection duties specifically includes the right to intercept communications with the exception of voice communications.[98] Interception of communications must be performed by an authorised person of a computer network. Authorised person in this context has two meanings. The amendments establish that a responsible person for the network must be designated, and that any other person performing interception of communications must have authorisation from the responsible person in writing.[99] Further restrictions are then placed on disclosure of the content of the intercepted communication to third parties. An ISP may elect to disclose to "an officer of an agency" any content of an intercepted communication whether there is reason to believe that a prescribed offence has been committed.[100] "Officer of an agency" is not defined in the legislation. Under the *TIA*, 'agency' means interception agency or another enforcement agency where these two terms essentially refer to similar agencies that are able to obtain interception warrants such as the Australian Federal Police, ACMA and so forth.[101] It remains unclear whether the restriction to disclose information is limited to officers of an agency, and therefore sharing of any list of IP addresses connected to bots with other ISPs would violate this provision. It appears that an ISP could disclose the information to ACMA who could then relay the information to other ISPs providing there was reason to believe that a prescribed offence had been committed. The direct disclosure of bot information retrieved from interception of communications to other ISPs remains legally ambiguous under the 2010 amendments.

7.5 ACTIONS TO BE TAKEN ONCE A COMPROMISED COMPUTER IS DETECTED

The IIA e-Security Report offers a series of potential actions to be taken by an ISP involving notification and quarantine methods. As outlined in the consultation document, the IIA recommends a series of potential actions, none of which are discussed in any detail. These are:

[98] *TIA Amending Act 2010,* section 7(3) excludes voice communciations such as VOIP and SKYPE.
[99] *TIA Amending Act* 2010, section 7(2).
[100] *TIA Amending Act* 2010 , section 63E.
[101] *TIA*, Interpretation section.

Actions to be Taken once a compromised customer is detected

Once an ISP has detected a compromised computer or malicious activity on its network, it should [ ] take action to address the problem.

ISPS should therefore attempt to identify the end user whose computer has been compromised, and contact them to educate them about the problem.

Examples of actions that ISPs can take when they become aware of a compromised computer and have identified the relevant customer are:

(a) Notify the customer directly (by phone or email);

(b) Apply an 'abuse' plan where the customer's Internet service is speed throttled;

(c) Temporarily suspend the customer's account until they advise they have taken remedial action. (Suspension could occur for customers appearing on the source lists for the first time and/or customers re-appearing on the lists);

(d) Place the customer's account in a 'walled garden' with links to relevant software-information pages that will assist them to clean-up their computers;

(e) Temporarily suspend compromised ports/protocol activity;

(f) Regenerate the customer's account password to prompt customers to call the helpdesk so they can be educated about the issue;

(g) In the case of Spam sources, apply restrictions to outbound SMTP; and/or

(h) Provide the customer with a timeframe in which to take remedial access and if this is not adhered to, terminate their service. (Termination of a customer's service would generally only be suggested in the most extreme of cases, where the customer has refused to take action to resolve the situation, e.g. by installing anti-virus software, or where the amount of Spam being sent via the customer's account is causing network impacts, etc.)

ISPs may choose to use one or more of the above examples, and may choose different options depending on whether it is the first time a customer's IP address has appeared on the source lists or whether they continue to appear on the lists and have taken no remedial action.

A variety of issues arise from the above possibilities, which are explored below. The options suggested in the IIA e-Security Code are not explored individually but instead, are grouped where relevant as many of the issues are overlapping. Due to the lack of discussion within the IAA Code on the relevant suggested methods, this section borrows discussion generated from the Comcast IETF draft and the ITU Botnet Toolkit.

7.7.1 Notification of Internet User

The IIA recommends that notification occur by phone or email. Telephone communication may be desirable method, as it allows the user to ask questions and become informed based on

personal interaction. This might be particularly desirable with high-risk situations where, for example, a user's computer is an active malicious bot used in a DDoS attack against a bank. This, however, would be costly to ISPs and would require well-trained personnel and would likely not be feasible from an organisation's resource perspective.

Email notification will likely prove the more common form of notification. Weaknesses in this format of notification include notices being ignored by the customer or the notification being sent to an email that the user does not often use. Indeed the notice may be perceived by the user as spam. On a more serious basis, as pointed out in the IETF Comcast draft, "Bot masters have also been known to impersonate the ISP or a trusted sender and send fraudulent emails to the users."[102] It is also possible that usernames and passwords have been compromised, that instructions to delete the ISP notification email could be given to the bot. ISPs will have to guard against malicious actors subverting the notification process for ill purpose.

7.7.2 Abuse Plan for Speed Throttling

Where a customer's computer becomes infected, a speed throttle may be imposed to act as a way to get the compromised machine remedied. Speed throttling works by slowing one's Internet connection. Speed throttling is used by many ISPs during heavy Internet traffic periods to prioritise certain types of packets, typically commercial services over other services such as peer-to-peer filesharing, as seen in **section 7.5.2**. Speed throttling will only be an issue where an ISP guarantees a customer a certain Internet speed which is then not met with the imposition of a speed throttle.

7.7.3 Temporary Suspension of Customer's Account

Temporary suspension of a customer's account provides a more disruptive means of incentivising the customer to remedy their infected machines. It may also provide a more effective method of encouraging customers to hastily clean their machines. A temporary suspension of service raises similar issues to walled gardens which are discussed in greater detail below.

[102] Comcast, note 3 above, page 12.

7.7.4 Walled Gardens, Temporary Suspension of Customer's Account or Port, and Similar Quarantines

An ISP could suspend a user's connectivity until otherwise notified by the customer that they had remedied their computer. A method gaining more popularity that runs along a similar vein is placing customers in a "walled garden". A walled garden is defined below as:

> A walled garden refers to an environment that controls the information and services that a subscriber is allowed to utilize and what network access permissions are granted. This is an effective technique because it could be able to block all communication between the bot and the command and control channel, which may impair the ability of a bot to disrupt or block attempts to notify the user.

A walled-garden is the equivalent of being pulled over while driving for having a vehicle that, unbeknownst to you, is unfit and dangerous. The car is then placed in a tow lot or is towed to a mechanics garage for repair. The car is not allowed the road while it is not safe. Once the car has been fixed by a mechanic and deemed fit for use, the owner is once again able to drive the car. The inability to use the dysfunctional car is, of course, an inconvenience to the owner but these measures are taken as motorway safety is thought to trump other considerations. Walled-gardens are similar. When a computer is compromised, the ISP restricts its use. This is like being placed in a virtual tow lot. The user is still able to perform certain functions with the computer, just as a driver would be able to sit in the car, listen to the stereo, turn it on to run air conditioning, and so forth. Only the hazardous services are restricted until a computer is remedied.

Walled-gardens also pose many challenges including when to let a user out of a walled garden. One approach, as outlined in the IIA proposal, is to allow the user to judge when they are to be let out of a walled-garden. The walled-garden would direct users to information to remedy the computer. The user then decides whether they will remedy the computer first before exiting the walled garden, or exit first then remedy at a later date in time. This is the equivalent of being pulled over and notified that your car is unfit, but then being allowed to drive the car away. The driver could continue to drive the unsafe vehicle without repairing it, and risk being pulled over again. Other options include the driver requesting to be towed straight to a mechanics shop, or repairing the car at a more convenient time to the driver. With this approach, the user makes the determination. If this method is adopted, there should be a verification process to ensure that it is indeed the user that has requested permission to exit and not the bot. Bots could be programmed to automatically request exit from walled-gardens.

A different approach might require the user to prove that the computer has been remedied. This more strict approach is a safer option but may not be feasible for a number of reasons. The ISP would need scanning tools to determine if the machine is still infected. While this is possible, it may not be cost effective for smaller ISPs. The greater issue concerns technical feasibility of bot removal. The sophistication of the bot may render any user attempt to remedy the machine difficult or in some situations, impossible. This is explored in greater detail in **section 7.9.**

If an ISP deploys a walled-garden it is imperative that users are still able to access security vendors to search for security updates, and patches to remedy their computers. An ISP should keep a list of well-known and trusted security and bot removal vendors to recommend to their customers.

7.7.5 Temporarily Suspend Compromised Ports/Protocols Activity

Temporary suspend of compromised ports and protocols is a more tailored approach to suspension of Internet activities. If, for example, there were heavy malicious traffic in port 80, the ISP may block traffic on that port. Similarly ISPs may block certain protocols such as a peer-to-peer program which is involved in the breakout of a new and serious botnet, until such time as anti-virus vendors may develop a patch that protects against the malicious software.

7.7.6 Regeneration of Customer Password

The regeneration of a customer password is an incentive mechanism to get the customer to communicate with the ISP. Upon making a request for a new password the ISP would use the opportunity to explain to the customer that a new password is required because their computer has been compromised. The ISP would then direct the customer to information to help clean the computer.

7.7.7 Restrict Outbound SMTP

Where a botnet or malware with high threat classification (**Chapter 1**) is propagating through outbound SMTP, temporary suspension or restriction of SMTP may be necessary until a patch can be found for anti-virus software. With a botnet with a lower threat rating – one where anti-

virus software protects a customer from the exploit – the user outbound SMTP (email) may be restricted until such time as the customer remedies his/her machine.

7.7.8 Termination of Service

Termination of service is a measure that should only be taken in extreme situations. The IIA suggests that extreme cases might include a users' refusal to install anti-virus software within a specified timeframe or in situations where the Spam volume sent from the user's account is impacting on the network. No mention is made in terms of what a reasonable time frame might be for the installation of anti-virus software or what volume level of spam sent or network impact thresholds are necessary. There are a number of potential problems with these two examples.

What is a reasonable time frame for anti-virus installation once a customer has been notified that their computer is a bot? If, for example, two weeks is deemed reasonable notice, then question becomes whether notification means actual notification (ie. The customer opens the email) or deemed notification (the notification is deemed to have been read by the customer as it is received in the email inbox). Termination of services should operate similarly to other essential services and billing procedures. Where a customer has not paid their bill for a telephone or Internet connection, a warning is issued, followed by successive warnings with a set date for disconnection. It is arguable, that any termination of Internet service should involve a method other than email due to its volatility. Post mail seems a more appropriate method for termination of services.

7.7.9 Reporting Malicious Activity To Law Enforcement

> (a) Where the ISP believes that the nature and extent of the network compromise is of sufficient severity, the ISP should report this to the relevant agencies as set out in Schedule 3 of this Code. In the event of serious network incursions which invoke concerns about major cyber attack or major criminal activity, [.] Schedule 3 contains a list of agencies to be notified.

Schedule 3 specifies AusCERT or its successor as the only agency to be notified in the event of a serious attack. This recommendation does not present a new development. ISPs have been notifying AusCERT of serious network compromise for quite some time. There is also significant industry sharing of intelligence within the ISP sector.

7.8 EDUCATING CUSTOMERS

There is a universal call for the need to educate users about their online activities. The need for education and training is echoed in Government documents, policies, by security experts, banks, ISPs, consumer groups, and end-users. Notification and education of customers by ISPs will merely be one of many required initiatives in the effort to educate users.[103] The IIA recommends that:

> (a) It is recommended that customers be notified that their computers are suspected of being compromised according to standardised notifications as set out in Schedule 1 to this Code.
>
> (b) Additional resources are available at www.tortoise.iia.net.au. ISPs are encouraged to direct customers to this resource.

The biggest question which remains to be seen is if educating the customer through providing links to information, and then sending the customer away to fix the problem on their own will prove too big an onus on the user. As will be discussed in **section 7.9**, users in many instances will not be able to remedy their computers.

7.9 LIMITATIONS AND SCOPE OF BOT REMOVAL

7.9.1 Bot Removal Side Effects

The techniques described in this chapter are not absolute in their effectiveness. There are no examples of success or failure rates of such programs at present. Bot removal may be beyond the ability of many users. It may be the case that bot removal requires specialized knowledge and skills. The reality is that attempts to remove bots may prove unsuccessful or only partially successful. Comcast states that "the only way a user can be sure they have removed some of today's increasingly sophisticated malware is by 'nuking-and-paving' the system: reformatting the drive, reinstalling the operating system and applications (including all patches) from scratch, and then restoring user files from a clean backup".[104] ISPs who have used bot remediation programs, such as Comcast in the United States, Rogers in Canada and Australian ISPs participating in AISI have not published any statistics on the effectiveness of bot remediation programs.[105]

---

[103] *See for example*, Australian Government, *Cyber Security Strategy* (2009) available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf (last accessed January 29, 2010).

[104] Comcast, note 3 above, page 7

[105] I have asked AISI (of ACMA) for the statistics of the trial period and have not received a response.

Comcast notes that bot remediation programs "may leave a user's system in an unstable and unsatisfactory state or even in a state where it is still infected [and] ... attempts at bot removal can also result in side effects ranging from a loss of data or other files, all the way through partial or complete loss of system usability."[106] Again, the effectiveness of such bot remediation programs should be analysed against any damages and side-effects of a program. Currently the IIA Code does not provide for review of the program in order to ensure its effectiveness.

7.9.2 Recidivism

Recidivism refers to the recurrence of infection in a remedied machine. Compromised machines are cleaned and basically re-infected. According to the ITU, the Internet Architecture Board considered the issue at a workshop on "Unwanted Internet Traffic".[107] The IETF noted that notifications by ISPs would likely have a limited impact on user's remedying their machines. Users might ignore the notification, or clean their machine only to become re-infected within a short period of time. Notification where coupled with a mechanism designed to illicit expedient customer action such as speed throttling, walled gardens, suspension of services and ultimately, termination of services where machines are unremedied, will prove more effective than mere notification with a link to how to clean up a machine. It is possible that machines will become re-infected once cleaned up. By installing anti-virus software and software to update routers and operating systems, the likelihood of re-infection is reduced significantly. One must remember that ISP involvement will be infinitely more effective with an overall cyber strategy where multiple-enablers, along with law enforcement agencies are involved. Changes, for example, to domain name resolving as discussed earlier in this chapter, along with changes to law enforcement as discussed in **Chapters 4 and 6.**

7.10 THE EVOLVING LIABILITY STRUCTURE FOR ISPS

As a cultural phenomenon, the Internet has been strongly associated with freedom of communication. Since their inception in the early 1990s, ISPs have not been required to police the content their users place upon the Internet. At the same time, ISPs are in an unrivalled

[106] Comcast, note 3 above, page 7.
[107] ITU, note 27 above, page 32 referring to IETF's Internet Architecture Board workshop on "Unwanted Internet Traffic". The workshop proceedings are summarized in RFC 4984 and are available at http:??www.isi.edu/in-notes/rfc4948.txt (last accessed January 29, 2010).

position to suppress content held on their systems by removing access to resources — web space, connectivity, file access permissions, and so on — from their customers.[108] The ISP is often the only entity that can identify customers in the real world, and so they must necessarily become involved before the true originator can be held accountable for the presence of unlawful content. Hence many content removal regimes make ISPs liable for content once they have been informed of its existence. If they fail to 'take-down' the material then sanctions against them may then proceed. This gives rise to various complexities because the ISP, and the network professionals working for them, may be constrained by data protection legislation, by professional codes of practice or ethics, or by common law notions of confidentiality, from disclosing the information haphazardly. ISPs, intermediaries and network professionals are also reluctant to be drawn into acting as a plaintiffs' agent against their own individual or business customers — and at the very least demand recompense for their efforts, along with immunities when errors are made.

While potential liability proves as a disincentive in many respects, the role of ISPs is shifting to that of a vital intermediary to collect and broker information to law enforcement and other parties.[109] ISPs are being asked to censor in an indirect way. As Clarke describes it, "It's not 'censor': it is 'monitor, contact, report/disconnect"', whereby ISPs are certifying whether a computer is 'fit for connection to the Internet."[110] This can be seen in a number of contexts outside of Internet security. ISPs, for example, are required to takedown materials that violate copyright law once they have been notified of the infringing content.[111] The shielding parameters of the safe harbour provision were fortified in the recent iiNet decision .[112] The Australian Internet Industry Association have indicated that they are putting together a new industry code on copyright notice and takedown procedures following the decision.[113] Defamatory material and other types of offensive material must likewise be taken down within a reasonable timeframe once an ISP is notified. Clause 91 of Schedule 5 of the *Broadcasting Services*

---

[108] Schruers, M. "The History and Economics of ISP Liability for Third Party Content" Vol. 88 Virginia Law Review 205.
[109] 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.
[110] Clarke, R. Comments made in the Link-ed list serve. On file with author.
[111] Service providers were found liable for secondary copyright infringement in the seminal case of *University of New South Wales v Moorhouse* [1975] 133 CLR 1. Since this 1975 High Court of Australia decision the *Copyright Act 1968* was amended following the signing of the *United States and Australia Free Trade Agreement*. ISPs now have a safe harbour where they are compliant with a series of requirements related to notice and takedown of infringing material.
[112] *Roadshow Films Pty Limited v iiNet Limited* [2011] FCAFC 23
[113] At an informal gathering of an IEEE event, a member of the Internet Industry Association stated that the IIA was putting together a new code on copyright notice and takedown for ISPs. The event was (March 21, 2011).

Act 1992 (Cth) shield ISPs and Internet Content Hosts (ICHs)[114] from liability for carrying or hosting offensive third party Internet content where they were not aware of the nature of the content. Once an ISP becomes aware of the nature of content, they must act expeditiously to remove such content. Recent 2010 amendments to the *Telecommunications (Interception and Access) Act 1979*, remove much of the ambiguity of ISPs ability to actively monitor, collect data, and protect their networks. The liability, however, is not absolute. ISPs must still comply with privacy law, telecommunications law and the contractual provisions in any terms of service agreements.

Where ISPs take action against customers who have been identified as having a compromised machine, and/or have been identified as a source of a cyber-attack, the ISP is exposed to liability. The customer may initiate civil court action for wrongful disconnection. Telstra made a submission to the Inquiry Into Cybercrime calling for ISP immunity. Specifically, the Telstra document asks the government to:

> "Provide legislative protection for a carrier or Internet Service Provider (ISP) from third party claims when it undertakes activities, in good faith (or as agreed with government and/or industry), to protect their networks and services and customers from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or the States or Territories. (This would be similar to the protection given under section 313(5) of the Telecommunications Act 1997)."[115]

This seems like a reasonable request given that telecommunications carriers are being asked to actively monitor and remedy insecure computers, and thus may be seem to be making content determinations. There have been a number of vexatious civil actions taken against security software vendors for blacklisting websites which are considered below.

Anti-spyware, anti-virus and anti-spam organisations have found themselves exposed to legal challenges. 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

---

[114] An 'internet content host" is defined under the *Broadcasting Services Act 1992* as a person who hosts or proposes to host internet content in Australia. ICHs would include bulletin board hosts, blogs, email companies and so forth. They are contrasted with ISPs who are defined under clause 8 of Schedule 5 as "a person who supplies or proposes to supply an internet carriage service to the public."

[115] Telstra submission to the Senate Inquiry on Cybercrime (2010), page 5.

issued a default judgment.[116] 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, 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'.[117] A series of cases of a similar nature have been filed and heard between 2005 and 2009, with most settling.[118]

The notion of "good faith" or its equivalent will be imperative to ensure that ISPs do not abuse this power. The Canadian case of Telus is a good example. Telus, a major telecommunications carrier, was in a labour dispute with its employees where there was a lengthy strike. Telus blocked a pro-union website during the strike.[119] There are also instances where large security vendors blacklist websites that point out vulnerabilities of their products by categorising such sites as "pornography". These websites, that have nothing to do with pornography, are then blocked from those users who use the vendor's products. The vendor's filtering products might also be used at the ISP level or on the backbone of a nation with a heavy filtering mandate.

7.11 IMPLICATIONS OF ISPS PERFORMING LAW ENFORCEMENT FUNCTIONS

When ISPs detect and monitor data traffic, whether it be for "network protection duties" or obligations to comply with law enforcement, a wide range of information may be collected. As

---

[116] 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.
[117] Messmer, E. "Symantec vs. Hotbar: Who Won?" (January 3, 2006) available at http://www.networkworld.com/weblogs/security/011312.html
[118] 1-800 Contacts v WhenU., 1-800 Solutions v. Zone Labs, Cassav (CasinoOnNet) v Sunbelt Software, Glaria (Gator) v Internet Advertising Bureau.
[119] Geist, M. "Telus Blocks Subscriber Access to Union Website" (July 4, 2005) available at http://www.michaelgeist.ca/index.php?option=com_content&task=view&id=904&Itemid=85&nsub (last accessed at January 30, 2010).

one expert comments, "Digital traffic might reveal intimate details of the lifestyle and personal choices of an individual, and intimate relations or political or religious opinions."[120]

There is no international consensus on the definition of "traffic data". The *Cybercrime Convention* defines the term as:

> **"'traffic data' means any computer data relating to a communication by means of** computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."[121]

Conversely "traffic data" is not defined in Australian legislation. An ISP may collect and store data related to "network protection duties." As seen in **section 7.5.3** passive monitoring techniques are sufficient to retrieve information relevant for bot remediation and network protection purposes. Collection of information, nonetheless, has privacy, and freedom of expression and association issues. Privacy issues were explored in **section 7.5**. Freedom of expression, association and freedom issues are explored below.

The monitoring of Internet traffic may have freedom of expression and freedom of association ramifications for Australian users.[122] Australians' rights to access internet content and freely engage in online discussions are based less in law than in the shared understanding of a fair and free society. Legal protection for free speech is limited to the constitutionally implied freedom of political communication, which only extends to the limited context of political discourse during an election.[123] The full range of human rights in Australia, unlike in other developed democratic nations, are not protected by a bill of rights or similar legislative instrument, though the country is a signatory to the *International Covenant on Civil and Political Rights.* Nonetheless, Australians benefit greatly from a culture of freedom of expression and freedom of information.

Law enforcement agencies may search and seize computers, and compel an ISP to intercept and store data from those suspected of committing a crime. Such actions require a lawful warrant.

---

[120] Young, J., "Surfing While Musium: 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, page 348.

[121] Article 1(d)

[122] This section borrows heavily from Maurushat, A. "Freedom House Report on Internet Freedom: Australia" (2011). The report will be released in 2011 on http://freedomhouse.org. A copy of the report is on file with the author.

[123] *Catch the Fire Ministries Inc v Islamic Cuncil of Victoria Inc* [2006] VSCA 284; *Lange v ABC* (1997) 189 CLR 520; *Michael Brown v Members of the Classification Review Board of the Office of Film and Literature* [1998] FCA 319; *NSW Council for Civil Liberties Inc. v Classification Review Board* (No. 2) [2007] FCA 896; and *Theophanous v Herald & Weekly Times Ltd.* (1994) 182 CLR 104.

The collection and monitoring of the content of a communication falls within the purview of the *Telecommunications (Interception and Access) Act 1979 (TIAA*). Call-charge records, however, are regulated by the *Telecommunications Act 1997* (TA).[124] It is prohibited for ISPs and similar entities, acting on their own, to monitor and disclose the content of communications without the customer's consent.[125] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.[126] The TIAA and TA expressly authorize a range of disclosures, including to specified law enforcement and revenue-protection (tax) agencies, all of which require a warrant.

ISPs are currently able to monitor their networks without a warrant for "network protection duties," such as curtailing malicious software and spam.[127] Australia has announced plans to accede to the *Convention on Cybercrime*.[128] Unlike many other countries that have already ratified the convention such as the United States, Australia is expected to go beyond the treaty's terms in calling for greater monitoring of all internet communications by ISPs. Under the convention, an ISP is only required to monitor, intercept, and retain data when presented with a warrant, and only in conjunction with an active and ongoing criminal investigation.

A document leaked in June 2010 from the Attorney General's Department describes a range of possible policy options under which Australian ISPs would be required to monitor, collect, and store information pertaining to all users' communications. This would be done without a warrant and enforced against all users regardless of whether there is a criminal investigation.[129] The bot remediation program arguably satisfies the first component of the AGs project in that ISPs are already monitoring their networks without warrants. Where the proposal significantly differs, however, is that ISPS are not necessarily retaining and storing their data logs for long periods of time. This compulsory data-retention policy, if enacted, could become a significant threat to online freedom in Australia. The document is not official policy in Australia nor has it evolved

---

[124] *Telecommunications Act 1997*, Part 13, http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/, accessed June 2010.
[125] Part 2-1, section 7, of the Telecommunications (Interception and Access) Act 1979 (TIAA) prohibits disclosure of an interception or communications, and Part 3-1, section 108, of the TIAA prohibits access to stored communications. See http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/, accessed June 2010.
[126] Criminal offenses are outlined in Part 2-9 of the *TIAA,* while civil remedies are outlined in Part 2-10.
[127] Maurushat, A. "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Obfuscation Crime Tools?" (2010) University of New South Wales Law Journal 16, no. 1.
[128] Convention on Cybercrime, Council of Europe, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG, accessed June 2010.
[129] Asher Moses, "Web Snooping Policy Shrouded in Secrecy," *The Age*, June 17, 2010, http://www.theage.com.au/technology/technology-news/web-snooping-policy-shrouded-in-secrecy-20100617-yi1u.html.

to a concrete proposal or bill. It is unknown, therefore, whether data retention will be realised in Australia.

Freedom of association is likewise not a fully guaranteed right in Australia.[130] The *Anti-Terrorism Act 2005 (Cth)* revived laws against sedition and unlawful association. The unlawful association provisions have been used widely since their enactment with the banning of several organizations perceived to be potentially dangerous.[131] The sedition provisions, however, have not been used. Further, insults against government institutions or officials would not fall within the sedition provisions.[132] Increasingly, intelligence gathering of suspected terrorist groups is performed through surveillance of communication channels. This naturally includes Internet and mobile phone communications. Freedom of expression, as previously seen, is restricted to political communications. Freedom of association is also restricted to situations where people gather to express political communication or to picket in a labour dispute. The reality is that information is collected about suspected terrorists, often assumed to be Muslim, through communications channels. Where communications reveal the potential of further terrorist campaigns and provoke terrorist acts, these types of groups or associations can be prohibited to associate.[133] The grounds for unlawful association when connected to national security do not fall within the purview of anti-discrimination law in Australia on the grounds of freedom of religion.[134]

One of the greatest problems with the transference (whether intentional or unintentional) of law enforcement functions to private entities is the loss of safeguards and transparency. The transfer of functions to ISPs (as discussed in this chapter), security corporations, university researchers and self-organised security communities (as will be discussed in **Chapter 8)**, involves minimal safeguards to civil liberties. In the case of ISPs, the situation is more acute in Australia than in other nations such as Canada and France with strong human rights instruments embodied in law. The ability of an Australian to challenge data preservation, a production order or similar communications surveillance is limited in Australia to properly obtained warrants and privacy laws. This is compounded if one considers the potential for lack of transparency in the process. Programs should be reviewed annually, and both ISPs and law enforcement should provide accurate statistics to the public.

---

130 *See Mulholland v Australian Electoral Commission* (2004) 220 CLR 181
131 Andrew Lynch and George Williams, *What Price Security?* (UNSW Press, 2006) pages 41 to 59.
132 Above.
133 Blackshield and Williams, *Australian Constitutional Law and Theory* 4th ed (Federation Press, 2008) 4th, pages1376-1381.
134 *Adelaide Company of Jehova Witnesses Inc. v Commonwealth* [1943] HCA 12.

7.12 THEORETICAL FRAMEWORK

Architecture according to Lessig if invisible and self-executing. We are not physically able to see proxy servers, time-to-live speeds for DNS rotation, bots, botnets and other technological components. Computer programs are written which allow the botnet to self-replicate, perform functions and continue to propagate even once a botnet master is no longer "behind the wheel". In this respect, botnets are like the serpent whose head once removed simply grows another head. The question becomes how do we regain control of the architecture of the Internet from organised cybercrime groups? One possible solution is to indirectly regulate the architecture through soft law. In Australia, the IIA has implemented an self-industry code designed to remove compromised computers from the hands of botnet masters. While there are no statistics yet to suggest if this approach will work, this approach at least envisions regaining control of the architecture. Imperfect as the approach is, in particular, on the impact to civil liberties, it is possible that, at least in Australia, the architecture of individual machines connected to the Internet will no longer be in control of the cyber underworld but, rather, in the control of the ISP. It remains to be seen how users will respond to this gentle and perhaps invisible "grab" to strip control from the underground economy and the user.

7.13 CONCLUDING REMARKS

Entities that enable malware and botnet actors are a critical component to cyber security. This chapter has looked at the role of ISPs as a connectivity enabler. The Australian proposal for ISPs to detect and monitor their networks for bots, take action to prevent bots from causing damage, and educating users to remedy their computers has been examined. Bot remediation programs are imperative in cleaning up infected machines. As seen in the takedown of the Waledac botnet in **Chapter 3**, blocking the instructions to a botnet does not remove the very real and significant problem that compromised machines remain infected, and therefore, ready to be taken over by another botnet herder or ready to receive instructions in a different manner such as through peer to peer or through Google search queries. Disinfecting bots is an imperative element of any long-term solution to botnets.

The recommendations put forth by Comcast are well thought out and should be considered further by the IIA. Comcast argues that detection and monitoring technologies be restricted to small and medium packet inspection – that which is already being used, and that such technologies not be used for surveillance of individuals unless in lawful cooperation with a

criminal investigation. Detection and monitoring methods should adhere to several principles. Privacy principles and protection of personal information should be maintained. Passive monitoring methods should be use as opposed to pervasive methods such as deep packet inspection. Methods should be non-disruptive and should not block legitimate traffic. Multiple Point Bot Detection data points should be used to minimize false-positive identification of computers. ISPs should err on the side of caution when a likely bot infection has taken place, and should notify a customer even in the event of a benign or dormant botnet. Time-sensitive detection methods are imperative.

ISPs should not be expected to shift their role to an active filter or intermediary without liability exemption. As seen in the 2010 amendments to the *Telecommunications (Interception and Access) Act,* Australian ISPs may legally perform content inspection in connection with network protection. This ability to perform content inspection does not equate to an exemption from liability where a customer has been wrongfully disconnected. Any liability exemption should, however, contain a good faith clause so that ISPs do not use their position in an abusive manner.

Finally, it is recommended that the proposed e-Security Code be reviewed after a year of implementation and periodically every three years after that and that such a review should be a public report. This review should outline the Code's objectives, unforseen impacts, and should produce statistics where outcomes are measures against objectives. Such a review should include statistics on what portion of computers were detected as compromised? What portion of detected computers were remedied after ISP notified the customer? Rates of recidivism should be detailed along with recommendations to improve the process. Reviews of the program will additionally allow ISPs to constantly improve bot remediation.

This chapter has highlighted the new role that ISPs are taking to perform bot remediation programs. The next chapter highlights a more experienced approach to combating botnets, the work of self-organised security activists. It will be seen that self-organised security activists will need to work with ISPs and law enforcement to more effectively combat botnets.

Chapter 8

SELF-ORGANISED SECURITY COMMUNITIES

Table of Contents

8.0 AIMS OF CHAPTER

Botnet countermeasures may be taken by ISPs, DNS registrars, domestic law enforcement as well as international collaborative law enforcement initiatives, and by end-users typically in the form of using security products such as anti-virus software, firewalls and learning safer online habits. **Chapter 3** explored countermeasures taken against Torpig, Mebroot, Waledac and Mariposa botnets where university security researchers played a key role. The role, however, of self-organised security communities (SOSC) has not been explored within the larger body of technical and legal literature.[1] The primary aim of this chapter is to provide an account of the functions and activities of SOSCs in their efforts to counter botnets.

The term "self-organized security communities" takes into account the wide range of non-state parties active in the field of policing the Internet. By way of illustration, when the Miami Superbowl website was hit with a denial of service attack, the IT team contacted some well-known computer security experts within the SANS Institute to help them determine the source of the attack. This group of individuals was able to determine the source of the attack, and locate the DNS of the botmaster originating in China. The group was able to contact a member of CINIC who was able to shut the botmaster down by placing the DNS into a sinkhole (sinkholes were explained in **Chapter 3**). Law enforcement agencies were an "after fact" in the matter. The role which SOSCs play in Internet security is not well documented. Such self-organised groups and individuals include a sliding scale of players ranging from professional security activists to vigilantes to hybrid communities comprised of members of corporations, security experts, researchers and law enforcement. A small sample of these groups include: Artists Against 419, datawales, CAT, kier, PhishTank, APWG, VANK, Castle Cops, ZERT, 29A Hack Group, Perverted Justice, Shadowserver, Kitten crushers, Team Cymru, spamhaus, stopbadware.org, JIDF, Dr. Rusty, ISOTF.org and Global Watchlist.

[1] There are a few notable exceptions. *See* Chandler, J. "Technological Self-Help and Equality in Cyberspace" (2010) 55 McGill Law Journal. This article looks at the the particular role that self-organised communities play on the Internet though the emphasis is not on security communities. Other researchers have noted legal issues, such as the role of liability for self-help remedies, but do not explore in any detail some of the popular techniques of a honeynet which are used by security researchers. *See* Walden, I. And Flanagan, A. "Honeypots: A Sticky Legal Landscape?" 29 Rutgers Communications and Technology Law 315 (2003). See also Scottberg, B., Yurick, W. And Doss, D. "Internet Honeypots: Protection or Entrapment"Internet Symposium on Technology and Society (2002) available at www.ieeexplore.ieee.org/xpls/abs_all.jsp?arnuber=1013842&tag=1 (last accessed November 6, 2010).

8.1 BOTNET COUNTERMEASURES

In this chapter botnet countermeasures are revisited and are followed by an analysis of countermeasure activities of self-organised security communities. The remainder of the chapter is devoted to larger ethical and legal issues which apply to a broad range of self-organised communities. Examples of such issues includes whether governments grant immunity from liability to selected parties for damages caused by unauthorised access to personal computers and networks; whether there is a role for ethics (Eg. Code of Ethical Security Activism) given the uncertainty of the law; and what is the appropriate response to activism which causes collateral damage? In doing so, this chapter describes and documents the activities of three broadly classified groups: self-organised security communities, university researchers and botnet working groups. A SOSC is a not-for-profit organisation comprised of volunteers who perform countermeasures against cybercrime. I have drawn on the example of three groups and one individual for self-organised security communities whose work is directly relevant to combating botnets. These groups are Shadowserver and Spamhaus, a small independent research community known as Offense-in-Depth Initiative, and an individual who shall remain anonymous. University researchers are considered as a separate category in spite of the fact that many graduate students and professors are actively involved with SOSCs. The University of Southern California's efforts to gain information on the Torpig and Mebroot botnets will be examined, along with The Honeynet Project. The last category is botnet working groups. These working groups are comprised of major computer corporations, such as Microsoft, who work in conjunction with university researchers and SOSCs. I will not specifically examine any larger botnet working group operations because the Mariposa, Waledac, Torpig and Mega-D botnet countermeasure efforts have already been examined in detail in **Chapter 3**. The point is to highlight that there is a sliding scale of types of groups active in combating botnets. The categorisation provided is artificial in that members of SOSCs, university researchers and botnet working groups often overlap. The differentiation is provided for the purpose of exploring the essential workings of individuals and groups that do not easily fall within Lessig's four modalities. Lessig's four modalities are considered in greater detail at the end of this chapter and in the concluding chapter.

There are a number of terms which may be applicable to self-organised activist groups. These are explained below to better situate the later analysis that will ensue when addressing specific botnet counter measures.

"Hacktivism""is the use of computer hacking techniques such as virus or worm for some form of political protest. For example, types of political protests in this context involve information retrieval of documents which hackers believe should be 'free' and denial of service attacks of websites of organizations engaged in unethical activity (Eg. virtual blockage/political sit-in).[2]

"Cyber-Activism" is an intentional action which promotes change, normally in a social or political context.[3] It differs from hacktivism in the sense that hacking techniques are not necessarily utilised. Activism could involve cyber patrollers who search for online crime and security exploits, or merely those who publish information for a cause on a website.

"Self-Defense" is associated with an individual defending one's self from attack or defense of property.[4] In an online environment this might, for instance, involve an individual or corporation defending itself from a denial of service attack or from an attempt by an outside party to steal privately held corporate information.

"Vigilantism" tends to be used loosely. A more robust definition of 'vigilantism' requires a set of features: "1) planning and premeditation, 2) performed voluntary by private citizens, 3) is a form of 'autonomous citizenship' similar to a social movement, 4) it uses force or threatens the use of force, 5) occurs when an established order is under threat from transgression, and 6) offers a higher level of 'security' such as crime control".[5] A less robust version would describe vigilante activities as "taking the law into one's hands."[6]

'Information Warfare" (IW) is a highly contentious term. The only consensus in the literature is that writers disagree on the boundaries of information warfare. For the purpose of this paper

---

[2] Taylor, P., " Hacktivism: In Search of Lost Ethics?" in *Crime and the Internet* (London & New York: Routledge), page 63.
[3] The Oxford Pocket Dictionary of Current English (2009)
[4] Oleson, K. and Darley, J., "Community Perceptions of Allowable Counterforce in Self-Defense and Defense of Property"(1999) Law and Human Behavior, 23, pages 629-651.
[5] Johnston, L., "What is Vigilantism?" (1996) British Journal of Criminology, vol. 26, No. 2, page 220. For Internet perspectives *see* de Villiers, M., "Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare" (2005) Northwestern Journal of Technology and Intellectual Property, Vol. 4, No. 1, pages 13-60.
[6] Both supervisors found these definitions of limited use at this stage of the thesis. They have deliberately been left in to make sure that readers are able to distinguish the difference between an activist and researcher as opposed to a vigilante: the latter performs no worthwhile role in countering botnets. I presented a paper at the ISOI conference held in Estonia entitled, "The Limits of 'Permitted Self-Help' in Internet Security and Intelligence" to a group of security experts and cyber-activists who spend countless hours voluntarily combating cybercrime. The ISOI group is comprised by leading security experts from corporations such as Microsoft, Arbour Networks, ICANN, various Certs, Shadowserver, SANS and former Chief Cybersecurity Advisors to Prime Ministers and Presidents of various western countries. This attentive audience grilled me for over an hour on characterisation of vigilantes, activities, self-defense and information warfare. For this reason, I feel the strong need to provide defiinitions, lest the actions of these communities be wrongly categorised.

IW refers to actions taken to affect an adversary's information infrastructure while defending one's own information infrastructure. IW involves traditional military operations such as 'command and control warfare' but may include, depending on the definition adopted, attacks to critical infrastructure such as hospitals, banking facilities, stock markets, electrical grids and airports.

None of the above terms, however, adequately describe the specific activities of many self-organised communities. In most cases, as will be explored in the following sections, self-organised communities perform functions traditionally associated with law enforcement activities. Unlike traditional vigilantism though, many activities performed by self-organised communities cooperate with and contribute to police investigations. The categorisation structure of botnet countermeasures from **Chapter 3** will be used to describe the actions of self-organised security communities.

Chapter 3 canvassed different types of botnet countermeasure which included: Prevention and Detection, Intelligence Gathering, Disruption, Counter-Attack and Take-down Mechanisms. Self-organised communities, depending on their size, structure and goals may perform one or all of the above functions. A brief re-examination of these categories is now provided below.

8.1.1 Prevention and Detection

Prevention and detection refers to a wide range of activities. This could mean the implementation of methods to prevent a computer or network from becoming compromised as well as methods which prevent a botnet from performing damage to its target. Prevention and detection most commonly refer to the development and use of security software and hardware both to prevent malicious activity (Eg. firewalls, anti-virus) and to detect malicious activity. Prevention also refers to education efforts to inform users of safer computer usage. Some self-organised communities develop software programs. Most, however, are engaged in the information end of prevention by providing best practices, policy advice, and updates about botnets and malware.

8.1.2 Intelligence Gathering

Intelligence gathering refers to passively observing and recording information about a botnet. Intelligence gathering may be performed by observing traffic in the IRC, or in other protocols such as HTTP2P, and others. Specific observation techniques of IRC and P2P traffic was explored in **Chapter 3** where it was noted that much intelligence gathering is performed using honeynets. Honeynets are explored below in **section 8.3.4** below.

8.1.3 Disruption

Disruption is referred to in two senses. The first is in a technical sense while the second is more general. Disruption of botnet activities may be seen as a technical effort to subvert a botnet, or mitigate any harm and damage caused by a botnet. An example of subversion would be to infiltrate the botnet and redirect traffic from the C&C to a sinkhole. Other technical measures may involve efforts to stop the spread of the propagation method (often a worm). In a more general sense, disruption may refer to any effort to curtail the botnet. This may mean legal efforts pursued against botnet masters or spammers who contract botnet services. It may also involve attempts to make a botnet less profitable by injecting or removing compromised computers from a botnet, rendering it less effective. Disruption may also coincide with counter-attacks and detection measures. An organisation may launch a denial of service attack to known C&C servers where they are located on domain name pages. An organisation may also deploy a honeynet which not only detects attackers but may also run programs that implement protective security strategies upon attack.

8.1.4 Counter-Attack

Counter-attack involves engaging the botnet master in a form of hacking attack. This may include attempts to program and re-program bots issued from the C&C server, altering payloads of malicious applications delivered on botnets, and more often than not, launching a denial of service attack on C&C servers.[7]

[7] See Smith, B., "Hacking, Poaching and Counterattacking: Digital Counterstrikes and the Contours of Self-Help" (2005) 1 Journal of Law, Economics and Policy 185.

8.1.5 Take-Down Methods

The expression "take-down of a botnet" is a misnomer. As previously outlined in **Chapter 3**, a botnet cannot be completely taken down unless all points of the C&C servers are shut down in a near simultaneous fashion (so as not to allow the botnet master a chance to regroup) and all compromised computers connected to the botnet are remedied. Ideally, a take-down would also include the arrest and prosecution of the botnet master. The term "take-down" for our purposes is limited to taking down the C&C servers and pro-actively cleansing compromised machines.

8.2 SECURITY ORGANISATIONS

8.2.1 Self-Organised Security Communities

There are many such active communities that are relevant to botnets. The following communities have been selected as they are the primary organisations involved in botnet countermeasures and there is available information about such groups to analyse. Specifically, the operations of Shadowserver, Spamhaus, OID Initiative, and anonymous independent spamhunter will be reviewed as these organisations are most tied to botnet countermeasures. There are many other SOSCs active in the area such as the Anti-Phishing Working Group (APWG)[8], the SysAdmin, Audit, Network, Security Institute (SANS Institute)[9], Zeroday

[8] *See* http://www.antiphishing.org. According to the website the APWG is:

> "The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The organization provides a forum to discuss phishing issues and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks."

[9] See http://www.sans.org. According to the website:

> "SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.
>
> The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they

Emergency Response Team (ZERT)[10], and the Messaging Anti-Abuse Working Group (MAAWG).[11] These groups and the many others will not be included in the analysis because their work does not directly target botnets in the same way as the selected sample organisations.

8.2.1.1 Shadowserver

Shadowserver is a non-profit organisation comprised of security professions who volunteer their time to gather intelligence on botnet activity, malware and electronic fraud. Shadowserver is one of the most highly reputed self-organised communities in the botnet area as evidenced by both the volume and diversity of entities (independent researchers, security companies, law

---

face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

Many of the valuable SANS resources are free to all who ask. They include the very popular Internet Storm Center (the Internet's early warning system), the weekly news digest (NewsBites), the weekly vulnerability digest (@RISK), and more than 1,200 award-winning, original information security research papers."

[10] *See http://www.isotf.org/zert/. According to ZERT's website their manifesto involves providing security patches for zeroday exploits. Their manifesto is reproduced below:*

"ZERT is a group of engineers with extensive experience in reverse engineering software, firmware and hardware coupled with liaisons from industry, community and incident response groups. While ZERT works with several Internet security operations and has liaisons to anti-virus and network operations communities, ZERT is not affiliated with a particular vendor.

ZERT members work together as a team to release a non-vendor patch when a so-called "0day" (zero-day) exploit appears in the open which poses a serious risk to the public, to the infrastructure of the Internet or both. The purpose of ZERT is not to "crack" products, but rather to "uncrack" them by averting security vulnerabilities in them before they can be widely exploited.

It is always a good idea to wait for a vendor-supplied patch and apply it as soon as possible, but there will be times when an ad-hoc group such as ours can release a working patch before a vendor can release their solution."

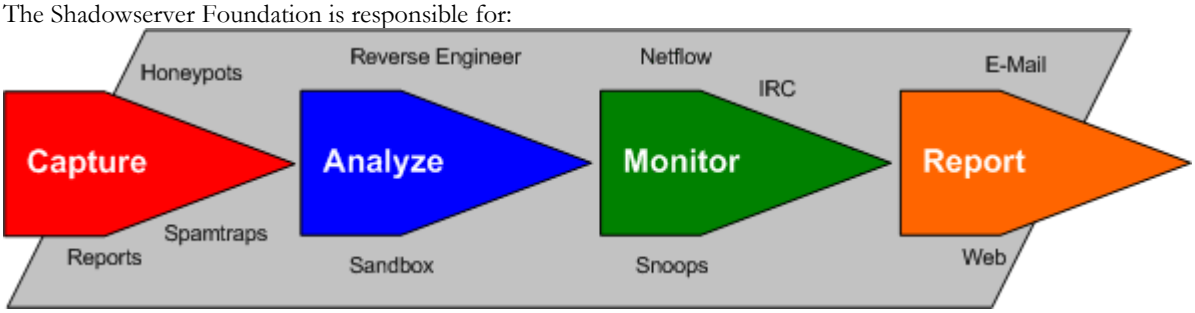
[11] See www.maawg.org. The organisation describes themselves on their website as:

"MAAWG is driven by market needs and the insight of its global membership. With member companies from Asia, Europe, North America and South America, the organization currently is working on a variety of initiatives addressing ongoing and emerging messaging abuse issues, including bot mitigation, cooperative industry outreach, Web messaging abuse, DNS abuse, wireless messaging, senders issues and other topics.

MAAWG is the only organization that targets messaging abuse by simultaneously focusing on the varied facets of the international challenge. Our committees are organized around technology, industry collaboration, cooperative public policy efforts and special interest groups. Projects are accomplished within these groups and their associated subcommittees. MAAWG is a member of the London Action Plan (LAP) and an associate partner of the StopSpamAlliance, has liaison relationships with the IETF and other organizations, and often joins forces with public policies agencies and other anti-abuse organizations."

enforcement and Internet governing agencies) that make reference to statistics and general information from the organisation. The Mission Statement of this organisation is as follows[12]:

> "The Shadowserver Foundation is an all volunteer watchdog group of security professionals that gather, track, and report on malware, botnet activity, and electronic fraud. It is the mission of the Shadowserver Foundation to improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware.
>
> The Shadowserver Foundation is responsible for:



> - Capturing and receiving malicious software, or information related to compromised devices
> - Disassembling, sandboxing, and analyzing viruses and trojans
> - Monitoring and reporting on malicious attackers
> - Tracking and reporting on botnet activities
> - Disseminating cyber threat information
> - Coordinating incident response"

The organisation's activities are best categorised as prevention, intelligence gathering, interdiction and harm mitigation as they do not engage in any form of counter-attack. Specifically, they do not take-over of the botnet's command and control by altering payloads, or perform any type of activity associated with hacking or hacking back at a botnet master. They perform prevention in the form of information dissemination and education. Likewise, the extent of their activities as interdiction is also limited. They are active in disrupting botnets by providing a sinkhole for other groups engaged in botnet takedown. For example, Shadowserver provided the Domain Name Service sinkhole (DNS) for the takedown of Mega-D botnet by FireEye, a security software company.[13]

The Mega-D botnet utilised several different types of command and controls. The primary C&C used a set of domain names. In the event that the primary C&C became impaired, there were fallback C&C mechanisms where a different string of domain names were used to communicate instructions. The FireEye researchers were able to ascertain which domain names would be used as a fallback mechanism for the C&C. As the fallback C&Cs domain names had not yet been registered, FireEye was able to register the names and then had the domains point to the

[12] Shadowserver website available at http://www.shadowserver.org (last accessed October 31, 2010).
[13] Lin, P. "Anatomy of the Mega-D Takedown" (Dec. 2009) Network Security, pages 4-7.

Shadowserver DNS sinkhole.[14] Once the main C&Cs were disabled, the fallback C&Cs became inoperative. All traffic that used any of the fallback names was directly to the Shadowserver sinkhole. The traffic, therefore, directed to the domain names used for C&C was redirected into the DNS sinkhole rendering the botnet incapable of connecting to the real domain name and receiving its instructions.

The predominant function of Shadowserver is one of intelligence gathering and harm mitigation. The organisation utilises honeypots to gather and collect information about different botnets and malware. Such information may include size of botnet, proliferation rate, location of command and control, IP addresses or domain names utilised by command and control, as well as IP addresses of individual infected machines. This information is analysed and then the botnet is studied and tracked. According to their standards and guidelines:

> "As part of the botnet research process, detailed information about the botnet is gathered and studied. After this information has been assembled, a command and control point is tested by simply emulating the malware that is already connecting to the system. This is done via a method that will not allow the Shadowserver's testing or monitoring system to participate or act as a drone of the botnet. At no time is there any attempt to exceed any authority levels or to cause any harm to the subject system.
>
> During any testing phase, no member of the Shadowserver team will engage or establish a dialogue in a taunting or challenging manner with the bot herder or any other of the botnet. In fact, any direct communication on a C&C server between a Shadowserver team member and the bot operators is discouraged."[15]

The methods that Shadowserver utilises differ from other communities in that they do not allow their computers to become part of the botnet, nor are any authority levels exceeded. Authority levels in this context refers to authorisation whereby certain individuals or groups have permission or privilege to access or perform certain functions. Clarke describes the process as:

> **"Authorisation**. An (id)entity, once it has been (id)entified - i.e. an (id)entifier has been collected - and after (id)entity authentication has been performed, may be permitted to perform particular acts. The process whereby it is determined what a particular Entity or Identity is permitted to do is referred to as authorisation.
>
> A **permission** or **privilege** is a capability that an (id)entity is permitted to perform. In a physical context, the capability may be access to particular premises, or to particular parts of premises. In a virtual context, an identity is provided with access to system resources, and in particular authorised to run particular software, use particular functions performed by that software, access particular data collections and/or access particular data within those data collections."

Authorisation to access or use data may be limited to those performing certain tasks or restriction may be imposed by type of data. For instance, a doctor or nurse of a hospital would

[14] Lin, note 13 above, page 6.
[15] Shadowserver, note 10 above.

have access to sensitive personal health information whereas a janitor would not. Authorisation is determined in this context as by those performing medical tasks in the hospital. Similarly, the results of certain types of medical tests may be limited to doctors and not nurses based on the type of data contained in the test. Imagery of an MRI would not be useful to those not trained to view the medical images. The virtual context is similar. Only certain people within an organisation would be authorised to perform certain network functions or to access certain types of data. In the context of Shadowserver, authority levels indicate that the organisation does not access data and files (Eg. hacking) without authorisation. The legal implications of authorisation are explored in **section 8.3.2 Unauthorised Access, Modification or Impairment of Data.**

Shadowserver works in conjunction with many other corporations and organisations delivering some of the most up-to-date information about botnets as well as to track a botnet over its lifespan. In some instances a botnet may be operable, growing and causing damage for several years. The organisation reports in three distinct manners. First, they share information with partner organisations as threats develop. Second, they share information with the public in the form of statistics and information about threats from their website www.shadowserver.org. Third, where appropriate the organisation shares information with law enforcement agencies. For example, if intelligence allows for traceback to the source of a botnet operation, this information is forwarded to law enforcement.[16]

8.2.1.2 Spamhaus

The Spamhaus Project, referred to as Spamhaus, is an international non-profit organisation run by volunteers who gather intelligence on spam operations. The organisation works with a number of organisations including governments, corporations, internet service providers and security experts in the area of prevention and detection, and interdiction.

Spamhaus produces anti-spam protection for networks in the form of real-time blacklists which may be implemented by internet service providers, e-mail providers, governments and corporations. According to Spamhaus, there are 1.4 billion email accounts protected by Spamhaus realtime blocklists known as the Domain Name Server Blocklist (DNSBLs). These DNSLBs are comprised of several specialised lists which include the Spamhaus Block List (SBL),

[16] Perlotto, R. "Conficker" AusCERT Online Crime Symposium (2009). Presentation available online at https://www.auscert.org.au/download.html?f=318 (last accessed November 10, 2010).

the Exploits Block List (XBL), the Policy Block List (PBL) and the Domain Black List (DBL). These blacklists serve to as a prevention and detection function for blocking spam traffic.

These blacklists may additionally be seen as performing functions associated with interdiction in their ability to disrupt the spam economic model. As was examined in **Chapters 1 and 4** some adware companies have sued Spamhaus for their inclusion on a blocklist. Spamhaus provides information for law enforcement through tracking, and collecting evidence against the more well-known international spammers. The database is known as the Register of Known Spam Operations (ROKSO) and has been used to assist law enforcement agents in pursuing spam investigations.

Charges of fraud, money laundering and identity theft were successfully brought against known spammer Robert Alan Soloway after a joint investigation between the Washington State Attorney General's Office, the Federal Bureau of Investigation (FBI), the Federal Trade Commission (FTC), the Internal Revenue Service Department of Criminal Investigations (IRS-CI) and the United States Postal Inspection Service (USPIS).[17] Spamhaus claims to have documented Soloway's use of botnets to send out spam which contained malicious software. According to the ROKSO records Soloway hired blackhat hackers to create botnets specifically for his spam operations.[18] Review of the publicly accessible Spamhaus records, however, did not reveal any information about botnets or virus writers. While the media has reported Soloway's use of botnets, there is no publicly available information in civil trials against him claiming such use.[19] A copy of the plea bargain in the case reveals that Soloway confessed to charges of tax fraud, mail fraud, and fraud in connection with electronic mail.[20] There is no mention of the use of

---

[17] The court decision has not been published due to a plea bargain being reached. There are many media stories that discuss the charges. *See, for example*, MSNBC, "One of the World's Top 10 Spammers Held in Seattle" (May 5, 2007) available at http://www.msnbc.msn.com/id/18955115/ (last accessed October 26, 2010). See also, Carter, M., "Spam King Pleads Guilty to Felony Fraud" (March 15, 2008) The Seattle Times available at http://seattletimes.nwsource.com/html/localnews/2004283998_spamking15m.html (last accessed October 29, 2010).

[18] This information was obtained from the spamhaus website available at http://www.spamhaus.org/news.lasso?article=611 (last accessed October 19, 2010).

[19] *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).

[20] A copy of the plea bargain was posted to the internet by John Levine who, had the matter gone to trial, would have been called to testify as a technical expert in the matter. The plea bargain may be accessed at http://www.circleid.com/pdf/soloway-73.pdf (last accessed October 26, 2010).

botnets in the plea bargain. The volume of the spam sent coupled with the use of a technique designed to avoid spam filters[21] strongly suggests that botnets were utilised.[22]

Spamhaus does not disclose the organisation's methodologies for determination of who appears on the ROKSO database nor do they disclose methods of information gathering on spamming operations. This has led to the dismissal of subsequent spam suits that have relied on Spamhaus information. In the decision of *ASIS Internet Services v. Optin Global*[23] the court dismissed all claims and denied summary judgment against the defendent for alleged spamming operations in violation of the United States *CAN-SPAM Act*. The court specifically stated:

> "Although these assertions concerning the alleged relationship between Defendant and Bluerockdov have some force, Plaintiff offers no concrete evidence to support them. The only evidence that Plaintiff offers linking Azoogle and bluerockdove is that they are listed as "partners in spam" in SPAMHAUS ROKSO reports. Plaintiff does not, however, provide any information regarding the legitimacy of this organisation, how its reports were created, the time period that the reports cover, or the meaning of the 'Partners in spam' label."[24]

There is no transparency as to how Spamhaus generates information. My requests to Spamhaus for information gathering methodologies were not met with responses.[25] It does not appear that the organisation provides such information even when faced with a civil suit. The judge in the US decision of *e360 INSIGHT v The Spamhaus Project* also noted that Spamhaus' practices were not clear.[26] It remains unknown whether the information guarding is intentional. There are a number of good reasons why Spamhaus limits public knowledge of internal practices. Such reasons may include not wanting to give any advantage to spam and botnet operators, the desire to shield the organisation from law suits, and due to the uncertain criminal law territory of security research. **Chapters 4 and 6** discussed the lack of security research exemptions to "hacking" provisions as well as liability issues with honeynets and other research tools.

---

[21] *See, for example,* the work of Li Zhuang, John Dunagan, Daniel R. Simon, Helen J. Wang, J. D. Tygar, "Characterizing Botnets From Email Spam Records" Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (2008)

[22] The technique is one where the "to" and "from" fields are the same. So, for instance, an email promoting viagra may appear to be sent to and from the same account.

[23] *ASIS Internet Services v. Optin Global*, et al., United States District Court for the Northern district of California (2007) No. C-05-05124 JCS.

[24] *See* note 21 above, page 12.

[25] An email was sent to Spamhaus on October 26, 2010. The organisation acknowledged receipt of the email but have yet to send a reply.

[26] *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, page 2.

8.2.1.3 Small Independent Research Communities (Offense-in-Depth Initiative)

There exist a number of undocumented small independent research communities that are actively involved with botnet harm mitigation, interdiction, counter-attack and take-down. 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.[27] 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.[28]

The group's aim is to form small working groups singling out one botnet or criminal operation with the purpose of long-term disruption. 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."[29] OID's focus is 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.[30] 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.[31] 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

---

[27] Observations from email orrespondance with members of the OID Initiative. Emails on file with the author and are included in Appendix A.
[28] One commentator within the group noted that he wasn't even sure what some of these terms event meant. For instance, what is an information warrior? Observations from listserve correspondance. Correspondence is found in Appendix A.
[29] ISOI is one such group. Members complained of the unfocused, ad hoc short-term approach of ISOI.
[30] Observations from founder of OID in listserve correspondance. Correspondence found in **Appendix C**.
[31] *See* Li, Z., Liao, Q., and Striegel, A., *Botnet Economics: Uncertainty Matters* (Springer 2009).

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.

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.[32] 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.[33]

---

[32] Observations from listserve correspondance found in **Appendix C**.

[33] *See generally* 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). Internal correspondence within the OID-Kraken group on Friday, December 2008 where it was noted that, "if you're wondering why this botnet is off-the-air at the moment or why you've stopped seeing fake Gucci spam in the past 24 hours, it was us (with assistance from Spamhaus)." Correspondence found in **Appendix C.**

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."[34] In a similar fashion to the Torpig and Mega-D countermeasures as seen in **Chapter 3**, the groups registered future domain names that the C&C would migrate to. 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.[35]

The methods used by TippingPoint are not novel, as seen in the instances of the Waledac, Mariposa, Torpig and Mega-D botnet countermeasures. Unlike in these instances, 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 for ethical and legal reasons cleaned up the botnet. The ethical and legal issues of botnet cleansing through what is known as "pro cleansing", "good worms" and "pro-active patching" are discussed in **section 8.3.**

8.2.1.4 Independent Robert Soloway Spamhunter

There exist a number of botnet hunters and spam hunters who operate individually to post information about botnets, and to actively perform counter-attacks against botnets. They are described here as vigilantes for two reasons. First, these hunters go beyond mere collection of evidence relevant to gathering information about a botnet or spamming operation. Second, they gather information that would well be considered as distinctly private and seemingly unnecessary for any use relevant to spam or botnet operations. One such independent vigilante is an anonymous Swedish spamhunter who has produced 360 webpages of information against the

[34] *See* TippingPoint, note 38 above, comment 25.
[35] Above.

spammer and botnet user Robert Soloway. In addition to providing links to Spamhaus directories, YouTube videos of victims, copies of restricted civil court decisions and detailed technical information about Soloway's spamming activities, the author makes it known that he was one of Soloway's victims. Additionally, the website posts information about Soloway's sexual activities as a gay man, displays photographs of the interior of his home, provides tracking maps, as well as detailed information about members of his family who are not involved in Soloway's activities.[36] Such activity extends beyond useful information gathering and into the realm of revenge and vindication and possibly in breach of United States privacy laws. US privacy laws are contained in a myriad of statutes at the federal and state level.[37] Most statutes deal with privacy in the context of consumer transactions, and information held by government agencies. Disputes between private citizens may be settled under civil privacy actions of intrusion. It is questionable whether the information collected by the vigilante is public and if not, whether it is actionable. If there has been no harassment of Soloway in the real world and the information is non-private and then used to shame him, the tort of privacy intrusion will not allow for redress.[38] The photographs of the interior of Soloway's home may well be private but this depends on how the photographs were taken. For instance, if the home had been for sale and there were photos available on the Internet this would likely not cross the line of privacy intrusion. By contrast, if the photos were taken by a vigilante trespassing onto Soloways's property and taking photos through the windows then there is a much higher chance of privacy invasion. Publication of truthful and accurate information is not actionable in the United States. The test of privacy invasion is whether the situation would be highly offensive to a reasonable person and is not newsworthy.[39]

---

[36] *See* Anonymous, website of information on Rob Soloway available at http://4431647708582819520-a-1802744773732722657-s-sites.googlegroups.com/site/sjwest01/broadcastspam.html?attachauth=ANoY7cpmIg82OvP9mKMCxMq5HfmzDusdBYThE248ncZYvEPYhELM5CzkoCUdS50ml0WRSY7V6GL0MqYFJoTyOjg-FK3sXmaOmMlIfWVEgPlqtrFFrxTGaoBBgxo_GXISt9Q3MmmKjMxKEY3L4SDpCjR1OCehGzHuPNBwadjQGDheH8bXsG65sEES1VqfZTyQQCaALzaYMROi&attredirects=0#31052007 (last accessed October 25, 2010).

[37] Daniel Solove describes the US privacy situation as:

> "Privacy law consists of a mosaic of various types of law: tort law, constitutional law, federal and state statutory law, evidentiary privileges, property law, and contract law. Privacy law is best described with the notion of the *bricoleur*—a person who uses whatever is at hand as a tool to solve problems."

Solove, D. "Privacy and Power: Computer Databases and Metaphors for Information Privacy", (2001)53 Stanford Law Review 1393, page 1430

[38] See *Nader v. General Motors Corp*., (1970) 255 New York 2nd Division 765

[39] The RESTATEMENT § 652D, provides:

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

(a) would be highly offensive to a reasonable person, and

In a similar vein, there are individuals who enjoy locating command and controls, infiltrating such controls, changing instructions, and launching denial of service attacks on addresses they believe to be associated with a botnet master.[40] Such activity may be classified as counter-attacks.[41] This type of activity, however, is not reported in any public fashion owing to the fact that such types of countermeasures are not legal (as will be seen in **section 8.3.2 "Unauthorised Access, Modification or Impairment of Data**". This type of ad hoc loner hacker activity is likewise not encouraged in the wider security community, and certainly *not* within the groups specifically discussed in this chapter. This type of loner vigilante activity may take down the C&C of a botnet for a short period of time (Eg. the length that the vigilante is able to stay awake monitoring and changing the instructions of the C&C). Loner vigilante activity is an ineffective method of countering botnets.

8.2.2 University Researchers

University researchers provide invaluable contributions to extending to a full range of countermeasures which would include prevention and detection, harm mitigation, interdiction, information gathering, and take down. First, the role of university researchers is explored, drawing on the University of Southern California's involvement with the Torpig botnet. This recount will be non-exhaustive given that Torpig was previously considered in **Chapter 3.** Nonetheless, this example provides a clearer picture of university research involvement in the area. The second example looks at The Honeynet Project.

8.2.2.1 Torpig Botnet

Researchers at the University of Southern California infiltrated the Torpig botnet as was explored in detail in **Chapter 3.** In this instance, they established a honeynet, reverse engineered the encrypted bot code, registered the domain names where the C&C would eventually be located, handed relevant information over to law enforcement and then published this information in the form of an academic paper and video conference – both available to the public from the Internet. In this instance, the countermeasures taken mostly involved

---

(b) is not of legitimate concern to the public.

[40] ISOI 5, Estonia, 2008, Chathom House Rules applied. Some of those present in the room boldly asserted that they hacked, performed counter-attacks and taunted botnet herders and other types of cybercriminals on an individual basis from time to time as an exercise of fun.
[41] Open acknowledgement of one participant at ISOI5, Estonia. Chatham House Rules apply. Notes from the workshop on file with author.

intelligence gathering. No effort was made to take-down the C&C by subverting traffic to a sinkhole. The information gathered was handed over to the FBI who then handed over the information to the National Cyber-Forensics Training Alliance (NCFTA). The FBI and NCFTA contacted the ISPs and DNS providers who then removed the C&C sources from their servers. Thus they were able to shut down the primary C&C sources of the botnet. The botnet, however, was simply able to revert to a secondary C&C, which in this instance was a second botnet known as Mebroot. Mebroot received its C&C through the rootkit and used encrypted commands which no researcher at the time was able to break.[42] University researchers were also involved in the Waledac and Mariposa botnet takedowns as seen in **Chapter 3**.

8.2.2.2 The Honeynet Project

The Honeynet Project is an international non-profit research organisation with 26 chapters in 19 countries.[43] Most of the honeynet chapters are run by university researchers. The goal of the project is to improve the security of the Internet by: raising awareness of threats and vulnerabilities; providing information as to motives of an attack, communication structure, and actions once a system is compromised[44]; and providing other organisations interested in cyber threat research with access to the honeynet tools and techniques that the project develops.

Researchers often use honeynets to gather information about how malware or a botnet is being used. Honeynets provide some of the richest information on botnets, including locations of the control and command (C&C), mutation routes (Eg. C&C is located on webinex.com for two months then becomes webinex.biz then webinex.tv and so forth), commonly utilised ports, bots connected to the botnet, types of malicious activities (Eg. Trojans or denial of service), patterns of replication (Eg. how a worm is spreading), and potentially information about the botnet master. This information benefits security vendors by allowing them to develop better anti-virus and anti-spyware software. The information is equally valuable to corporations and organisations in providing information about vulnerabilities in their network. Internet service

---

[42] There are some security researchers who claim to have broken the Mebroot encryption but they do not provide a proof of concept. TrustDefender, an Australian corporation is one entity that provides a product which claims to detect and secure an organisation from Mebroot. It is unknown, however, if TrustDefender has been able to break the Mebroot encryption. *See* 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).

[43] See The Honeynet Project at http://old.honeynet.org/misc/project.html (last accessed November 12, 2010).

[44] This is done through a series of white papers knowing as the "Know Your Enemy" series available at http://old.honeynet.org/papers/index.html (last accessed November 12, 2010).

providers use the information to develop spam filters, to identify vulnerable points in their networks, to identify customers at risk and so forth (ISPs were examined in **Chapter 7**). A virtual honeynet may allow its operators to identify bots. This in turn presents the opportunity to notify the owners of compromised machines. Virtual honeynets, for the purpose of this chapter, may also present evidence which is later used in the prosecution of a botnet master. The research and intelligence gathering from the Honeynet Project has been an invaluable tool in aiding organisations to safeguard against security threats, including botnets.

8.2.3 Not-for-Profit Security Corporations

Not-for-profit security corporations have emerged to help combat cybercrime.[45] Of these corporations, the National Cyber-Forensics Training Alliance (NCFTA) is one of the most significant. The organisation plays the role of intermediary between public and private sectors to counter cybercrime. The NCFTA describes itself as a "High Tech Task Force" made up of experts from industry, academia and government. The organisation is run by Ron Plescoe, former employee of the Department of Homeland Security and Chair the Cyber Attacks Committee for the PA Homeland Security Council. The primary objectives of the NCFTA are to:

- "Identify, mitigate, and neutralize cyber crime threats
- Rapidly build intelligence to the actionable level so that the threat can be:
    - Further located/identified (who all are involved and where they are located)
    - Mitigated through timely enhancement of security practices/procedures
    - Effectively neutralized through:
        - Proactive law enforcement engagement (domestically & internationally) – This can/may include both criminal and civil avenues in coordination with appropriate authorities
        - Implementation of interim technology solutions (i.e. null-routing of botnet traffic or similar interdiction action via TLD's or ICANN)"[46]

The NCFTA has headquarters in Pittsburg at the University of Carnegie Melon and a smaller office located in the FBI's Internet Crime Complaint Centre in headquarters in Washington, DC.[47] In effect, the NCFTA operates as an intermediary between corporations and law

---

[45] Many not-for-profit as well as for-profit security corporations employ former prosecutors and police officers with experience in high tech crime. For example, Scott Charney, of Trustworthy Computing (a subsidiary of Microsoft) was formerly Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the U.S. Department of Justice. Yahoo and Google have employed Richard Selgado, former Senior Counsel at Computer Crime and Intellectual Property Section, U.S. Deparment of Justice. Ebay employed Alister McGibbon, former head of the Australian Federal Police High Tech Crime Division.

[46] *See* the NCFTA website available at http://www.ncfta.net/about-ncfta (last accessed March 3, 2011).

[47] Correspondance with Ron Plescoe (2009). Notes on file with author.

enforcement, though, most of its functions are related to triage of cyber-attacks on corporations, and industry focused security initiatives. When a corporation has been attacked and wishes to involve law enforcement, the *NCFTA* acts as the middle man between these two entities.

The NCFTA operates a Malware and Botnet Initiative, "to gather, correlate, analyze, and disseminate intelligence related to the attribution of cyber criminals who utilize malicious code as a tool in order to further various types of cyber crimes."[48] While university researchers, honeynet projects and other security corporations all perform similar functions such as gathering intelligence, the NCFTA's primary role is to distribute botnet information to its partners, and to help them to mitigate any attacks from botnets.

The NCFTA played a role in disseminating information on the Torpig botnet and in helping the FBI to shut down the C&C sources, if only temporarily.

The NCFTA has also played a significant role in the FBI sting of the black market credit card forum, DarkMarket.[49] The NCFTA coordinated a taskforce led by private sector corporations with the FBI to set up the forum, and trace intelligence, which led to the arrest of many members of the forum trading in credit card information.[50]

8.2.3.2 Team Cymru

According to their website, "Team Cymru Research NFP is a specialized Internet security research firm and 501(c)3 non-profit dedicated to making the Internet more secure. Team Cymru helps organizations identify and eradicate problems in their networks, providing insight that improves lives." Team Cymru employs computer security experts and former police officers from all over the world who have worked in high tech crime units.[51] Team Cymru was active in the gathering of intelligence of the DollarRevenue adware company in the Netherlands which led to the arrest of amateur botnet master, Owen Walker. Team Cymru also performs functions similar to Shadowserver by providing sinkholes for take downs of C&C sources. Team Cymru invite law enforcement agencies from around the globe to contact them if there is

[48] The National Cyber-Forensics Training Alliance website available at http://www.ncfta.net/ncfta-initiatives/malware-botnet (last accessed March 2, 2011).
[49] Poulsen, K., *Kingpin: The True Story of Max Butler, the Master Hacker who Ran a Billion Dollar Cyber Crime Network* (Hachett, 2011).
[50] Purdy, A. and Plescoe, R., "National Cyber-Forensics Training Alliance" (2009) AusCERT Security Conference. Notes on file with author.
[51] Team Cymru, "Confickr" (2009) AusCERT Security Conference. Notes on file with author.

an investigation where they require assistance.[52] This part of their operations is not transparent on their websites but is known among high tech crime units.

8.2.4 Botnet Working Groups

Countermeasures against botnets increasingly involve collaborated efforts between many security actors. Such actors, as will be seen below, include law enforcement, government agencies, large and small computer corporations, university researchers, domain name registrars, Internet service providers, and self-organised security communities. Examples of such botnet working groups are briefly revisited below as they were more fully canvassed in **Chapter 3 (Waledac, Mariposa and Mega-D Botnets).**

The Waledac Working Group was led by Microsoft but included Shadowserver, China CERT and university researchers[53] who actively worked to disrupt the command and control that operated in the peer-to-peer protocols. Microsoft was able obtain a court order forcing ICANN to remove the IP addresses of the primary command & controls. China CERT voluntarily removed the IP addresses.[54] In this instance, Waledac countermeasures included a large corporation, a self-organised security community, a government CERT, university researchers, the court and, to a lesser extent, domain name registrars.

The Mariposa Working Group was coordinated by researchers from universities, private corporations (Defence Intelligence, Georgia Tech Information Security Center, and Panda Labs Security), and the relevant DNS registrars and ISPs.[55] The take down of the Mariposa botnet

---

[52] Team Cymru presentations at AusCERT Security Conference (2007 and 2009). Closed sessions on cybercrime.
[53] University researchers were involved from the Vienna University of Technology, the University of Manheim, the University of Bonn and the University of Washington.
[54] According to the CNCERT website:

> **"CNCERT/CC** is a functional organization under Internet Emergency Response Coordination Office of Ministry of Information Industry of China, who is responsible for the coordination of activities among all Computer Emergency Response Teams within China concerning incidents in national public networks. It provides computer network security services and technology support in the handling of security incidents for national public networks, important national application systems and key organizations, involving detection, prediction, response and prevention. It collects, verifies, accumulates and publishes authoritative information on the Internet security issues. It is also responsible for the exchange of information, coordination of action with International Security Organizations."

Available at http://www.cert.org.cn/english_web/overview.htm (last accessed February 20, 2011)
[55] Quarterly Report PandaLabs (January-March 2010) available at http://www.pandasecurity.com/img/enc/Quarterly_Report_Pandalabs_Q1_2010.pdf (last accessed June 24, 2010).

was coordinated with international law enforcement in the United States and Spain as the identity of one of the botnet masters was known.

MWG found the DDP team had data belonging to over 800 000 users spread over 180 countries. In addition to installing adware for an affiliate fee, the Mariposa botnet was programmed to steal credit card information which was then sold to other criminals. The DDP team also stole directly from bank accounts. The money was laundered through online poker activities and by using money mules. It is estimated that fraud losses and damages are in the millions. Several counts of fraud charges were brought against the members of DDP. These botnet masters will not, however, be charged with any form of unauthorised access or modification of a computer as Spain, while signatory to the *Cybercrime Convention*, has yet to ratify. The *Cybercrime Convention* was considered in **Chapter 5**. As of the end of June the investigation of the DDP is ongoing and there have been claims that the botnet is still functioning.[56]

Countermeasures against the Mega-D botnet were mainly performed by the security corporation FireEye, although some were also taken by Spamhaus, Internet service providers and domain name registrars. This working party did not involve university researchers or law enforcement. In this case, FireEye was able to register the domain names ahead of the botnet master for the command and control which then allowed them to control the botnet traffic. In this case, traffic was redirected to the Spamhaus sinkhole.

The efforts of the botnet working groups has so far proven to be the most effective countermeasure against botnets as the botnet is rendered non-functioning. Most botnet working groups have involved security organisations, private corporations, law enforcement, Internet service providers and domain name service registrars. Coordinating these types of activities, however, is hugely time consuming and costly. Microsoft had to expend thousands of dollars in time, effort and money for legal fees for the removal of domain names in the Waledac botnet. Security organisations such as Spamhaus, Shadowserver and OID operate through volunteers. A formalised working structure with proper funding will be needed if botnet working groups are to be sustainable long-term. Additionally, botnet cleansing has predominantly not been used. This means that machines are still compromised and ready to be taken over by a new command and control. Bot remediation, as explored in **Chapter 7**, is essential to any effective countermeasure.

[56] 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).

8.3 ETHICS AND LEGAL ISSUES

The botnet situation has been described by one security expert as "a full blown case of AIDS and no one is making a cure."[57] Seen in this light, traditional responses to botnets through regulation, policy, and technologies could be seen as non-functional. Non-functionality could extend in a number of directions. It could include the inability of law enforcement agents to enforce and prosecute crimes associated with botnets. It could refer to the need to remove security research barriers. It could refer to a lack of adequate response from communications enablers and financial enablers. It could equally refer to the inadequacy of relying on end-users to use anti-virus software and to continually patch and update their anti-virus software. 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 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"[58] is potentially applicable to both botnet and anti-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.[59] 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.

---

[57] Comment made by MJ an anonymous commenter on the security blog operated by Tipping Point. The comment was made in relation to the Kraken botnet and is available at http://dvlabs.tippingpoint.com/blog/2008/04/28/kraken-botnet-infiltration (last accessed February 9, 2011).

[58] Tamanaha explores the term "to do justice" in Tamanaha, B. "Socio-Legal Positivism and a General Jurisprudence" (2001) Oxford Journal of Legal Studies, Vol. 21, No.1, p. 21. Under this theory, a legal system may consist of one single rule, "to do justice".

[59] The author does not make the assumption necessarily that regulation can ever effectively deal with malware. 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.

Some of the countermeasures used by self-organised security communities contain many ethical and legal issues. These are discussed below.

8.3.1 Pro-Active Cleansing

Pro-active cleansing is a term similar to pro-active patching, benevolent worms and benevolent payload. Pro-active cleansing or patching is the process whereby an organisation takes over the command and control of a botnet, then writes software code (bot) which essentially cleans the compromised computer. The process is similar to the ISP bot remediation programs in that compromised computers are remedied. It differs, however, in that with ISP bot remediation, the user is instructed how to clean their own machine with the aid of informative websites and the ISP. Pro-active cleansing of a botnet involves access and modifying the compromised computer without any authorisation. As seen in **section 8.2.1.3**, which explored the take-down of the Kraken botnet, the security firm TippingPoint had written a computer program which could automatically clean up compromised computers that were part of a botnet.[60] TippingPoint decided not to perform pro-active patching of the Kraken computers due to legal liability issues and possibility of criminal sanction.

The idea of pro-active cleansing is similar to earlier notions of benevolent virus, worms and payloads. A benevolent worm is a form of malware. Malware refers to computer software which either acts maliciously or whose effects are malicious – the two are not necessarily synonymous. In a wider context, malicious would extend to any type of computer code installed without consent regardless if any damage occurs to the computer. The theory is that the malicious component encompasses the use of bandwidth and, again, that there is no consent. The idea of a benevolent virus or worm is not novel.

Early research and debate focused on the use of a worm to patch existing security flaws in software.[61] For example, a virus could be written that compresses executable files to save disk space.[62] Infected/compressed files would be automatically decompressed by the virus as needed as realised by the Cruncher virus in 1993.[63] The KOH virus encrypted floppy disks and hard disk

[60] The proof of concept is available at "Owning Kraken Zombies: A Detailed Dissection" (April, 2008) available at http://dvlabs.tippingpoint.com/blog/2008/04/28/owning-kraken-zombies (last accessed November 11, 2010).
[61] Aycock, J. and Maurushat, A., 'Good' Worms and Human Rights. Technical Report 2006-846-39. Department of Computer Science, University of Calgary, 2006.

[62] Cohen, F., "Computer Viruses: Theory and Experiments" (1987) Computers & Seucirty, 6(1), pages 22-35.
[63] Kaspersky, E., "Cruncher – the First Beneficial Virus?" (1993) Virus Bulletin, pages 8-9.

partitions for security reasons.[64] A legitimate user would know the decryption key and could access the files.

Meanwhile, early worm research implemented a distributed computing framework at Xerox PARC.[65] After solving some problems controlling the worms, a variety of applications were built including network diagnostics. A virus or worm could perform system maintenance, like upgrading outdated versions of programs.[66]

The last example involves what has been sometimes referred to as predator worms. Such worms are revisited periodically with the somewhat romantic notion that benevolent worms can hunt down and destroy bad worms, or that good worms can find and patch vulnerable machines.[67] Real attempts at predator worms, such as the Welchia worm which tried to clean up after Blaster,[68] have generally proven disastrous and have resulted in more trouble than the original worm caused. Worms may be released with one purpose but propagate and perform unanticipated functions such as altering default settings, or damaging hardware. The pro-active cleansing proof of concept by TippingPoint demonstrated that they could remedy the compromised computers with little to no damage to the computers in question.[69] If we take this as true and we ignore any legal liability issues for the purpose of our analysis, it becomes necessary to first examine whether such pro-active cleansing is ethical and second, whether or not such pro-activity should be legal.

There are many experts that have expressed strong views on benevolent payloads. For example, leading security expert Bruce Schneier describes such activity in the following terms: "Patching other people's machines without annoying them is good; patching other people's machines without their consent is not…Viral propagation mechanisms are inherently bad, and giving them beneficial payloads doesn't make things better."[70] Under this definition, no payload for a worm or botnet could be construed as morally benevolent unless there was consent. The weakness of this argument is that its discussion has been limited to similar e-commerce activities, where

---

[64] Ludwig, M., *The Giant Black Book of Computer Viruses* 2nd ed. (American Eale, 1998).
[65] Shock, J. and Hupp, J., "The 'Worm' Programs – Early Experience with a Distributed Computation" (1982) Communications of the ACM, 25(3), pages 172-`80.
[66] *See generally* Cohen, F., *A Short Course on Computer Viruses* 2nd ed (Wiley, 1994).
[67] Gupta, A. and DuVarney, D., "Using Predators to Combat Worms and Viruses: A Simulation-based Study" (2004) Proceedings of the 20th Annual Computer Security Applications Conference, ACM Digital Library.
[68] Perriot, F. And Knowles, D., "W32.Welchia.Worm" (July 28, 2004) Symantec Security Response.
[69] Tipping Point, note 57 above.
[70] B. Schneier, Benevolent Worms, Crypto-Gram Newsletter, 2003, available at http://www.schneier.com/cryptogram-0309.html (last accessed November 12, 2010).

consent is desirable from a corporate ethics perspective and is necessary in order to conclude a binding legal contract. Missing from this discussion is the application of a benevolent worm outside of the e-commerce realm, along with the discussion of the difference between consent and informed consent. The subject of informed consent in the digital age is contentious. Consent is given in most Internet applications by checking the "I Agree" button of end-user license agreements and privacy policy statements, provided that the user has had the opportunity to review the terms and conditions. This has been deemed to represent "reasonable notice" similar to the ticket cases in contract law.[71] The reality, however, is that most users do not read end-user-license agreements (EULA). When they do, such licenses contain onerous obligations which are unilaterally imposed on them and are expressed in complex, aggressive legal rhetoric. Most of these types of terms remain untested in law and run against the basic tenants of the law of contracts, namely consideration, meeting of the minds, and adequate notice of change of terms.[72]

Under Australian law dishonest use of a document or computer is criminalised when a person does more than borrow an item.[73] Dishonesty offences are pursued where there is intent to steal or commit fraud. For example, if you borrow an item such as a kitchen knife through dishonest means (take it without permission) for the purpose of committing a crime (theft) the conduct is criminalised. If, on the other hand, you borrow the knife without permission to chop up vegetables then return the item, this would not be criminalised. Fraud and dishonesty law expert Steele argues that the test should be whether there is a moral component to the action.[74] Acts that are perceived as moral though dishonest should not be criminalised under Steele's theory. In the context of a benevolent worm, strictly speaking the use of bandwidth is done without

---

[71] *Standard form online contracts where the user consents by clicking "I Agree" are often referred to as click-wrap contracts. There is no caselaw in Australia on the validity of clickwrap contracts. There is, however, caselaw on the topic in the United States where clickwrap agreements were held to be binding. See* Specht v. Netscape Communications Corp*., 306 F. 3d 17 - Court of Appeals, 2nd Circuit 2002;* Ticketmaster Corp, v Tickets.com, Inc*., (2003) WL 21406289 Central District California; and* ProCD, Inc. V Zeidenberg *(1996) 86 Federal Court 3rd District 1447 (7th Circuit).*

[72] There are many articles that canvass legal issues in clickwrap agreements. See Davis, N., "Presumed Assent: The Judicial Acceptance of Clickwrap" (2007) 22 Berkely Technology Law Journal 577; Gomulkiewicz, R., "The License is the Product: Commonets on the Promise of Article 2B for Software and Information Licensing," (1998) 13 Verkeley Technology Law Jounral 891; Newitz, A., "Dangerous Terms: A User's Guide to EULAs" available at http://www.eff.org/wp/eula.php (last visited January 17, 2011); and Geist, M., "Is There a There There: Toward Greater Certain for Internet Jurisdiction".

[73] See *Peters v The Queen* (1998) 192 CLR 493

[74] Steele, A. Alex Steel, "Describing Dishonest Means: The Implications Of Seeing Dishonesty As A Course Of Conduct Or Mental Element and the Parallels with Indecency", (2010) 31 *Adelaide Law Review* 7

permission but it is used for a moral purpose – that of cleaning up a person's computer connected to a criminal group.[75]

This is perhaps best illustrated by way of example. Many corporations, such as Sony, release products with an end-user license term authorising them to utilise rootkits, backdoors and digital rights management systems for a variety of unspecified purposes, all of which may be subject to change without notification to the user. The rootkits, in turn, render computers vulnerable to intruders to install malicious applications onto their computers. Digital rights management systems allow monitoring devices which track the use of a work (for example, a music CD), which could theoretically be used as evidence to bring legal suits against those who make illegal use of the copyrighted work. The author uses the example of consent to illustrate the discrepancy between tangential concepts of theory and practice. The author agrees that informed consent is a desirable feature in software distribution mechanisms. Concluding that consent is required in all contexts is to prematurely rule on an issue which has, so far, only been discussed in the limited context of electronic commerce. If consent is gained, do benevolent payloads become ethical? If there is no consent, are benevolent worms precluded from becoming ethical? It appears as though the debate on consent and malware has inherited the intellectual baggage of assumptions surrounding consent. Nowhere is this better articulated than in the famous essay by Robin West, "Authority, Autonomy, and Choice: The Role of Consent in the Moral and Political Visions of Franz

Kafka and Richard Posner."[76] West exposes the fallacy in Posner's theory that choice and consent in a legal system allow for an increase both in morality and autonomy. Within the confines of benevolent payloads, there is an assumption that lack of consent is inherently bad or unethical contrasted with acts where a vague notion of consent is obtained, thereby magically summoning the requisites of legal and ethical action. The presence of consent should be regarded as one component in an analysis of all factors contributing to an ethical framework. An effects analysis would look to whether any tangible damage, other than use of bandwidth, has been done to the computer, webserver or user, or in the event that other types of damage are sustained, whether there are compelling reasons to derogate from the principles of user consent and avoiding damaging third party property. More importantly, an effects analysis would address

[75] The New Zealand decision of *Hayes v The Queen* [2006] New Zealand Court of Appeal 318 addressed issues of dishonest computer access. In this instance bandwidth was used to install key-logging trojans which would retrieve personal information to steal money.
[76] West, R., "Authority, Autonomy and Choice: The Role of Consent in the Moral and Political Visions in Franz Kafka and Richard Posner" (1985) Harvard Law Review 99(2).

the issues of when it is permissible to utilise bandwidth and install software on a user's computer without their consent. When, if ever, does a benevolent payload become permissible or mandatory as a moral duty?[77]

The easiest solution to cleansing is to obtain consent from the third party. This could be achieved in a number of ways. The organisation with the list of infected computers could contact the owner of the compromised computer via email and seek permission. The organisation could contact law enforcement and ask that they seek permission. The ISP could be contacted to seek permission to cleanse from the owner of the compromised computer. Consent is preferable to no consent. Of these three entities, the ISP is best placed to inform the customer and see permission to cleanse the computer. This is explored further below.

The take-down of a botnet is rendered somewhat inconsequential if compromised computers are not cleaned. As explored in **Chapter 3**, infiltration and disruption of the C&C source only puts off the botnet herder for a period of time. The botnet herder can still set up new C&C sources, and write new bots (malicious software programs) to communicate with the zombie computers. The takedown of the botnet is, therefore, only temporary as most botnets use self-replicating worms. This means that stopping the C&C of the botnet does not necessarily prevent the botnet from continuing to spread and thus acquiring new zombie computers. It also does not prevent a botnet from spreading new bots once a new C&C source is established. Prosecuting the botnet herder also is not an absolute solution as the botnet is highly susceptible to being taken over by another botnet herder. Moreover, the zombie machines sit dormant awaiting new instructions. Only bot remediation potentially removes the compromised computers from the equation. To use an analogy to war, one can disrupt an army by interfering with its communications systems, and one can kill the General but there will always be more Generals willing to step up, and ways of re-establishing communications. But if there are no soldiers, the General has no one to carry out the orders in his command. Without cleansing of the computers the initial infection vector still exists and the machine remains susceptible to new commands.

The TippingPoint paper on the Kraken botnet and cleansing program contain detailed discussion among security experts in the comments section including discussion within the security team at TippingPoint.[78] The main arguments against pro-active cleansing are that 1) it

[77] The issue may be seen as one of normative ethics drawing on effects-based analysis in consequentialism as well as that of moral duty in deontology.
[78] TippingPoint., note 57 above, pages 2-10.

exposes the company to legal liability and criminal sanction, 2) it might accidentally crash the target system causing damage, and 3) such crashing of a target system may have serious repercussions if, for example, the system is responsible for someone's life support, attached to a nuclear power plant or military operations.

There were a number of commentators on the TippingPoint blog that iterated that the life support system was an extreme and somewhat ridiculous example, noting that life support systems would never be connected to the Internet.[79] Some life support systems are connected to the Internet. Medical ICDs (defibrillators) communicate information about a patient's heart to external machines and to a central database for a doctor to monitor.[80] Researchers have exposed security risks of ICDs.[81] ICDs currently do not use a cryptographic key to secure wireless communication. If an ICD is connected to a network and that network is connected to the Internet it is theoretically possible for ICD devices to be hacked, as well as for computers monitoring the heart-rates to be compromised. This example is stretched somewhat. A more compelling example is the recent infection of computers at the Iranian Bushehr nuclear power plant with the Stuxnet worm.[82] As many botnets propagate through worms, it is possible that botnets could utilise computers attached to critical infrastructure networks as seen in the very real Bushehr nuclear power plant example.

There has been much speculation and conflicting viewpoints on the Stuxnet worm that infected the Iranian Bushehr nuclear power plant. The principal point of contention is identification of who wrote and distribution the worm with speculation pointed at the United States and Israeli governments. There is no known conclusive proof that these governments were responsible.[83]

---

[79] Comment 9 by Anonymous states, "do you know of any such life support machine that is actually connected to the internet?" Comment 14 by Not so Anonymous added, "I know of no medical place that has windows running heart monitoring systems." Comment 18 by John, "there are no life support systems running on Windows."

[80] An "ICD device is a small battery-powered electrical impulse generator which is implanted into patients who are at risk of sudden cardiac death due to ventricular arrhythmias. The device is programmed to detect cardiac arrhythmias and to correct them by delivering a jolt of electricity." Note 81 below.

[81] Daniel Halperin et al, 'Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses' (2008) Secure Medicine <http://www.secure-medicine.org/icd-study/icd-study.pdf> at 9 May 2010. Susan W. Brenner, *Law in an Era of "Smart" Technology* (2007) 173.

[82] 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). *See also* Schneier, B. "Stuxnet" (October 7, 2010) available at http://www.schneier.com/blog/archives/2010/10/stuxnet.html (last accessed November 12, 2010).

[83] The New York Times does write a compelling story conveying circumstantial evidence indicating that the worm may have been a joint U.S./Israeli operative. *See* Broad, W., Markoff, J. and Sander, D., "Israeili 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). Many hacking sites, however, report that a dodgy company known as SERCO may be behind the attacks and have indicated that it is more likely that Stuxnet was released by a criminal malware group or by a company that does

There is equal speculation as to whether the worm was able to penetrate the computer systems of the nuclear power plant and if so, whether any data was lost or altered[84]. There is, however, consensus on how the Stuxnet worm propagates. According to security expert Schneier:

> "Stuxnet is an Internet worm that infects Windows computers. It primarily spreads via USB sticks, which allows it to get into computers and networks not normally connected to the Internet. Once inside a network, it uses a variety of mechanisms to propagate to other machines within that network and gain privilege once it has infected those machines. These mechanisms include both known and patched vulnerabilities, and four "zero-day exploits": vulnerabilities that were unknown and unpatched when the worm was released. (All the infection vulnerabilities have since been patched.)
>
> Stuxnet doesn't actually do anything on those infected Windows computers, because they're not the real target. What Stuxnet looks for is a particular model of Programmable Logic Controller (PLC) made by Siemens (the press often refers to these as SCADA systems, which is technically incorrect). These are small embedded industrial control systems that run all sorts of automated processes: on factory floors, in chemical plants, in oil refineries, at pipelines--and, yes, in nuclear power plants. These PLCs are often controlled by computers, and Stuxnet looks for Siemens SIMATIC WinCC/Step 7 controller software."[85]

Essentially, Stuxnet first propagated through a USB stick but once on the computer's systems Stuxnet looks for PLC on Seimen's SCADA control systems. At this point the infected machine would receive instructions from a bot and join the Stuxnet botnet.[86] The Stuxnet botnet receives instructions in a P2P channel, and operates similar to Mebroot with the worm hiding in the rootkit. While there remain speculation as to who wrote Stuxnet and for what purpose, there seems to be consensus that Stuxnet is one of the first exceptional tools in waging cyberwar due to its ability to penetrate the control systems of critical infrastructure systems such as nuclear plants and electrical grids. Pro-active cleansing of machines connected to critical infrastructure

---

business with governments for defense contracts. *See for example*, "Is Serco Behind Stuxnet" (thread started September, 2010 and ongoing) available at http://www.abovetopsecret.com/forum/thread615788/pg1 (last accessed February 7, 2011).

[84] The New York Times reports that retiring chief of Israel's intelligence agency, MOSSAD, has stated that Iran's nuclear power program has run into technical difficulties which will delay the nuclear program until 2015. Broad, note 83 above. The Iranian government has publicly announced that Stuxnet did not set back their nuclear program though there is aknowledgeable that there has been some disruption to Iranian centrifuges. This acknowledgement, however, does not specifically refer to Stuxnet. See for example, Madrigal, A., "Ahmadiejad Publicly Acknowledges Stuxnet Disrupted Iranian Centrifuges" (November 29, 2 010) available at http://www.theatlantic.com/technology/archive/2010/11/ahmadinejad-publicly-acknowledges-stuxnet-disrupted-iranian-centrifuges/67155/# (last accessed February 7, 2011).

[85] Schneier, B., "Stuxnet" (October 7, 2010) available at http://www.schneier.com/blog/archives/2010/10/stuxnet.html (last accessed February 7, 2011). Similar descriptions may be found on all major anti-virus companies' websites. *See for example* 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). *See also* Microsoft, "The Stuxnet Sting" (July 16, 2010) available at http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx (last accessed February 7, 2011).

[86] *See* report from the United States National Cyber-Forensics and Training Alliance on Stuxnet available at http://www.ncfta.net/ncfta-news/ncfta-cyber-alerts/stuxnet (last accessed February 7, 2011). A detailed video examining Stuxnet is provided by 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). Excellent information is also found by Symanetc, note 85 above.

without consent is a real possibility and could potentially have serious ramifications. Consent and pro-active cleansing is explored in greater detail below.

Pro-Active cleaning involves unauthorised access and modification to the compromised computers (the "unauthorised access, modification and impairment" criminal provisions were explored in detail in **Chapter 4,** and will be examined in **section 8.3.2** below). There are two methods, however, which would allow for lawful pro-active cleansing. First, if the owner of the compromised computer was contacted and granted informed consent to the cleansing, this would not be construed as unauthorised. Second, if the ISP performed the pro-active cleansing there would be no unauthorised actions (providing that pro-active cleansing provisions were included in the service agreement with end-users). Although the ISP Bot Remediation program as canvassed in **Chapter 7** does not contemplate pro-active cleansing in the manner proposed by TippingPoint, that is not to say that there is anything preventing the ISP from performing the cleansing, either through modification of the e-Security Code of Practice (the Australian Internet Industry Association's self-regulatory instrument as previously explored in **Chapter 7**) to allow for such intervention, or through the terms in the service agreement with end-users.

TippingPoint has not made public the computer code they wrote to pro-actively clean Kraken-infected computers. This is potentially important as placing the code in the public domain would allow another actor to perform pro-active cleansing. It might also afford the botnet master the opportunity to modify the code and use it for malicious purposes. This is similar to those who release information about vulnerabilities in software and how to exploit them, but who do not actually release the worm and take advantage of those vulnerabilities. Comment 14 from TippingPoint provides more context to this scenario by stating:

> "hey guys. Great job, wish I could help in some way ... i guess maybe if you had someone that wasn't working for you, but had access to this info, they could be the ones to push that red go button, and leave you without blame, I would be proud to help in any way as a means to an end...
>
> If you want to contact me, u know what you have to do.
>
> cya"

Unfortunately for the commenter above, he or she does not realise that this type of action would not remove TippingPoint from liability. In this scenario, it would still be possible to construe the public dissemination of the code as negligent conduct, and possibly as "aiding and abetting" in the commission of a crime as explored in **Chapter 4**.

8.3.2 Unauthorised Access, Modification or Impairment of Data, and the Absence of Exemptions

Members of self-organised security communities are not exempt from the "unauthorised use and abuse" provisions. As seen in **Chapter 4,** there are no security research or public interest exemptions from unauthorised access, modification or impairment of data provisions. Where a university, corporation or individual researcher, no matter what the good intention, performs any type of unauthorised action, they expose themselves to criminal sanction. The decision to bring criminal proceedings against the security activists rests with the discretion of the public prosecutor. The only type of legal countermeasures are ones that are passive and thereby do not involve any unauthorised access, modification or impairment to data. Prevention and detection and some forms of intelligence gathering (passive honeynets as will be explored below) would fall outside of the scope of criminality. However, most of the actions performed by self-organised security communities are clearly unauthorised.

Whether or not taking over the command and control servers of a botnet is unauthorised will depend on ownership of the C&C points. Where researchers are first to register domain names, they are able to control how to direct or redirect traffic to their website. Where botnet masters are the first to register the domain names used in the C&C the matter is different as interference with the traffic here would not be authorised. Command and control servers located in peer-to-peer systems present a novel legal issue as no one has a legal right over any point of the system. When signing up for a peer-to-peer protocol such as BitTorrent, users must consent to the terms of agreement which include not using the software for illicit purposes.[87] Clearly a botnet master would be in violation of the terms of agreement. Would a security researcher's efforts to take-over the C&C server in the peer-to-peer realm be construed as illegal? This is an unsettled area of law. That said, peer-to-peer systems are commonly referred to as filesharing programs. Users make available certain files to be shared on their systems with other members of the peer-to-peer community. This does not authorise botnet masters or security researchers to leverage the computational power of computers connected to a system to place any type of file, or to interfere with the computers connected to the peer-to-peer system. In my view, this would be considered unauthorised access under Australian law because there is no exemption for security research (explored in **Chapter 4**).

[87] The exact wording of clause 2 is, "You will not use BitTorrent for illegal purposes." A copy of the end user license is provided in **Appendix B**. The license is available at http://www.bittorrent.com/legal/bittorrent-eula (last accessed Feb. 10, 2011).

As seen in the cases of the Torpig, Waledec and Mariposa botnets in **Chapter 3**, the work of security researchers is imperative in botnet intelligence gathering and dismantling. Much of the work of security researchers and corporations is prohibited by the law as the work involves unauthorised access and modification of data and data systems. The fact that security researchers haven't been prosecuted is only a matter of lack of public will to do so. This is not a comforting fact to most security researchers.

The Australian Commonwealth *Criminal Code* and State criminal acts and codes do not include a security research exemption to computer offences. As will be explored in the next chapter, Australia will accede to the *Cybercrime Convention* which encourages member states to make security research exemptions to computer offences. The *misuse of a device* provision specifically allows nations to provide exemptions for security researchers. It cannot be stressed enough how important this exemption is. There is no discussion in the Model Code about exemptions to the proposed computer offences other than in the context of self-defense.

Security researchers, organisations, university computer science departments and technology companies are the primary forces behind tackling botnets and other forms of obfuscation crime tools such as malware. There has yet to be a single takedown of a botnet or prosecution of a botnet master that only involved law enforcement agents. In all publicly disclosed instances,[88] security researchers were involved in spite of the fact that they could have potentially been charged with a form of unauthorised access to computer data.

Law enforcement agents work with security researchers, as seen in the Waledec and Mariposa botnet investigations, through a variety of means. Researchers are key figures in information gathering on botnets, often through virtual honeynets. Security researchers may also visit known hacker chatrooms and websites to gather and collect information. It is difficult to conceive of a successful botnet prosecution without some information from security researchers. It is strongly recommended therefore that Australia adopt a security research exemption to those computer offences dealing with unauthorised access, modification or impairment of data or electronic communications. It is not recommended, however, that such security research exemptions

[88] Pandalabs was heavily involved in the takedown of the Mariposa botnet. Microsoft was heavily involved in the takedown of the Waledec botnet. Law enforcement, and a number of international computer security organisations and university researchers aided Microsoft and Pandalabs in the takedown of these botnets. *See* "Waledac Questions Answered" available at http://www.lavasoft.com/mylavasoft/company/blog/waledec-questions-answered. *See* Corrons, L. "Mariposa Botnet" (March 3, 2010) available at http://pandalabs.pandasecurity.com/mariposa-botnet/

extend to instances where government data and electronic communications are the target as this would be an open invitation for cyber espionage and information warfare.

A security research exemption is clearly needed. Special attention will need to be paid to the drafting of a security research exemption such that it is not open to abuse. One mechanism may be to adopt the Queensland approach where individuals and corporations in the security industry are required to be licensed.[89] This includes computer security entities. Only those licensed security entities would be entitled to use the security exemption. An additional feature would require security entities to report their activities pre-engagement of self-help mechanisms to a designated authority such as AusCERT or its equivalent.

A complementary alternative is to provide clear a Code of Conduct for ethical engagement in hacking. Where the entity strictly adhered to the Code of Conduct, they would be granted immunity against criminal proceedings. The Code of Conduct would have similar rules to that of the legalisation of third party hackback as explored in **Chapter 4** with three additional rules (rules 8-10). For clarification, they are:

Step 1: sufficient attribution of the source of attack has been achieved and verified by more than one source (this may entail more than one method such as liaising with AusCERT or NCTSI to see if other organisations have been attacked in a similar method, consulting honeynet groups and researchers at SANS or Shadowserver),

Step 2: other alternatives are ineffective. If there is sufficient attribution, other alternatives such as police enforcement would not be effective (Eg. party is located in a cybercrime haven such as in a country that has not ratified the *Cybercrime Convention*),

Step 3: minimal damage to third party systems. There is a minimal possibility of innocent third parties being seriously affected,

Step 4: record of a data log. A data log is kept documenting each step of the counter attack inclusive of potentially affected third parties. The data log must then be kept for a minimum of 90 days,

[89] Queensland Government Office of Fair Trading. The various types of licenses and their requirements are available at http://www.fairtrading.qld.gov.au/security-industry-licence-types.htm (last accessed March 1, 2011).

Step 5: copy of data log is sent to AusCERT. It is vital that those organisations engaged in hackback be held accountable for any actions which deviate from lawful hackback or in those instances where damage is suffered to innocent third parties. AusCERT (or its equivalent) is in the best situation to know if a third party has suffered any damages as many corporations or organisations under attack consult and report the incidences to AusCERT. They are in the best position to know when an innocent third party has been affected. Such compulsory disclosure is necessary as an effective restraint to not overstep reasonable self defence,

Step 6: **reasonable measures.** The hackback method is limited to measures that are reasonable, proportionate and necessary to avoid damage to third party systems. This would include methods which are protective in nature and not retaliatory (designed to destroy the other party's computer system). It would be useful to have a nation-wide consultation to produce a "Code of Hackback" which would outline specific examples of what measures are reasonable, proportionate and necessary in different scenarios, and

Step 7: engagement of security expert. Where an expert third party is used to perform hackback, the entity who hired the expert is jointly responsible for any damages or losses sustained to innocent third parties. There should be a list of accepted security experts and organisations (Eg. registered computer security consultants, SANS Institute).

Step 8: tell the most affected party first. Where, for example, a vulnerability has been found in a software program or hardware component, the vendors should be first to be notified in order to allow them the opportunity to remedy the vulnerability before public disclosure.

Step 9: test on your own system where possible. Where information is needed to verify the vulnerability on a system or to determine how a botnet propagates it should be tested on your own system or honeynet, and not on a third party system unless otherwise authorised.

Step 10: notification to Privacy Commission. Where security research has inadvertently violated privacy rights, providing that the research has been performed in accordance with the Code of Conduct, the researcher should be exempt from liability. However, the Privacy Commissioner should be made aware that such privacy violations have occurred in much the same way that AusCERT or its equivalent is notified.

8.3.4 Honeynets

The use of honeynets has not attracted attention in Australia in the same manner that it has in the United States where there has been an ongoing debate about ethical and legal issues surrounding the use of honeynets. Many of the ethical and legal issues are intertwined with the use of honeypots. Legal issues such as entrapment and interception of communications were explored in **Chapter 4**. According to expert Richard Salgado, "The very purpose of your honeypot is to be attacked ... so it's a little odd to say we're doing our monitoring of this computer to prevent it from being monitored."[90] Here Salgado was referring to corporations using honeypots to collect information. As we have seen in **Chapter 7**, ISPs may legally use honeypots to collect information about botnets as they are exempt from interception of communications rules under the provision of "network protection duties."

Security researchers are not exempt from either unauthorised data provisions, nor are they lawfully able to intercept communications as all communications, whether criminal or otherwise, are protected under the law unless an exemption may be found in the *Telecommunications Interception Act*. As noted in **Chapter 7**, interception of communications in a honeypot is lawful where owners of compromised machines as well as botnet masters are notified (Eg. via banner display) that their communications are being monitored. This, of course, would defeat the purpose of a honeynet. The other way to legally operate a honeynet is to establish a production machine, wait to first be attacked, then use the honeynet. The malicious traffic is rerouted to the honeynet only after an attack on the production server is initiated.

8.4 THEORETICAL FRAMEWORK

Scholarship on self-help is well-developed.[91] Experts have explored the use of self-help remedies such as physical force in the offline world and counter-attack in the online world. This self-help literature to date is limited to situations of owners of private property and does not include a third party performing such actions. It is difficult to see how self-help remedies fit in Lessig's

---

[90] Salgado, R., "The Legal Ramifications of Operating a Honeypot" (2005) IEEE Magazine Security and Privacy, vol. 1 . Salgado is considered as a recognized authority of legal issues in honeypots. He is former attorney with the United States Department of Justice, Computer Crime and Intellectual Property Section, U.S. Department of Justice, and Senior Counsel with Yahoo!, Inc. He is now Senior Counsel of Google and Adjunct Professor at Stanford University.

[91] See for example, 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. Posner, R., "Killing or Wounding to Protect a Property Interest" (1971) 14 Journal of Law and Economics 201.

paradigm. This may be seen as problematic given that an entity is regulated through market, law, norms, and architecture.[92] Where corporation employs self-help remedies this *might* be seen as falling within a market response with possible utilisation of technologies to achieve these ends. The use of self-help remedies by corporations *may* also be seen as a norm within corporate culture. From an end-user perspective. self-help remedies may be viewed as normative as well. It is difficult, however, to see where the activities of self-organised security communities fall within Lessig's paradigm. In situations such as the Mega-D and Waledac Working Groups it may be appropriate to suggest that these were market-led initiatives that interacted with technologies to achieve effective countermeasures. It is more difficult to categorise such efforts of groups such as Shadowserver, Spamhaus, OID and individual spamhunters as falling within Lessig's modalities. Self-organised security communities have formed to fill an absence of effective response to botnets by governments, law enforcement, anti-virus software programs, and the market. It is the failure of each of Lessig's four modalities to address botnets that has led to the extent of self-organised security communities forming to fight botnets. The final chapter provides a summary of approaches to combating botnets and offers a critique of Lessig's modalities when applied to botnets. Suggested changes to Lessig's model will be examined in this final chapter. This will include an analysis of how self-help remedies act as a constraint, and how potentially Lessig's theory of norms could be altered to better accommodate the work of self-organised security communities.

[92] The topic of self-help remedies was discussed in detail with my supervisor Graham Greenleaf, who has in his own research encountered similar queries with Lessig's model.

Chapter 9

CONCLUSIONS: REGULATING BOTNETS, REVISING LESSIG

Table of Contents

9.0 AIMS OF CHAPTER

This chapter will summarise regulatory approaches to botnets with a list of recommendations for three main areas: criminal law, ISPs and DNS providers, and self-organised security communities. Lessig's four modalities regulatory model will be briefly restated then applied to the botnets discussed in the thesis: Kraken, Torpig, Waledac, Mariposa, Mega-D and Akill's Botnet. The chapter will conclude with discussion on possible amendments to Lessig's modalities.

9.1 REGULATORY APPROACHES TO BOTNETS

9.1.1 Criminal Law

This thesis considered the national and international criminal law frameworks relevant to botnets in **Chapters 4, 5** and **6**. These chapters demonstrated the limited role that criminal law plays in botnet countermeasures. To the extent that the law will play a limited role, that role was discussed and recommendations made to enhance the ability of law enforcement to play a more effective role in combating botnets.

Chapter 4 analysed the national criminal framework relevant to botnets. Specific recommendations included:

- that misuse of a device under the Criminal Code (Cth) should expressly include "botnets" as a device
- that there should be a security exception from unauthorised access, modification and impairment provisions as well as the misuse of a device provision
- that self-defence measures in the form of hackback / strikeback be legalised with clear guidance using seven steps:

    1: sufficient attribution has been achieved and verified;

    2: other alternatives are ineffective;

    3: minimal damage to third party systems;

    4: record of a data log;

    5: copy of data log is sent to AusCERT;

    6: reasonable measures; and

    7: performed by licensed security expert.
- that third parties performing hackback be subject to the same guidelines as those first parties acting in self-defence
- that any security research exemption expressly include language on the legality of honeynets
- that a public interest exemption to unauthorised access be considered by the government (discussion of this possibility under the Model Criminal Code)
- that informed consent become the standard for online consumer terms and conditions

- ACMA to have clear mandate for investigation into unwanted software, malware and botnets which would be coordinated with AusCERT and AusGovCert

Chapter 5 addressed the international criminal framework relevant to botnets, focusing on the *Cybercrime Convention*. Recommendations included:

- Australia should adopt the aspects of the *Cybercrime Convention* that are relevant to botnet regulation
- Civil liberties should be impaired as minimally as possible with the accession to the *Convention*
- Specifically, Australia should include the requirement of a dual criminality clause
- Guidelines be provided on maximum duration of retaining a computer or computer system through search and seizure without laying charges
- Clear language on data retention and disposal and security standards should be given to ISPs.
- Australia should make a recommendation to Interpol to include a database on botnets as one of its projects for more effective law enforcement cooperation

Chapter 6 discussed general issues which made the use of criminal law difficult. It was noted that traceback to the source of attack was extremely difficult, that there were complex jurisdiction issues, that digital evidence was volatile, and that the Australian warrant regime was adequate for gathering evidence against botnet masters in the event that traceback was possible. It was recommended that:

- remote search and seizure by Australian authorities for serious crimes be allowed under the supervision of a judge
- Internet Service Providers will need real-time evidence collection abilities
- Memoranda of Understanding should be signed between Australian States and Territories and foreign jurisdictions so that damages may be aggregated thereby triggering investigation

9.1.2 The Role of ISPs and DNS Providers in Combating Botnets

Chapter 7 demonstrated the essential role that ISPs and DNS providers will play in combating botnets. **Chapter 5** addressed how ISPs would be compelled to preserve data, respond to production orders, and allow real-time interception abilities to run on their networks. **Chapters 5 and 7** advocated for a cautionary approach by ISPs and DNS providers in performing law enforcement activities, especially where such activities impacted on civil liberties, most notably privacy and freedom of expression. The following recommendations were made:

- Australia should pilot a bot remediation program
- The bot remediation program should be coordinated between ACMA and the IIA where statistics are compiled throughout the duration of the program in order to improve on its impact, and to assess whether there has been a positive impact on reducing compromised computers
- ISPs should not be liable for bot remediation programs
- Both the Cybercrime Convention and the Bot Remediation program require ISPs to monitor and detect data traffic which in turn creates the need for:
    - Clear guidelines on permissible detection and monitoring techniques
    - The preference for passive monitoring techniques
    - Data retention and destruction policies
    - High security standards to safeguard the information collected and stored
    - Small ISPs must follow the National Privacy Principles

9.1.3 Self-Organised Security Communities

Chapter 8 examined the inner workings of several self-organised security communities (SOSCs) including Shadowserver, Spamhaus, Offense-in-Depth, and an independent spam hunter. Additionally the work of university researchers, not-for-profit security corporations and working parties were examined. In this instance the botnet working parties comprised a combination of members of SOSCs, private security firms (Eg. Pandalabs), non-for-profit corporations (National Cyber-Forensics Training Alliance), university researchers, ISPs and DNS providers, and law enforcement.

A strong recommendation was made to provide a security research exemption for the actions of SOSCs and other security researchers. Security researchers (university computer science

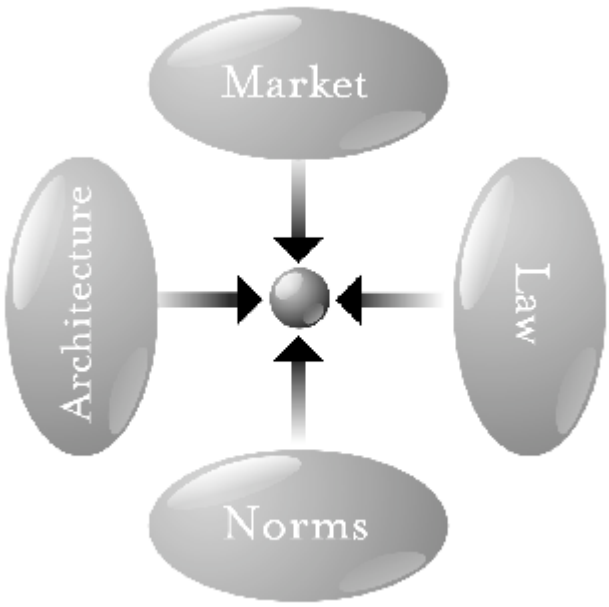
departments, technology companies, and self-organised communities) are the primary forces behind tackling botnets and many other forms of cybercrime. It was noted that currently, security researchers in Australia are not exempt from the computer provisions of the *Criminal Code (Cth)* or the equivalent computer offence provisions in the Australian States and Territories. There has yet to be a single takedown of a botnet or prosecution of a botnet master that did not involve security researchers. Cyber-crime prosecution rarely occur without their help, therefore, it was argued that such entities must be free from legal sanctions against reasonable research behaviour, rather than discouraged from participation.

The actions of the SOSCs groups were classified as a self-help remedy. It was demonstrated that the workings of SOSCs, university researchers and botnet working parties were not easily situated in Lessig's modalities. This is discussed below.

9.2 LESSIG'S FOUR MODALITIES

Lessig's four modalities model remains the most influential Internet regulatory theory. **Chapter 2** examined the four modalities: market, law, norms and code. Lessig's modality diagram is reproduced below in **Figure 9(A).**

Figure 9(A) Lessig's Four Modalities



Lessig's primary thesis is that the behaviour of the entity in the centre of the diagram would be regulated by market, code (architecture), law and norms. Of these regulatory modalities, Lessig viewed architecture and then law as being the most influential. Market and Norms, while still important, are less developed in Lessig's theory.

Many of the activities and groups working to counter botnets cannot be categorised into the four modalities without difficulty. Self-organised security groups remain a highly problematic categorisation while the work of not-for-profit security corporations, working parties and university researchers are also not easily situated into Lessig's modalities. Looking at the example of botnet take downs will best illustrate the point. Five botnets will be considered: Kraken, Torpig, Waledac, Mariposa, Mega-D, and Akill's Botnet.

9.2.1 Kraken Botnet

Countermeasures to take down the Kraken botnet were performed by the security corporation, TippingPoint and the SOSC, Offense in Depth Initiative (ODI). These groups gathered intelligence on the botnet, and then redirected the C&C sources to a sinkhole. TippingPoint may be reconciled within Lessig's modaliy of the "Market" to the extent that, as a for profit security computer security corporation, they perceive reputation arising from their activities leading to commercial advantage. The "Market" as a regulatory influence, however, has typically meant operating a business in a competitive fashion in order to turn profit done through price setting, supply and demand, and competitive practice. Linking the actions of TippingPoint and other security firms to the "Market" is somewhat of a stretch.

Members of ODI are diverse spanning over multiple countries and including university researchers, and those who work in the computer security field. The activities of ODI, however, are not endorsed openly by the universities and companies that their members work for nor is the work typically performed during regular company hours. Members of ODI participate in botnet take downs on their own time. They work on their own time because they perceive the action to be "the right thing to do". They are not motivated by commercial advantage as security firms may be.

The actions of many botnet working groups, whether they are self-organised security communities, working groups, university researchers or security firms, is that they are taking

retaliatory self-help actions, some of which the law may not prohibit, but in many instances, the actions are illegal and would constitute unauthorised access or modification to data or a data system. In the case of botnets, the extent of the problem and damage caused is so grave that everyone wants to turn a blind eye to the illegal methods used. Botnet masters perform unauthorised access and modification to data systems. Groups working to counter botnets perform self-help by also accessing and modifying data systems in an unauthorised manner. In this sense, regulation happens. Regulation happens not because the law prohibits or does not prohibit and action, but because self-help actions are unlikely to be detected, and where detected, there is no serious threat of possible prosecution. This type of action is not law. It is not market and it is not norms. It is the missing fifth modality in Lessig's theory.

9.2.1.2 Torpig

Countermeasures against Torpig involved intelligence gathering and an unsuccessful attempt to take down the botnet. Researchers at the University of South California (USC) set up a honeynet to observe the botnet. In doing so they were able to see how the C&C source would rotate. They then registered the domain names of the future C&C sources in order to take over the botnet (which they did for 10 days). They identified that Torpig had an ultimate C&C source which was a secondary botnet found in the rootkit known as Mebroot. USC notified the FBI of their activities. The FBI notified the not-for-profit organisation National Cyber-Forensics Training Alliance (NCTA). These organisations contacted the ISPs who had IP addresses linked to the C&C sources. Most of these ISPs took measures to remove the IP addresses that were linked to the C&C source. Once NCTA and the FBI became involved the botnet, literally within hours, utilised its secondary C&C source, the Mebroot botnet, to take over Torpig.

To the extent that the actions of the USC researchers and NCTA can be said to be influenced by Lessig's modalities, the university researchers' actions could be regulated by norms as, with this particular case, the researchers were from a small closed-knit group. The NCTA is more difficult to properly categorise as they are a middle man between law enforcement and corporations who have fallen victim to cyber attacks. The NCTA is run by a former cybercrime prosecutor, and provides unpaid internships to a variety of students who have studied computer science, commerce and law. While the NCTA is registered as a not-for-profit corporation it is difficult to see how its actions could be seen as falling within the "Markets" modality as they are not motivated by traditional notions of profit and capturing the market. They may be better categorised as a hybrid where they are influenced by the market, law and norms.

9.2.1.3 Waledac

The take down of the Waledac botnet involved corporations, university researchers, ISPs, the court, and a CERT. In this case, Microsoft's Digital Crime Unit sought a court order requesting the U.S. Federal Court to grant a temporary restraining order against domain owners of domain names of C&C sources. The majority of the C&C sources were registered with the United States ISP, VeriSign. Complying with the order, VeriSign (and a few other ISPs) removed the names from their servers. At the same time, a coordinated effort to shut down the C&C servers in the peer-to-peer channels was performed by those in the China CERT, Shadowserver Foundation, the Vienna University of Technology, University of Mannheim, University of Bonn, and the University of Washington.

Although Microsoft's actions would clearly fall under the "Market" modality, it is interesting to see that they have a unit known as the "Microsoft Digital Crime Unit". Crime units traditionally have been associated with governmental law enforcement. Many large Internet companies have similar units such as Google, Yahoo, VeriSign and EBay who all employ former cybercrime prosecutors and police officers to work with their security and crime unit teams. In this sense, the market is clearly involved with botnet countermeasures. Microsoft's actions are influenced by gathering the reputation to be seen as concerned about security and botnets; they wish to be seen as cleaning up their own backyard. The more impervious hotmail accounts are to botnets, the more likely, or so the theory goes, that customers will gravitate to the platform. Microsoft could only use the law to partially achieve their ends. Security researchers from universities had to be engaged to take down the C&C sources in the P2P nodes as this cannot be performed by gaining authorisation ahead of time.

China CERT is a government entity responsible for emergency computer security incidents in China. CNCERT coordinated the take down of domain names connected to IP addresses of C&C sources registered in China.

The SOSC, Shadowserver, was also involved with the takedown while security researchers from Europe and the United States. Members of Shadowserver and the various university researchers are diverse spanning over multiple countries and would may not be known to one another other than by reputation or handle names. As such, their actions are difficult to reconcile with Lessig's "Norms" modality.

9.2.1.4 Mariposa

The Mariposa Working Group (MWG) comprised the computer security corporation, Panda Labs, university researchers from Defence Intelligence Georgia Tech Information Security Centre (DIGTISC), and law authorities in Spain. The Mariposa botnet master was identified through an intelligence gathering from Panda Labs and DIGTISC. The information was passed to law authorities who arrested the botnet master. There are no challenges to Lessig's model with this initiative.

9.2.1.5 Mega-D

In the take down of the Mega-D botnet, employees of the computer security corporation Firefly gathered intelligence and coordinated the takedown of the C&C sources with the help of the SOSC, Shadowserver, who provided the sinkhole. This is capable of explanation by Lessig's model similar to the workings of TippingPoint in the Kraken botnet.

9.2.1.6 Akill's Botnet

Based on the investigation of adware company DollarRevenue in the Netherlands, information from the not-for-profit security corporation Team Cymru, the FBI and the Dutch regulator, OPTA was sent to the New Zealand law authorities. New Zealand law authorities arrested Owen Walker and brought him up on charges of dishonest use of a computer and unauthorised access and modification to data systems. As a not-for-profit corporation Team Cymru holds a similar position to NCTA. Team Cymru is also staffed by many former high tech crime police officers. It is difficult, therefore, to fully categorise their work as falling into the "Market" modality or "Law" modality as their actions are not performed by reason of obeying the law or capturing a competitive edge to increase profit.

9.3 ALTERNATIVE MODELS

Lessig's model has been attractive for its ability to categorise Internet regulatory efforts. The model is relatively simple and translates well across a variety of disciplines. As has been demonstrated in the botnet take down examples above and throughout this thesis, it is difficult to categorise the actions of many individual and groups as falling neatly into the four modalities.

Let us turn to the Lessig framework in the context of the individual botnet master. As demonstrated in **Chapters 3 through 8** the four modalities do not effectively constrain the botnet master. Whether the constraint is considered objectively or subjectively it does not seem to be an important factor. Put differently, the botnet master does not have sufficient constraint, objective or subjective, to deter him/her from using botnets for criminal activity.

The market does not offer a deterrent. It could be argued, that the market, free dynamic hosting, actively facilitates illicit behaviour. The law is equally impotent to impact on botnets, partially due to techniques developed to evade law enforcement thus making traceback, evidence collection and prosecution unfeasible. Where the botnet master is located in a "cybercrime friendly" jurisdiction, such as many Eastern European countries, parts of Asia and Africa – whether due to lack of political will to prosecute, lack of law enforcement resources, or the legitimate prioritizing of other legal issues – the botnet master is out of reach from prosecution.

The present architecture and norms likewise provide few constraints. Both software and hardware are inherently insecure. Additionally, dynamic technologies are built to run on the Internet.

Equally ineffective are social norms. While the larger computer programming field could be said to have their own internal code of ethical conduct, there are few social sanctions that effectively operate within the botnet industry. It could be that in order for social norms to be effective, they need to evolve from smaller communities whose entities are known to one another, or that there are different social norms amongst the computer programming community. In other words, the computer programming community involves some disconnected communities. As previously noted there were periods of malware deployment in the early 2000s where many Russian programmers justified their fraudulent activities by the fact that they were only stealing from those who could afford it, individuals from first world countries with over a certain amount in their bank account.[1] Professional security experts are offended at the suggestion that their work is activist or vigitalist.[2] The worlds of security experts and cybercriminals, however, collide

[1] According to Moscow cybercrime analyst Kimberly Zenz the amount varied depending on the malware programmer but a reoccurring figure was $1000 USD. Zenz, note 54 above.
[2] I presented a paper at ISOI 2009 conference held in Estonia entitled, "The Limits of 'Permitted Self-Help' in Internet Security and Intelligence" to a group of security experts and cyber-activists who spend countless hours voluntarily combating cybercrime. The ISOI group is comprised by leading security experts from corporations such as Microsoft, Arbour Networks, ICANN, various Certs, Shadowserver, SANS and former Chief Cybersecurity Advisors to Prime Ministers and Presidents of various western countries. This attentive audience grilled me for over an hour on characterisation of vigilantes, activities, self-defense and information warfare.

in hacking conferences such as Chaos Club Conference in Germany, Blackhat in Los Vegas, Def Con in Los Vegas and Ruxcon in Australia.[3]

The activities of self-organized communities such as Shadowserver play an important role in responding to the threat of botnets. This is documented in **Chapter 8**. Many of these groups are comprised of security experts and white hat hackers who take an active role in combating security threats. The activities of these groups range from providing research and statistics, reporting threats, issuing notice and takedowns to Internet Service Providers and Domain Name Registries, collecting evidence for prosecution, and in some instances, responding to attacks with counter-attacks. Such groups are not affiliated with law enforcement agencies, therefore, to the extent that they influence the behaviour of online programmers, they cannot be categorized as stemming from the modalities of law, market or architecture. Norms is the only modality with some remote possible affiliation to self-organized communities but this is doubtful.

If the activities of botnet masters could be said to fall within a larger community of either "computer programmers" or "Internet users", then there may be some social norms operating which constraint actions but this is a big stretch to make such a claim tenable. The botnet master writes and distributes malicious programs for commercial gain. These activities are deemed unacceptable by the larger Internet user community and by the computer programming community. The first community, "Internet users", are not in the position to impose sanctions against the botnet master. The second community, "computer programmers", are in a better position to impose sanctions such as counter attacking, black-holing or sink-holing problematic websites, and alerting anti-virus and anti-spyware companies to new threats. This categorization, however, seems contrived. After all, such self-organized communities have internal ethics which guide how they sanction. Each group has developed a unique set of social norms. These norms range from disrupting the command and control of botnets to launching a counter of denial of service attack to collaborating with law enforcement to gain evidence to mere gathering of statistics. Social norms, as Lessig writes, are constraints imposed not through the organized or centralized actions of a state, but through the many slight and sometimes forceful moral and customary sanctions that members of a community impose on each other." Many of the moral sanctions imposed by self-organized security communities are also linked to state actions, such as evidence gathering for prosecution. Typically, "a norm governs socially salient behaviour,

[3] *See* Poulsen, note 74 above. I have attended Ruxcon and have viewed video sessionss from Chaos Club, Blackhat and Def Con.

deviation from which makes you socially abnormal."[4] The high levels of botnet and malware proliferation undermine the notion of malicious programming as "socially abnormal". Arguably, malware distribution in certain parts of the world is the norm. As Zenz, an expert on Russian cybercrime, articulates, "They see themselves as law abiding. They don't view what they're doing as wrong…. The Russian Minister of Information stated proudly 'our hackers are the best in the world'."[5] In Code, Lessig focuses predominantly on the role of architecture, as well as the role of indirect and direct regulation to shape architecture. In later books such as the Future of Ideas, Free Culture and Remix the focus is extended to markets and online commerce in general. Norms are not a modality given a great deal of attention in his works with the exception his detailed analysis of the copyright industry and, in particular, to the social norms developed in online file-sharing through peer-to-peer networks. Lessig's work on copyright, however, is neither relevant nor helpful in exploring social norms in the current context. More explanation of what social norms might entail is required.

The inability of Lessig's theory to adequately account for botnets suggests that an alternative model is required. Two possible ways forward are outlined below.

9.3.1 Expansion of Lessig's Notions of Norms and Markets

This approach would involve expanding Lessig's notions of "Norms "and "Markets". Any new articulation of norms would need to better encapsulate the workings self-help remedies, especially the works of SOSCs. It is challenging to find a parallel where norms in any context have been so widely stretched. Indeed, retrofitting self-help remedies into norms may not prove feasible without completing distorting the term.

The modality of markets though less challenging than norms, still requires re-articulation so as to include non-traditional incentives where the market does not exclusively regulate through price, supply and demand, and competitive practice, but also to include reputation enhancement which *may* lead to commercial benefit in the future.

An exposition of norms by Ellickson is provided below to better understand the components of what is meant by norms.

[4] Lessig, note 1 above, page 235.
[5] Zenze, note 73 above.

In 1991 Ellickson published a seminal book which postulated a new theory of norms, *Order Without Law*.[6] In his book, Ellickson spent a period of time studying the cattle industry in Shasta County, and specifically, how disputes are settled between neighbours for cattle-trespass damages. Ellickson arrived at three broad conclusions. The first, "that people frequently resolve their disputes in a cooperative fashion without paying any attention to the laws that apply to those disputes." The second, that disputes were most frequently settled through a set of informal norms even when the parties concerned were aware that such norms were inconsistent with the law. And third, the close-knit cattle community generated informal norms that maximized the welfare of the group. Put more concretely by Ellickson, his hypothesis was that "members of a close-knit group develop and maintain norms whose content serves to maximize the aggregate welfare that members obtain in their workday affairs with one another."[7] He implies that his theory is not new citing many examples of those who have put forth a similar hypothesis. One broad example given is that "good-news" newspapers have not found a market simply because successful close-knit cooperative interactions occur far too often to be newsworthy.[8] What differentiates Ellickson's work from those who have come before him, such as George Edwin Pugh and Edna Ullmann-Margalit, and those who have come after him, such as Lawrence Lessig, is that Ellickson has not merely put forth a hypothesis but has tested his hypothesis through a detailed case study using hard data. The question relevant to this thesis, is the utility of Ellickson's theory of norms in the context of the botnet industry.

To what extent does Ellickson's theory of norms help us to understand how norms or the lack of norms affect the behavior of botnet masters? Ellickson's theory, while important, is based on the examination of close-knit groups where disputing parties are ranching neighbours. These are two distinguishing factors from the players active within the botnet industry: 1) not necessarily known to one another or known to one another through handles and 2) not physically adjacent. Disputes are not between neighbours in the physical sense of the word – that is people whose physical land and property are located next to or within a set physical boundary. Disputes occur between those individuals or organized crime groups who hack into computer systems using malware to commit crimes such as fraud, theft, assault and so forth. Those who respond to these problems, in most cases, do not know who they are fighting. In Ellickson's work, disputes arise between two or more parties who are known and adjacent physically to one another. This precondition does not exist in the context of combating botnets.

---

[6] Elickson, R., *Order Without Law: How Neighbors Settle Disputes* (Massachusetts: Harvard University Press, 1991).
[7] Ellickson, note 84 above, page 167.
[8] Ellickson, note 84 above, page 123.

Ellickson's theory contains a number of taxonomies. Only one taxonomy will be explored for the purpose of this chapter, who controls rules. This taxonomy is divided into three groups. First-party control actors are what Ellickson describes as personal ethics. Personal ethics form an individual's subjective ethical constraints to their behavior. For example, many people are vegetarians for ethical reasons. Abstaining from eating meat is not done because it is illegal. In the botnet context, a programmer may feel that it is ethical to steal but only from wealthy foreigners.

Second-party controllers stem from legal contracts. These are contractual provisions which outline restrictions of behavior. For example, my car may be worth $10 000 but if I agree to sell it to you for $2000 on the condition that you agree to let me use your pool facilities, then the contract provisions guide our transaction. As has been seen in **Chapter 3** using the case of botnet master aKill (Owen Walker), adware companies have detailed affiliate agreements that are meant to forbid software installs performed through malware and botnets, and where the user has not been given informed consent. These types of contracts, however, appear to have little impact on the behavior of programmers who by and large install unwanted software such as Dollar Revenue through exploits and botnets.

The last category, third-party controllers, may be divided into three subsets which include social forces whose rules are derived from norms, organizations whose rules derive from the organization's rules and governments whose rules flow from laws. We have already seen how norms might operate in the case of a botnet master in **section 3.4.5** – namely that norms do not appear to be a strong deterrent for the botnet master and that there appears to be a lack of community within the more skilled subsets of hackers who program alone. The rules from within an organization have not yet been explored. This would include an exposé of rules within a community, if one exists, of botnet masters who work for organized crime units. No such studies exist at this time, therefore, it is difficult to speculate on what rules are operative within this community. Governmental rules are seen to flow from the laws. In the case of botnet masters located in developing nations, it is often the case that nations have not criminalized computer misuse, have not ratified the *European Cybercrime Convention* mandating cooperation for cybercrime between member States, and is often the case, there simply isn't the political will or resources for governments to take action.

Borrowing on more detailed work on social norms from Ellickson does not shed much light on the matter. Ellickson's work is founded on two pre-existing conditions not present in the botnet industry: a close-knit community and physical proximity. A re-articulation of what is meant by norms in Lessig's theory is certainly a possibility but such re-articulation would have to accommodate these two pre-existing conditions that are simply not present within the botnet community.

9.3.2 Addition of Modality: Self-Help

The second alternative would be to add self-help as a new modality in Lessig's theory. The inability of traditional constraints such as market, norms, technologies and law enforcement to counter botnets, has led to the establishment of many self-organised anti-malware and anti-botnet communities. It was seen in **Chapters 1** and **3** that botnets were being used to commit crime in an unprecedented an unanticipated manner which were not predicted by early Internet scholars and industry players. Many of the former theories do not resonate well with what is currently seen both in terms of botnet proliferation, crime, and response to the problem.

The workings of self-organised security communities could be compared with that of self-help remedies where a community comes together to counter a problem. This is similar to the concept of neighbourhood watch groups who patrol communities in order to protect their households. In this instance, the actions of the neighbourhood watch communities are within the boundaries of the law. Neighbourhood watch groups are similar to the close-knit group of cattle ranch neighbours that Ellickson refers to in his depiction of norms. Where a neighbourhood watch community steps beyond the boundary of the law and actively defends their neighbour's property with physical force, and makes citizen's arrests, they move closer to the example of SOSCs in the botnet context. Within SOSCs there are three contrasting features than Ellickson's ranching community. First, members of a SOSC do not necessarily know one another. Many members communicate through a handle name. Second, there is no physical proximity of members of the group such as cattle ranch neighbours, or those members of a neighbourhood watch. Last, many countermeasures include illegal action such as unlawful data collection, or unauthorised access and modification of data or data systems. **Figure 9(B)** as seen below is one possible way of modifying Lessig's theory.

Figure 9(B) Self-Help Modality

The inclusion of a fifth modality, "Self-Help" would easily accommodate the actions of SOSCs, and does not place an undue strain on norms to accommodate what we are witnessing in combating botnets. Botnets has been the case study used in this thesis to highlight deficiencies in Lessig's theory but similar issues arise in the context of combating other types of cybercrime. Self-help groups have organised themselves to fight child pornography as seen with groups such as Perverted Justice and recently a sub-group of Anonymous known as Operation Darknet that took down the online server of Freedom Hosting . Freedom Hosting is notorious for hosting Lolita City which is an active forum in the exchange of child pornographic material.[9] The group further distributed the Internet Protocol addresses and names of those members of the group. This is particularly important given the group was able to identify users in spite of the fact that an anonymising proxy tool known as Tor was used by members to make traceback difficult. We even see self-help spilling into the classification of materials online. The Australian government in its review of the classification system is considering whether classification could be performed in real-time by online users interested in keeping the Internet safer.[10]

9.3.3 Theory and Practice

Regardless of what amendments are made to Lessig's theory it will do nothing to help the practical reality of the threat of botnets. Self-help modalities, and retrofitting of terms in Lessig's

[9] See Yin, S., "'Anonymous' Busts Child Porn Ring" (October 24, 2011) PC Magazine. Available at http://www.pcmag.com/article2/0,2817,2395175,00.asp#fbid=IKSEUVrwWUE.
[10] Discussion at Google Event, "Online Censorship" University of New South Wales (October 26, 2011).

theory may be considered mere badinage. Countermeasures against botnets have to date enjoyed limited success. Where an initiative has led to *relative* success, it has often been achieved by breaking the law. There are few if any botnet takedowns which have not, at some point in the operation, gathered personal information in contravention of privacy and data protection law, or accessed or modified data or a data system without authorisation. Respect for the rule of law and protection of civil liberties are the hallmarks of a democratic society. It is hard to reconcile breaking the law and impeding civil liberties to counter botnets with a successful operation. Combating botnets may work in an amended theory, but we are a long way from successfully tackling the problem in practice.

Appendix A

Dollar Revenue Affiliate Agreement

AFFILIATE AGREEMENT

Upon you agreeing to the terms and conditions of this Agreement by completing the online registration form, DollarRevenue.com (hereinafter "DollarRevenue"), grants to you (hereinafter "Affiliate") a limited, non-exclusive, royalty free license during the term of this Agreement to display DollarRevenue's exe code and use DollarRevenue Promotional Tools (hereinafter referred to individually or in combination as the "Tools") on Affiliate's web site only, and only in accordance with this Agreement. This Agreement shall append any existing agreements between the two parties.

This is a legal agreement between you and DollarRevenue. By signing up to our program you agree to have an understanding of these terms and conditions set forth herein. You cannot participate in our program unless you have accepted each and every term hereof.

Definitions

"DollarRevenue" means DollarRevenue partner interface materials, paper or electronic documentation, trademarks, service marks, and trade names as made available by DollarRevenue to its Affiliates from time to time.

The "Affiliate" as stated above, is an individual or group that signs up for DollarRevenue's program and/or uses the DollarRevenue Promotional Tools.

The "Referred Affiliate" is an individual or group that signs up for DollarRevenue's program being referred by an Affiliate through his referral link, with the Affiliate account ID being recorded upon sign up.

�User� means a new unique end-user who installs DollarRevenue (either alone or in

connection with installations of third parties) on such user's computer through the install process of Affiliate, who has not previously installed DollarRevenue (either alone or in connection with installations of third parties), and whose installation is reported by DollarRevenue's tracking system as a valid installation.

Acceptable Use

Affiliate may use or display the Tools only in the size, place and manner DollarRevenue may indicate within DollarRevenue's Affiliate's web page and only in a manner that complies in all respects with DollarRevenue's guidelines as described herein or as may be modified in writing, or electronically, from time to time by DollarRevenue in its sole discretion. Affiliate acknowledges that all right, title and interest in the Tools is exclusively owned by DollarRevenue and/or its licensors, and is DollarRevenue's proprietary property, and that no right other than the limited display license granted herein is provided to Affiliate.

DollarRevenue does not accept any form of SPAM and detects/discards all traffic from unsolicited e-mail, newsgroups, messengers, unauthorized adjustment of default home page or search features within standard browser settings and all other methods other than that generated from an active human. Spamming by any of these methods will cause the responsible Affiliate account to be terminated. Only one account is allowed per company or organization unless agreed to in writing by DollarRevenue, however, Affiliate may use this account for multiple domains and/or websites.

Without limitation, Affiliate's account may be terminated, where DollarRevenue in its sole discretion, determines that any content, goods, services, or links displayed on or made available through or in connection with Affiliate's Web site(s) are illegal, obscene, indecent, vulgar, offensive, dangerous, or are otherwise deemed inappropriate; or that Affiliate or Affiliate's web site(s) violates, has violated, or threatens to violate the terms and conditions of this Agreement or the spirit behind them.

The action of sending any hits from any URLs which contain and/or promote the following content: warez, MP3s, ROMs, EMUs, newsgroup postings, SPAM e-mails, or any other site which contains content or promotes activities which are illegal in the United States of America

will result in the immediate cancellation of the account from which the hits were sent and the forfeiture of any funds owed to that account.

Affiliate who wishes to install DollarRevenue by use of an executable file (bundled or attached to his own program) must abide by DollarRevenue's Distribution Code of Conduct Agreement:

Affiliate agrees to notify users about the installation of DollarRevenue's product before installing the application on the end user's computer and to give such end user an effective method of avoiding installation. DollarRevenue reserves the right to approve final wording of this notification and to require periodic changes as necessitated by changes to DollarRevenue's product or for other business reasons.

Each installation of DollarRevenue product by Affiliate must include and be subject to DollarRevenue product End User License Agreement (EULA), and Affiliate must obtain the informed consent from the end user to such EULA prior to installation. Our EULA is located at www.DollarRevenue.com/eula.asp

Affiliate is responsible for the actions of their partners and affiliates, and will ensure that appropriate messaging and EULA acceptance precedes every installation that is credited to their account. If the Affiliate discovers a partner or affiliate is in violation of these requirements the Affiliate agrees to call such action to the attention of DollarRevenue and to immediately terminate distribution with that partner or affiliate. If DollarRevenue discovers independently that the Affiliate, their partner or affiliate has failed to provide appropriate notification and EULA acceptance, in DollarRevenue's sole discretion, DollarRevenue may withhold payment for the current month's installations, terminate the AFFILIATE AGREEMENT or any other agreements between the parties, with cause, and take legal action against the Affiliate, their partner, or affiliate to recover damages.

The foregoing shall in no way limit the legal or equitable rights or remedies available to DollarRevenue in connection with a violation of the above requirements, or otherwise.

Affiliate may not install DollarRevenue by any type of automatic installs, browser exploits, viruses, bots or by any other means not previously approved by DollarRevenue. Affiliate may

not promote any competing programs at the same time as promoting DollarRevenue and using its Tools. If DollarRevenue discovers independently that the Affiliate, their partner or affiliate has failed to comply by the Acceptable Use, in DollarRevenue's sole discretion, DollarRevenue may withhold payment for the current month's installations, terminate the AFFILIATE AGREEMENT or any other agreements between the parties, with cause, and take legal action against the Affiliate, their partner, or affiliate to recover damages. The foregoing shall in no way limit the legal or equitable rights or remedies available to DollarRevenue in connection with a violation of the above requirements, or otherwise.

Any attempted fraud, fraud or suspicion of fraud will result in membership termination, voided commissions, and legal action.

Affiliate's Responsibility

Affiliate shall provide users of Affiliate's web site the possibility to install ad-distribution programs.

Affiliate shall not modify the Tools, which is herein licensed to Affiliate. Affiliate is solely responsible for the creation and maintenance of its own web site and for all contents that appears on Affiliates web site. Affiliate may not reference DollarRevenue, its directors or its parent companies in any way without first receiving written consent from DollarRevenue. Affiliate may not issue any press release or other public statements regarding this Agreement without DollarRevenue's prior written consent.

Compensation

DollarRevenue will pay Affiliate a commission based on User installations performed through the Affiliate ID. DollarRevenue reserves the right not to pay for installations coming from certain countries if they are not profitable to DollarRevenue.

Payout rates depend on the package that DollarRevenue chooses for the Affiliate. All packages have different payout rates for every country. DollarRevenue reserves the righ to change the package and/or payment rates at any time without notice.

Payments are sent 15 days after the end of the pay period. A pay period is one calendar month. Payment is equal to the total showed in Affiliate's account less any taxes or fees DollarRevenue may be required to withhold, and less any amount DollarRevenue determines, in its sole discretion, was not validly earned from proper use of the Tools on Affiliate's site. Affiliates are responsible for keeping their payment information up to date. Payments will be sent with the payment information located in the Partners Area at the time the pay period ends. No payment information change will be accepted between the end of the pay period and the time the payment is sent. Future payments will take account of any changes made during that time.

DollarRevenue will issue payment once Affiliate's account balance has reached two hundred and fifty ($250). If the amount is less it is carried over from month to month until Affiliate has accrued the minimum payout. DollarRevenue agrees to pay a referral bonus to Affiliate for all installations sent by Referred Affiliate. The referral bonus is equal to ten (10) percent of the referred webmaster's net revenue.

Methods of promotion

Affiliate agrees to follow DollarRevenue's promotion methods given on DollarRevenue's website. The use of inappropriate promotion methods by the affiliate will result in the immediate cancellation of the account from which the hits were sent and the forfeiture of any funds owed to that account. If you wish to modify the standard code in any way please contact us for approval. Failure to do so will result in account cancellation.

If requested by DollarRevenue, Affiliate has to provide all desired data to show how the DollarRevenue software is installed and who the users are. If Affiliate does not cooperate it will result in membership termination, voided commissions, and legal action.

Ownership of Tools

Affiliate agrees that this limited license to display DollarRevenue's Tools inures to the benefit of DollarRevenue. All good will or reputation generated by the display of DollarRevenue Tools shall automatically vest in and shall remain the property of DollarRevenue. Affiliate agrees not

to contest, in any court or other jurisdiction, the validity of any of the DollarRevenue Tools, including, but not limited to, DollarRevenue's trademarks, service marks or trade names. In so far as access to the use of any DollarRevenue software is granted herein such grant excludes any rights to any source code. For greater certainty, rights not expressly granted herein are reserved by DollarRevenue. During the term of this Agreement, Affiliate shall not adopt, use, register, or apply for registration of, whether as a corporate name, trademark, service mark or other indication of origin, any of the DollarRevenue trademarks, service marks or trade names, or any word or mark confusingly similar to them in any jurisdiction.

Email contact

DollarRevenue reserves the right to send e-mail to Affiliate for the purposes of informing you of applicable changes or additions to the Service or any DollarRevenue.com related products and services.

Representations and Warranties

A. As to DollarRevenue:

DollarRevenue represents and warrants that it has the authority to enter into this Agreement.

B. As to Affiliate:

Affiliate represents and warrants that he is 18 years or older and that he has full power and authority to enter into this Agreement; and Affiliate represents and warrants that the content on Affiliate's web site, and/or the technology used by Affiliate in connection with this Agreement are owned or legally licensed for use by Affiliate; and Affiliate represents and warrants that its web site does not violate applicable law or regulations and does not infringe or violate any copyright, patent, trademark or other similar Tools right, or otherwise violate or breach any duty toward, or rights of any person or entity.

Non-Liability of DollarRevenue

DollarRevenue does not warrant or represent that the Tools will meet all or any of Affiliate's

needs or requirements, or that performance of DollarRevenue's Tools will be uninterrupted or error free. DollarRevenue is not responsible for any content provided by third parties, including advertisers, or for any third party sites that can be linked to/from the Tools. DollarRevenue and its licensors make no other warranty of any kind, whether expressed or implied, including without limitation, warranties of merchantability, fitness for a particular use, and non-infringement.

Confidentiality

During the term of this Agreement, Affiliate may have access to certain non-public information of DollarRevenue, which information a reasonable person would consider confidential or which is marked as "confidential" or "proprietary" by DollarRevenue, collectively "Confidential Information". This Confidential Information does not include information that is generally in the public domain. Affiliate agrees not to disclose any Confidential Information to any third parties or to use any Confidential Information for any purposes except to carry out its obligations under this Agreement. Affiliate shall take every effort to keep such Confidential Information confidential, using the same degree of care Affiliate uses to protect its own confidential information, as long as it uses at least reasonable care. Each party acknowledges and agrees that due to the unique nature of the Confidential Information, any such breach may allow one party or third parties to unfairly compete with the other party resulting in great harm to non-breaching party.

This Agreement shall be governed by Dutch law and in the event of a dispute, Affiliate agrees to submit to the jurisdiction of the courts located in the Netherlands.

Indemnification

Affiliate shall indemnify, defend and hold DollarRevenue harmless (including DollarRevenue's legal and expert fees) against any and all damages, claims and awards brought or assessed against DollarRevenue, resulting from a breach of any warranty, representation or covenant made by Affiliate under this Agreement; or arising from any action against DollarRevenue arising from Affiliate's use or display of DollarRevenue's Tools or arising from any breach by Affiliate of any of the provisions or requirements of this Agreement, provided that DollarRevenue promptly notifies Affiliate in writing of any such

claim and promptly tenders the control of the defense and settlement of any such claim to Affiliate at Affiliate's expense and with Affiliate's choice of counsel. DollarRevenue shall cooperate with Affiliate, at Affiliate's expense, in defending or settling such claim. Affiliate will not enter into any settlement or compromise of any such claim without DollarRevenue's prior consent, which shall not be unreasonably withheld.

Limitation of DollarRevenue's Liability

In no event shall DollarRevenue's liability arising out of this Agreement exceed the net amount payable to Affiliate under this Agreement during the three (3) months prior to the date of such cause. DollarRevenue shall not be liable hereunder by reason of any failure or delay in the performance of its obligations on account of strikes, shortages, riots, insurrection, fires, flood, storm, explosions, earthquakes, Internet outages, acts of God, war, governmental action, or any other cause that is beyond the reasonable control of DollarRevenue.

Term

The term of this Agreement shall commence on the date DollarRevenue receives Affiliate's registration and shall continue in force thereafter, unless earlier terminated as provided herein. If Affiliate breaches this Agreement, or if Affiliate engages in any action that, in DollarRevenue's sole discretion, reflects poorly on DollarRevenue or its trademarks, service marks, trade name or reputation, DollarRevenue may terminate the Agreement immediately without notice to Affiliate.

Either party may terminate this Agreement on thirty (30) days written notice to the other party for any reason. Upon the termination of this Agreement for any reason, all license rights granted herein shall terminate immediately, and Affiliate shall immediately cease use of the Tools and of all DollarRevenue's trademarks, service marks and trade names incorporated in the Tools. DollarRevenue reserves the right to terminate any account if it is inactive for more than 14 calendar days.

DollarRevenue reserves the right to terminate the account of any Affiliate who publicly posts derogatory and/or slanderous statements about DollarRevenue, or any of its subsidiaries or officers. Any artificial means of generating traffic including, but not limited to, hitbots,

multiple clicking scripts, hidden links and incentivizing surfers in any way or any other similar activity will result in forfeiture of all money owed and possible criminal prosecution. Affiliate must have all referring pages written entirely in English. Non-compliance with these terms and conditions may result in the forfeiture of all money owed and permanent locking of account.

Notices

Any notice required for or permitted by this Agreement relating to the Affiliate shall be in writing and shall be delivered by personal delivery, by overnight courier, by certified or registered mail; or by email. Visit www.DollarRevenue.com for the correct contact email-adress. All notices must be sent to the addresses first described above, or to such other address that DollarRevenue may have provided for the purpose of notification in accordance with this Agreement.

Changes to Agreement

DollarRevenue may change this Agreement at any time. Any use of the Tools after such notice shall be deemed to be continued acceptance of this Agreement including its amendments and modifications.

Assignment

DollarRevenue may assign its rights or delegate its obligations under this Agreement without Affiliate's prior written consent, as long as the assignee expressly assumes in writing the performance of all of the terms of this Agreement.

Relationship of Parties

This Agreement shall not be construed to create a joint venture or partnership between the parties. Neither party shall be deemed to be an employee, agent, partner nor legal representative of the other for any purpose and neither shall have any right, power or authority to create any obligation or responsibility on behalf of the other.

Account information

Should any law enforcement agency, any internet service provider or other person or entity provide DollarRevenue with notice that you have engaged in transmission of unsolicited emails or have engaged in otherwise unlawful conduct or conduct in violation of any internet service provider's terms of service, we reserve the right to cooperate in any investigation relating to your activities including disclosure of your account information.

Entire Agreement

This Agreement constitutes the entire understanding between the parties with respect to the subject matter and supersedes all previous agreements, written or oral, between Affiliate and DollarRevenue. If any provision of this Agreement is held or made invalid or unenforceable for any reason, such invalidity shall not affect the remainder of this Agreement.

Non-Waiver

The terms or covenants of this Agreement may be waived only by a written instrument executed by the party waiving compliance. The failure of either party at any time or times to require performance of any provision hereof shall in no manner affect the right at a later time to enforce the same. No waiver by either party of the breach of any term or covenant contained in this Agreement, whether by conduct or otherwise, in anyone or more instances, shall be deemed to be, or construed as, a further or continuing waiver of any such breach or a waiver of the breach of any other term or covenant contained in this Agreement.

Section Headings

The section headings contained herein are for reference purposes only and shall not in any way affect the meaning or interpretation of this Agreement.

ANY ATTEMPTED FRAUD, FRAUD OR SUSPICION OF FRAUD WILL RESULT IN MEMBERSHIP TERMINATION, VOIDED COMMISSIONS, AND LEGAL ACTION.

THIS IS A LEGAL AGREEMENT BETWEEN YOU AND DOLLARREVENUE. BY SIGNING

UP TO OUR PROGRAM YOU AGREE TO HAVE AN UNDERSTANDING OF THESE TERMS AND CONDITIONS SET FORTH HEREIN. YOU CANNOT PARTICIPATE IN OUR PROGRAM UNLESS YOU HAVE ACCEPTED EACH AND EVERY TERM HEREOF.

APPENDIX B

Cyberspace Law and Policy Centre Domain Name Service Providers for the .au domain space (Registrars, Resellers and Registries)

Name of auDA-accredited registrar	**Does the registrar advertise for resellers or offer a reseller program?**	**(If YES): Is the registrar's agreement with resellers and registrants available?**	**Link to registrar's agreements with resellers/registrants, or general Terms & Conditions, if available on registrar's website**	**(If NO reselling program): General client Terms & Conditions, or registrant agreement**	**Notes about availability**
Anchor Systems Pty Ltd	YES	YES	http://www.anchor.com.au/reseller-web-hosting/reseller-hosting-reseller.py		
AussieHQ Pty Ltd	YES	YES	http://aussiehq.com.au/registrantagreement http://aussiehq.com.au/terms		Links given upon email request. All customers must agree to Registrant agreement, including resellers, and to the standard terms and conditions. This is all they require for domain name resellers to resell domain names under their .au accreditation.
Aust Domains Pty Ltd	YES	YES	http://policy.secureapi.com.au/reseller.html		
Cheaper Domains Pty Ltd	NO			Complaints policy: http://www.cheaperdomains.com.au/hspc/complaints-policy.php	
Connect West Pty Ltd (trading under **iiNet.net.au**)	NO		http://www.connectwest.net.au/termsconditions/tncagree.html		"Sorry to say we don't have a reseller agreement at this stage. For further queries please call 1300 378 638." – response to email request

Discount *Domain Name* Services Pty Ltd	YES	NO			Only a manual reseller agreement, no pdf or electronic copy. Will only show to potential resellers upon application and with provision of more information.
DistributeIT Pty Ltd trading as **Click'nGo**	NO			.au registrant agreement: http://distributeit.com.au/Agreements/agreement%20au.pdf gTLD registrant agreement: http://distributeit.com.au/Agreements/agreement%20com_net_org.pdf Dispute resolution policy (ICANN's): http://www.icann.org/en/udrp/udrp-rules-24oct99.htm	
Domain Candy Pty Ltd	YES – but they haven't actually signed any resellers on for years	YES	http://www.domaincandy.com.au/registrant_agreement.pdf		They do have a reseller program advertised, through which they provide domain names for the reseller to sell on to individual clients. However, after a quick phone call I discovered that they don't currently have any resellers, and haven't had for years. The representative couldn't find a copy of their old reseller agreement. The general registrant agreement was available online.
Domain Central Pty Ltd	YES	YES – but only in the form of a general registrant agreement	Link to all agreements and policies: http://www.domaincentral.com.au/service/		After contacting a representative through their live chat function, I was given a link to a page containing all their agreements and policies. This page seems to be inaccessible from anywhere else on the site (that is, there is no link to this page from anywhere else) except from the site map.
Domain Directors Pty	YES	EMAILED REQUEST FOR	T&C: http://www.instra.com/en		

Ltd trading as **Instra**		RESELLER AGREEMENT	/about-us/Terms-Conditions		
Domain8 Pty Ltd	NO			http://www.domain8.com.au/termsandconditions.php	
Domain Name Registrar (Australia) P/L T/A **Domain Registration Services**	NO			Policies: https://www.domainregistration.com.au/policies/	
Enetica Pty Ltd	YES		.au Registrant Agreement: http://www.enetica.com.au/tc.html gTLD Registrant Agreement: http://www.enetica.com.au/docs/gtld_doc.html		Links given upon email request.
Explorer Domains Pty Ltd	YES	EMAILED REQUEST FOR RESELLER AGREEMENT	T&C: http://www.explorer.net.au/show.php?f=terms		
Fabulous.com.au trading as **Drop.com.au**	NO			Customer Agreement Secondary Market Auction DN Listing Agreement Expiring and Deleted DN Auction Agreement	Drop operates as an auction platform for expiring and deleted domain names, and is a reseller for Domain8, DomainCandy, and NetStart, whose terms the auction bid winners must abide by. This implies that the domain names auctioned are those that are about to be purged from the registries of either of those three registrars because they are either deleted or expired, and are thus available for new owners/licencees. The agreements are available on Drop's website.
Hostess.com.au Pty Ltd	NO			Terms http://www.hostess.com.au/terms.php	Hostess does not offer

				Rules of registration http://support.hostess.com.au/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=30&nav=0,4	reseller/wholesale services.
IntaServe Pty Ltd	YES	YES – in the form of general registrant agreements	Registrant Agreements: http://www.intaserve.com/domainnames/terms-and-conditions.asp T&C: http://www.intaserve.com/about-us/terms-and-conditions.asp		Email request for specific reseller agreement sent, reply received but no agreement sent.
InternetX GmbH	YES		T&C (in German only): http://www.internetx.com/en/footer/terms-and-conditions.html Standard contract: InterNetXDomainPartnerAgrmt.pdf		
MD Web Hosting Pty Ltd	NO	No reseller agreement	T&C: http://www.mdwebhosting.com.au/tc.html	http://www.mdwebhosting.com.au/registrantagreement.html	"MD Webhosting do not offer a reseller program, we previously did offer something similar which was referred to as reseller hosting but this is no longer available." – response to email request for agreement
MelbourneIT	YES	YES – in the form of general registrant agreements (see right).	Affiliate T&C: http://www.melbourneit.com.au/policies/affiliate-terms-conditions.php List of all agreements and policies: http://www.melbourneit.com.au/policies/index		No response to email request for specific reseller agreement, but it is likely that resellers must agree to one or more of the general agreements.
Namescout Corporation	NO			http://www.namescout.com/TermsAndConditions.aspx	
NetRegistry Pty Ltd	YES		http://www.netregistry.com.au/terms-conditions/		

			(scroll down to Reseller & ISP Partner)		
Planet Domain Pty Ltd	YES		https://whitelabel.planetdomain.com/reseller/planetdomain/Agreement.html		
Safenames Ltd	YES	EMAIL REQUEST again FOR RESELLER AGREEMENT	T&C: http://www.safenames.net/MoreResources/TermsConditions.aspx		
SmartyHost Pty Ltd	NO			Terms of use, incl. T&C and Warranty Statement: http://www.smartyhost.com.au/terms.php	
SublimeIP Pty Ltd trading as **Go Domains**	NO			http://www.sublimeip.com/legal/terms/	
TPP Domains Pty Ltd	YES	YES	http://tppinternet.com.au/terms-conditions/general-terms-conditions.php		This link was given upon email request for the reseller agreement, with the note: "[This is] a page of links that contain all of our publicly accessible policy statements". It is likely that resellers agree to these general terms.
VentraIP	YES	YES	All agreements: http://www.ventraip.com.au/tpa/ VentraIP Terms of Service VentraIP .au Registrant Agreement		Will have resellers in future (working on reseller platform/interface) Agreements available on website
WebAccess Pty Ltd	YES	YES	auDA policies http://www.auda.org.au/policy/current-policies/		This link was given upon email request for the reseller agreement, with the note: "Although we do have resellers, we currently do not have a dedicated reseller system and corresponding prices or seperate web interface etc that would normally be associated with this kind of arrangement. Plans to implement such a seperate system

					and make all resellers enter into a formal agreement before access is given to such systems are in place, however currently our resellers just use the normal retail interface we have for all clients. Essentially our resellers are just normal retail clients currently, but get a discount on all services and provide their own support systems, in terms of policy we ask only that they abide by our normal agreements and the relevant published policies that relate, eg. for .au domains, those viewable at: http://www.auda.org.au/policy/current-policies/ Otherwise we check all registrations/transfers as normal to see they comply with policy and ask that our resellers have a valid written authority from any domain Registrant they are representing, as well as warrant this to us, when they are dealing with us on behalf of a domain Registrant."
Westnet Pty Ltd	NO			http://www.westnethosting.com.au/about-us/legal/registrant-agreement.aspx	

Appendix C Email Discussions of OID (this appendix will not be included in the formal PhD publication)

Appendix D http://www.bittorrent.com/legal/bittorrent-eula (February 2011)

BitTorrent End User License Agreement

BitTorrent is a peer-to-peer file sharing application distributed by BitTorrent, Inc.

By accepting this agreement or by installing BitTorrent, you agree to the following BitTorrent-specific terms, notwithstanding anything to the contrary in this agreement.

1. License.

Subject to your compliance with these terms and conditions, BitTorrent, Inc. grants you a royalty-free, non-exclusive, non-transferable license to use BitTorrent, solely for your personal, non-commercial purposes. BitTorrent, Inc. reserves all rights in BitTorrent not expressly granted to you here.

2. Restrictions.

The source code, design, and structure of BitTorrent are trade secrets. You will not disassemble, decompile, or reverse engineer it, in whole or in part, except to the extent expressly permitted by law. **You will not use BitTorrent for illegal purposes**. You will comply with all export laws. BitTorrent is licensed, not sold.

3. The BitTorrent Technologies.

a. Downloading and Updates.

BitTorrent downloads only those files that are both authorized by you for download (specifically or by category or subscription), except that BitTorrent automatically updates itself.

b. Automatic Uploading.

BitTorrent accelerates downloads by enabling your computer to grab pieces of files from other BitTorrent or BitTorrent users simultaneously. Your use of the BitTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In BitTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall BitTorrent through the Add/Remove Programs control panel utility. In addition, you can control BitTorrent in multiple ways through its user interface without affecting any files you have already downloaded.

4. Disclaimer of Warranty.

BitTorrent, Inc. disclaims any responsibility for harm resulting from BitTorrent or any software or content downloaded using BitTorrent, whether or not BitTorrent, Inc. approved such software or content. BitTorrent, Inc. approval does not guarantee that software or content from an approved partner will function, sound, or appear as offered or hoped, or be complete, accurate, or free from bugs, errors, viruses, or other harmful content. BitTorrent Inc expressly disclaims all warranties and conditions, express or implied, including any implied warranties and conditions of merchantability, fitness for a particular purpose, and noninfringement, and any warranties and conditions arising out of course of dealing or usage of trade regarding the BitTorrent software or any software or content you download using the BitTorrent software. No advice or information,

whether oral or written, obtained from BitTorrent Inc or elsewhere will create any warranty or condition not expressly stated in this agreement. Some jurisdictions do not allow certain limitations on implied warranties, so the above limitation may not apply to you to its full extent.

5. Limitation of Liability.

BitTorrent Inc's total liability to you from all causes of action and under all theories of liability will be limited to $50.00. In no event and under no theory of liability will BitTorrent Inc be liable to you for any special, incidental, exemplary, or consequential damages arising out of or in connection with this agreement or the software whether or not BitTorrent Inc has been advised of the possibility of such damages. The foregoing limitations will survive even if any limited remedy specified is found to have failed of its essential purpose. Some jurisdictions do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you to its full extent.

6. U.S. Government Users.

BitTorrent is "commercial computer software" any use of which by or on behalf of the U.S. Government is subject to the restrictions herein. Manufactured by BitTorrent, Inc.

7. General.

These BitTorrent, Inc. terms will be governed by and construed in accordance with the laws of California, USA, without regard to conflicts of law rules. The United Nations Convention on Contracts for the International Sale of Goods will not apply. The failure by either party to enforce any provision will not constitute a waiver. Any waiver, modification, or amendment of the BitTorrent, Inc. terms will be effective only if signed. If any provision is held to be unenforceable, it will be enforced to the maximum extent possible and will not diminish other provisions. BitTorrent, Inc. may make changes to these terms from time to time. When these changes are made, BitTorrent, Inc. will make a new copy of the terms available at this URL (http://www.bittorrent.com/legal/bittorrent-eula). You understand and agree that if you use BitTorrent after the date on which the terms have changed, BitTorrent, Inc. will treat your use as acceptance of the updated terms. You agree that BitTorrent, Inc. may provide you with notices, including those regarding changes to the terms, by postings at this URL (http://www.bittorrent.com/legal/bittorrent-eula). This is BitTorrent, Inc.'s complete and exclusive understanding with you regarding your use of BitTorrent as an end user.

8. Contact.

If you have any questions, please visit the µTorrent user forums at http://forum.utorrent.com/ or email help@bittorrent.com.

BIBLIOGRAPHY

Legislation and Treaties

Berne Convention for the Protection of Literary and Artistic Works 828 UNTS 222 (1970).

Broadcasting Service Act 1992 (Cth).

Communications Legislation Amendment Act (No 1) 2004 (Cth).

Communications Legislation Amendment (Content Services) Act 2007.

Competition and Consumer Act 2010 (Cth).

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

Copyright Act 1968.

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

Criminal Code 1995 (Cth).

Criminal Code 1899 (Queensland).

Criminal Code 1922 (Tasmania).

Criminal Code 1902 (Western Australia).

Fair Trading Act 1987 (NSW).

Marrakesh Agreement Establishing the World Trade Organization 1867 UNTS 3 (1995).

Model Criminal Code (January 2001).

Paris Act relating to the Berne Convention for the Protection of Literary and Artistic Works 1161 UNTS 30 (1972).

Privacy Act 1988 (Cth).

Regulation of Investigatory Powers Act 2000 (UK).

Sarbanes-Oxley Act 2002 , 15 U.S.C.§ 7241 (civil sections) and 18 U.S.C. § 1350 (criminal provisions).

Spam Act 2003 (Cth).

Telecommunications Act 1997.

Telecommunications Amendment Act 1997 (Cth).

Telecommunications (Interception and Access) Act 1979.

Telecommunications (Interception and Access) Amendment Act 2007 (Cth).

Telecommunications (Interception and Access) Bill 2009.

Trade Practices Act 1974 (Cth).

World Intellectual Property Organization Copyright Treaty, 2186 UNTS 121 (2002).

Caselaw

1-800 Contacts v WhenU.

1-800 Solutions v. Zone Labs.

ACCC v. Channel 7 Brisbane [HCA] 19.

ACCC v. Henry Kaye [2004] FCA 1363.

Adelaide Company of Jehova Witnesses Inc. v Commonwealth [1943] HCA 12.

Amlink Technologies and Australian Trade Commission [2005] AARA 359.

ASIS Internet Services v. Optin Global, et al., United States District Court for the Northern District of California (2007) No. C-05-05124 JCS.

Australian Competition and Consumer Commission v Chen (2003) 132 FCR 309.

Australian Style Pty Ltd v .au Domain Administration Limited [2009] VSC 422.

Australian Style Pty Ltd v .au Domain Administration Ltd [2010] VSCA 184.

Cassav (CasinoOnNet) v Sunbelt Software.

Catch the Fire Ministries Inc v Islamic Cuncil of Victoria Inc [2006] VSCA 284.

Clayton v R [2006] HCA 58.

Concrete Constructions (NSW) Pty Ltd v. Nelson [1990] HCA 17.

DPP v Sutcliff [2001] VSC 43.

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.

Gillard v R [2003] HCA 64.

Gilmour v Director of Public Prosecutions (1995) 43 NSWLR 243.

Glaria (Gator) v Internet Advertising Bureau.

Hayes v The Queen [2006] New Zealand Court of Appeal 318.

Johnston v Commissioner of Police [2007] NSWIR Comm 73.

Lange v ABC (1997) 189 CLR 520.

McAuliffe v The Queen [1995] 183 CLR 108.

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

McEwen v Simmons (2008) 73 NSWLR 10.

Michael Brown v Members of the Classification Review Board of the Office of Film and Literature [1998] FCA 319

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).

Mulholland v Australian Electoral Commission (2004) 220 CLR 181.

Nader v. General Motors Corp., (1970) 255 New York 2nd Division 765.

NSW Council for Civil Liberties Inc. v Classification Review Board (No. 2) [2007] FCA 896

Peters v The Queen (1998) 192 CLR 493.

Pilmer v Roberts (1997) 80 FCR 303.

ProCD, Inc. V Zeidenberg (1996) 86 Federal Court 3rd District 1447 (7th Circuit).

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

Roadshow Films Pty Limited v iiNet Limited [2011] FCAFC 23.

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.

Seven Network Ltd. v News Interactive Pty Ltd [2004] FCA 1047.

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.

Software Integrators Pty Ltd v Roadrunner Couriers Pty Ltd (1997) ATPR (Digest) Supreme Court of South Australia.

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

The Queen v LK; The Queen v RK [2010] HCA 17.

Theophanous v Herald & Weekly Times Ltd. (1994) 182 CLR 104.

Ticketmaster Corp, v Tickets.com, Inc., (2003) WL 21406289 Central District California.

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

University of New South Wales v Moorhouse [1975] 133 CLR 1.

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.

BLACKSHIELD and WILLIAMS, G., *Australian Constitutional Law and Theory* 4th ed (Federation Press, 2008).

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

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

BROWN, D., FARRIER, D., EGGER, S., MCNAMARA, L. and STEEL, A., *Criminal Laws: Materials and Commentary on Criminal Law and Process of New South Wales 4th ed.* (The Federation Press: 2006).

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).

DEFLEM, M., "The Origins of Interpol" in *Policing World Society: Historial Foundations of International Police Cooperation* (Oxford University Press, 2004).

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

ELICKSON, R., *Order Without Law: How Neighbors Settle Disputes* (Massachusetts: Harvard University Press, 1991).

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).

FOUCAULT, M., *Discipline and Punish: the Birth of the Prison* (New York: Random House, 1975).

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

GARRISON, O, *The Secret World of Interpol* (New York: Ralston-Pilot, 1976).

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. *Gray Hat Hacking: The Ethical Hacker's Handbook* (McGraw Hill 2008).

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).

LESSIG, L., *Code: And Other Laws of Cyberspace* (Basic Books, 1999).

LEVY, S. *Hackers: Heroes of the Computer Revolution* (New York: Doubleday, 1984).

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).

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).

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).

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).

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).

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).

WATERS, N. "Government Surveillance in Australia" in RULE, J. (ed) *Privacy under Pressure* (2006).

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

BANNON, A., "Cybercrime Investigation and Prosecution: Should Ireland Ratify the Cybercrime Convention?" (2007) 3 *Galway Student Law Review* 115, page 132.

BENSON, B., "The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement Without the State" (2005) 1(1) Journal of Law, Economics and Policy 269.

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 J*ournal 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.

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.

GANDHI, M., and JAKOBSSEN, M., "Bad Advertisements: Stealthy Click-Fraudwith Unwitting Accessories" (2006) *Journal of Digital Forensics Practice*, Volume 1 available at http://www.informaworld.com/smpp/content~db=all ~content=a762491449 (last accessed July 1, 2010).

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*.

GOMULKIEWICZ, R., "The License is the Product: Commonets on the Promise of Article 2B for Software and Information Licensing," (1998) 13 *Berkeley Technology Law Journal* 891.

GREENLEAF, G., "An Endnote on Regulating Cyberspace: Architecture vs. Law" (1998) 21(2) *University of New South Wales Law Journal* 52.

GUZMAN, L., "Unleashing a Cure for the Botnet Zombie Plague" (2010) 59 *Catholic University Law Review* 527.

HARDY, K., "Operation Titstorm: Hacktivism or Terrorist Act?" (2010) *University of New South Wales Law Journal* 16:1.

HUTCHINSON, W. And WARREN, M., "Attitudes of Australian Information System Managers Against Online Attackers" (2001) 9(3) *Information Management & Computer Security* 106.

IGBINOVIA, P., "Interpol: A Survey of Research Findings" (1984) 7 *Police Studies: International Review of Police Development* 112.

JOHNSTON, L., "What is Vigilantism?" (1996) *British Journal of Criminology*, vol. 26, No. 2.

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., "Constitution and Code"'(1996-7) 27 *Cumberland Law Review* 1.

LESSIG, L., "Intellectual Property and Code"(1996) 11 *St John's Journal of Legal Commentary* 3.

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.

LESSIG, L., "The New Chicago School" (1998) 27 *Legal Studies* 661.

LIN, P., "Anatomy of the Mega-D Takedown" (December, 2009) 12 *Network Security*, pages 4-7.

LITVAK, K., "Sarbanes-Oxley and the Cross-Listing Premium" (2007) 105 *Michigan Law Review*.

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.

MCGRANE, B., "The Audit Committee: Director Liability in the Wake of the Sarbanes-Oxley Act and *Tello v. Dean Witter Reynolds*" (2008-2009) 18 *Cornell Journal of Law & Public Policy*.

MCQUILLAN, J., FALK, G. and RICHER, R., "A Review of the Development and Performance of the ARPANET Routing Algorithm," *IEEE Transactions on Communications*, Vol. COM-26, December 1978.

MOLLETT, S., "Sarbanes-Oxley 307 Domestically and Abroad: Will Section 307 Lead to International Change?" (2008-2009) 11 *Duquesne. Business Law Journal.*

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.

POST and JOHNSON, "Law & Borders – The Rise of Law in Cyberspace" (1995) 48 *Stanford Law Review* at 13.

RYCHLICKI, T. "Legal Issues of Criminal Acts Committed Via Botnets." (2006) *Computer and Telecommunications Law Review* 12(5), p. 163.

SALGADO, R., "The Legal Ramifications of Operating a Honeypot" (2005) *IEEE Magazine Security and Privacy*, vol. 1.

SCHRUERS, M. "The History and Economics of ISP Liability for Third Party Content" Vol. 88 *Virginia Law Review* 205.

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.

STEELE, A., "Describing Dishonest Means: The Implications Of Seeing Dishonesty As A Course Of Conduct Or Mental Element and the Parallels with Indecency", (2010) 31 *Adelaide Law Review* 7.

STEEL, A., "New Fraud and Identity-Related Crimes in New South Wales" (2010) *Judicial Officers Bulletin* 22.3, pages 18-22.

STEEL, A., "The Meaning of Dishonesty in Theft" (2009) *Common Law World Review*; 38(2).

TAMANAHA, B. "Socio-Legal Positivism and a General Jurisprudence" (2001) *Oxford Journal of Legal Studies*, Vol. 21, No.1.

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

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.

WEST, R., "Authority, Autonomy and Choice: The Role of Consent in the Moral and Political Visions in Franz Kafka and Richard Posner" (1985) *Harvard Law Review* 99(2).

WILBUR, KC, and ZHU, R., "Click Fraud" (March, 2009) *ACM Marketing Science* Volume 28, Issue 2.

WINN, J. "Are 'Better' Security Breach Notification Laws Possible?" (2009) *Berkeley Technology Law Journal* Volume 24:3.

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.

Websites and Articles Published Online

ACMA, "Spam" available at http://www.acma.gov.au/spam (last accessed March 21, 2011).

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.

Anonymous, website of information on Rob Soloway available at http://443164770858281952O-a-1802744773732722657-s-sites.googlegroups.com/site/sjwest01/broadcastspam.html?attachauth=ANoY7cpmIg82OvP9mKMCxMq5HfmzDusdBYThE248ncZYvEPYhELM5CzkoCUdS50ml0WRSY7V6GL0MqYFJoTyOjg-FK3sXmaOmMlIfWVEgPlqtrFFrxTGaoBBgxo_GXISt9Q3MmmKjMxKEY3L4SDpCjR1OCehGzHuPNBwadjQGDheH8bXsG65sEES1VqfZTyQQCaALzaYMROi&attredirects=0#31052007 (last accessed October 25, 2010).

Anti-Phishing Working Group, available at http://www.antiphishing.org/index.html (last accessed June 30, 2010).

APEC Telecommunications and Information Working Group, "Guide on Policy and Technical Approaches Against Botnet" (December 2008) available at http://publications.apec.org/publication-detail.php?pub_id=145 (last accessed February 7, 2011).

Australian Competition and Consumer Commission available at http://www.accc.gov.au/content/index.phtml/itemId/3653 (last accessed February 2, 2011).

Australian Government, *Cyber Security Strategy* (2009) available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf (last accessed January 29, 2010).

Australian Press Council, "Press Law in Australia," http://www.presscouncil.org.au/pcsite/fop/auspres.html#insult, accessed June 2010.

BARLOW, J.P., "A Declaration of Independence in Cyberspace" *Humanist* 1996 available at http://editions-hache.com/essais/pdf/barlow1.pdf

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).

BitTorrent user license, available at http://www.bittorrent.com/legal/bittorrent-eula (last accessed Feb. 10, 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).

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.

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)

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).

CNCERT website available at http://www.cert.org.cn/english_web/overview.htm (last accessed February 20, 2011).

Computer World, "AKILL Controlled a Botnet of 1.3 Million PCs, Says OPTA" (2007) available at http://www.computerworld.co.nz/news.nsf/news/64482C4D3AAB769ACC2573B7007419F7 (last accessed June 25, 2010).

ComputerWorld, "Akill Evaluated: Crime Lord or Script Kiddie?" (2008) available at http://computerworld.co.nz.new.nsf/scrt/8965613190D60231CC257431007FCDA0 (last accessed June 24, 2010.558-352-5/09/11.

CORRONS, Luis, 'Mariposa Botnet' on *PandaLabs Blog* (3 March 2010) <http://pandalabs.pandasecurity.com/mariposa-botnet/>.

Damballa, *Introduction* http://www.damballa.com/overview/index.php (last accessed July 10, 2010).

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

DollarRevenue Affiliate Agreement, www.dollarrevenue.com/affiliateagreement.asp.

Domain Name System Security Extension, available at http://www.dnssec.net/ (last accessed November 10, 2010).

Domain UltraReach, available at http://www.ultrareach.com/company/aboutus.htm (last accessed March 21, 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).

GASSTER, L. of the ICANN GNSO Council, "GNSO Issues Report on Fast Flux Hosting" (March 25, 2008) available at http://www.st.icann.org/m/page/gnso-council/fast_flux (last accessed July 2, 2010).

GEIST, M. "Telus Blocks Subscriber Access to Union Website" (July 4, 2005) available at http://www.michaelgeist.ca/index.php?option=com_content&task=view&id=904&Itemid=85&nsub (last accessed at January 30, 2010).

[gnso-ff-pdp-may08] case study: fluxing domains used for unusual purpose, available at http://forum.icann.org/lists/gnso-ff-pdp-may08/msg00371.html (last accessed February 7, 2011).

GUTMAN, P. "The Commercial Malware Industry" available at www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf (last accessed February 4, 2011).

HAUBEN, M. Behind the Net – The untold history of the ARPANET available at http://www.dei.isep.ipp.pt/~acc/docs/arpa.html (last accessed January 14, 2008).

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).

ICANN Accreditation Termination Notice to EstDomains, available at http://www.icann.org/en/correspondence/burnette-to-tsastsin-28oct08-en.pdf (last accessed December 10, 2011).

INTERPOL, About INTERPOL available at http://www.interpol.int/Public/icpo/default.asp (last accessed March 21, 2011).

ISP-Planet available at http://www.isp-planet.com/index.html) (last accessed January 29, 2010).

"Is Serco Behind Stuxnet" (thread started September, 2010 and ongoing) available at http://www.abovetopsecret.com/forum/thread615788/pg1 (last accessed February 7, 2011).

ITU World Telecommunication/ICT Indicators Database, "Global Number of Internet Users, Total and Per 100 Inhabitants, 2000-2009" available at http://www.itu.int/IT-D/ict/statistics/material/groups/Internet_users_00-09.jpg (last accessed July 12, 2010)

JAISHANKAR, K., "Space Transition Theory of Cybercrimes" in Schmalleger, F. And Pittaro, M. *Crimes of the Internet* (Pearson: Prentice Hall, 2009).

KSHETRI, N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspective* (Springer, 2010)

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).

M86 Security Labs, "Mega-D Accounts for 32% of Spam" (2008) available at http://www.m86security.com/TRACE/traceitem.asp?article=510 (last accessed December 12, 2010).

MASNICK, Mike, "CIA claims cyberattacks at fault in blackouts" (January 14, 2008) available at http://www.techdirt.com/articles/20080118/181113.shtml.

Messaging Anti-Abuse Working Group (MAAWG) available at www.maawg.org.

MESSMER, E. "Symantec vs. Hotbar: Who Won?" (January 3, 2006) available at http://www.networkworld.com/weblogs/security/011312.html.

Microsoft, "The Stuxnet Sting" (July 16, 2010) available at http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx (last accessed February 7, 2011).

NCFTA website available at http://www.ncfta.net/about-ncfta (last accessed March 3, 2011).

NARAINE, R. "Storm Worm Botnet Partitions For Sale" (2007) available at http://www.zdnet.com/blog/security/storm-worm-botnet-partitions-for-sale/592.

National Cyber-Forensics Training Alliance website available at http://www.ncfta.net/ncfta-initiatives/malware-botnet (last accessed March 2, 2011).

NEWITZ, A., "Dangerous Terms: A User's Guide to EULAs" available at http://www.eff.org/wp/eula.php (last visited January 17, 2011).

OLLMANN, Gunter in ACHOHIDO, B., "Are there 6.8 million – or 24 million – bottled PCs on the Internet?" (April10, 2010) *The Last Watchdog on Internet Security* available at http://lastwatchdog.com/6-8-million-24-botted-pcs-internet/ (last accessed July 12, 2010).

OLLMANN, G., "Your Computer is Worth 30¢: This Battle for Control of Your Computer Isn't Personal, it's Business" (April 8, 2010) available at http://www.damballa.com/knowledge/presentations.php.

OPTA "Decision on objection concerning fines for distributing unsolicited software (DollarRevenue)" available at http://www.opta.nl/asp/en/publications/document.asp?id=2724.

OPTA, "Fact Sheet: Decision to Impose Fine on Dollarrevenue" (December, 2007) available at http://www.cytrap.eu/files/ReguStand/2007/pdf/2007-12-18-DollarRevenue-largestSpywareFineEurope-NL-OPTA.pdf.

"Owning Kraken Zombies: A Detailed Dissection" (April, 2008) available at http://dvlabs.tippingpoint.com/blog/2008/04/28/owning-kraken-zombies (last accessed November 11, 2010).

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).

PARSONS, C. "Deep Packet Inspection in Perspective: Tracing its Lineage and Surveillance Potentials" available at http://www.surveillanceproject.org/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf (last accessed May 25, 2009).

PARSONS, C., blog on DPI available at www.delicious.com/caparsons/dpi.

Ponemon Institute, 2009 Annual Study: U.S. Enterprise Encryption Trends available at http://www.encryptionreports.com/2009etrends.html and 2007 and 2008 trends at http://www.encryptionreports.com/encryptiontrends.html.

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).

PURDY, A. "Proposal for Malicious Activity/Cyber Crime Initiative" 2009.

RILEY, C. And SCOTT, B. "Deep Packet Inspection: The End of the Internet as We Know It?" March 2009 available at http://www.freepress.net/node/49007 (last accessed March 21, 2011).

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).

Russian Business Network "New and Improved Storm Botnet for 2008" available at http://rbnexploit.blogspot.com/.../rbn-new-and-improved-storm-botnet-for.html (last accessed June 25, 2010).

Sans.org, *SANS Newsbites* http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5.

SAWYER, J. "Tech Insight: The Enterprise Hacks Back!" *Dark Reading* available at http://darkreading.com/security/attacks/showArticle.jhtml?articleID=223100750.

SCHNEIER, B., Benevolent Worms, Crypto-Gram Newsletter, 2003, available at http://www.schneier.com/cryptogram-0309.html (last accessed November 12, 2010).

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., "The Techniques for Distributing Child Porn" available at *Schneier on Security* http://www.schneier.com/blog/archives/2009/03/the_techniques.html (last accessed February 7, 2011).

SCHNEIER, B., "The Storm Worm" (October 4, 2007) available at http://www.schneier.com/blog/archives/2007/10/the_storm_worm.html (last accessed December 2010).

Security Beyond Borders, "Salami technique" available at http://securitybeyondborders.org/global-security-glossary/global-security-glossary-s/ (last accessed Marc 18, 2011).

Shadowserver Foundation, *Botnet Charts* available at http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts (last accessed December 2010).

Shadowserver website available at http://www.shadowserver.org (last accessed October 31, 2010).

SocialText, "What Things Regulate" available at https://www.socialtext.net/codev2/index.cgi?what_things_regulate (last accessed March 18, 2011).

Soloway plea bargain, available at http://www.circleid.com/pdf/soloway-73.pdf (last accessed October 26, 2010).

Spamhaus website available at http://www.spamhaus.org/news.lasso?article=611 (last accessed October 19, 2010).

Spamlaws website, available at http://www.spamlaws.com/Dollarrevenue-adware.html (last accessed March 2011).

Stat-owl available at http://www.statowl.com/network_isp_market_share.php (last accessed January 29, 2010).

STEWART, J., "Mega-D/Mega-D Trojan Analysis," (2008) *Secure Works* available at http://www.secureworks.com/research/threats/Mega-D/ (last accessed December 12, 2010).

Stopbadware.org, *DollarRevenue Report* available at http://www.stopbadware.org/reports/reportdisplay?reportname=dollarrevenue (last accessed March 2011).

Sunbelt Software, list and video transmission of over 2000 unsolicited software, available at http://www.sunbelt-software.com/ihs/alex/deskwizzclickfraud542006.pdf.

SYPNOWICH, C. (2001) Law and Ideology, Stanford Encyclopedia of Philosophy, available at http://www.plato.stanford.edu./entries/law-ideology

SysAdmin, Audit, Network, Security Institute (SANS Institute) http://www.sans.org.

TAYLOR, R., CAETI, T., LOPER, K., FRITSCH, E., AND LIEDERBACH, *Digital Crime and Digital Terrorism* (UK: Pearson, 2005).

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).

The Ronald Coase Institute, "Publications of Ronald Coase" available at http://www.coase.org/coasepublications.htm (last accessed March 18, 2011).

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).

University of Chicago Law School, "Richard A. Posner: Publications" available at http://www.law.uchicago.edu/node/79/publications (last accessed March 18, 2011).

"Waledac Questions Answered" available at http://www.lavasoft.com/mylavasoft/company/blog/waledac-questions-answered.

WHOIS Task Force, available at http://www.gnso.icann.org/issues/whois-privacy/whois-tfl-preliminary.html#GTLDRegistriesconstituency (last accessed April 30, 2010).

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>.

YAR, M., "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory" (2005) 2(4) European Journal of Criminology 407

Zeroday Emergency Response Team (ZERT), available at http://www.isotf.org/zert/.

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.

Governmental Reports and Submissions

2005 Australian Computer Crime and Security Survey. The survey included questioning of 110 organisations in Australia. It is available at http://www.aic.gov.au/statistics/hightech/cybercrime.aspx (last accessed May 24, 2010).

AISI project, available at http://www.acma.gov.au/aisi (last accessed January 25, 2010).

Australian Law Reform Commission, Review of Australian Privacy Law, Discussion Paper 72, September 2007.

Australian Government, *Cyber Security Strategy* (2009) available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf (last accessed January 29, 2010).

CHOO, R., SMITH, R. and MCCUSKER, R. Future Directions in Technology Enabled Crime (Australian Institute of Criminology 2007-2009).

Council of the European Union, "Strategy to Combat Cybercrime" (2010) 5957/2/10FR22.

Council of Europe, European Committee on Crime Problems, Committee of Experts on the Operation of European Conventions on Co-Operation in Criminal Matters, "Summary of the Replies to the Questionnaire on Mutual Legal Assistance in Computer-Related Cases" February 18, 2009.

Council of Europe, The Cybercrime Convention Committee, "Questionnaire for the Parties Concerning the Practical Implementation of the Convention on Cybercrime by the Parties." September 3, 2007.

Council of Europe, Project on Cybercrime, Economic Crime Division, "The Functioning of 24/7 Points of Contact for Cybercrime" April 2, 2009.

Council of Europe, Project on Cybercrime, Pedro Verdelho, "The Effectiveness of International Co-operation Against Cybercrime: Examples of Good Practice" March 2008.

DCITA, "Outcome of Review of the Legislative Framework on Spyware" 2004 available at http://www.dbcde.gov.au/communications_for_consumers/security/spyware/outcome.

Government Response to the House of Representatives Standing Committee on Communications Report on the Inquiry into Cyber Crime, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime* (2010)

House of Representatives Standing Committee on Communications, The Report of the Inquiry into Cyber Crime, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime* (June 2010) available at http://aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf (last accessed July 13, 2010).

MAURUSHAT, A., "Supplementary Submission 62.1" Inquiry into Cybercrime (September 2009) available at http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub62_1.pdf (last accessed February 8, 2011).

MAYHW, P. "Counting the Costs of Crime in Australia" (April 2003) *Trends & Issues in Crime and Criminal Justice,* No 247.

Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General ('MCCOC'), *Model Criminal Code Report Chapter 4: Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction* (2001).

Office of the Privacy Commissioner, Submission to the Australian Law Reform Commission Privacy Inquiry.

PILGRIM, T. "Draft Internet Industry Association eSecurity Code of Practice" Office of the Privacy Commissioner submission to the Internet Industry Association.

P*rivy Council Review of Intercept as Evidence Report CM7324 (*January 30, 2008) available at http://www.official-documents.gov.uk/document/cm73/7324/7324.pdf

Spam and Spyware Study SMART 2008/0013 Country profile (Netherlands).

Senate Legal and Constitutional Committee*, Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000.*

Telstra, "Telstra Submission House of Representations Communication Committee Enquiry Into Cybercrime", Submission No. 43 available at http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub43.pdf (last accessed February 7, 2011).

United Kingdom Office of Cyber Security, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (2009) available at http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf (last accessed January 29, 2010)

United States-Canada Working Group, United States-Canada Cooperation Against Cross-Border Telemarketing Fraud (November 1997) available at http://strategis.ic.gc.ca/pics/ct/reporte.pdf (last accessed February 9, 2011).
--> LINK DOESN'T WORK – TRY http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/01290.html FOR EXECUTIVE SUMMARY

United States Government, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009) available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (last accessed January 29, 2010)

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.

CROCKER, S. and BERNSTEIN, M. "ARPANET Disruptions: Insight into Future Catastrophes." TIS (Trusted Information Systems) Report, 247, 24 Aug 1989.

Electronic & Secure Municipal Administration for European Citizens at http://www.deloitte.com/dtt/cda/doc/content/dtt_eMayorFinalReport06_021706.pdf

GAASTER, L., GNSO Council Issues Report on FastFlux Hosting (March 31, 2008) available at http://www.icann.org

GASSTER, L. of the ICANN GNSO Council, "GNSO Issues Report on Fast Flux Hosting" (March 25, 2008) available at http://www.st.icann.org/m/page/gnso-council/fast_flux (last accessed July 2, 2010).

HALPERIN, D., et al, 'Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses' (2008) *Secure Medicine* <http://www.secure-medicine.org/icd-study/icd-study.pdf> at 9 May 2010.

iDefense, *The Russian Business Network: The Rise and Fall of a Criminal ISP* (27 June 2007).

International Telecommunications Unions, "ITU Botnet Mitigation Toolkit" (January 2008) available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf (last accessed February 7, 2011).

International Telecommunications Unions (ITU) Study Group q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts (January 2008).

Internet Industry Association, *Internet Service Providers Coluntary Code of Practice for Industry Self-Regulation in the Area of e-Security* (September 2009).

LEINEN, S. RFC 3955: Evaluation of Candidate Protocols for IP Flow Information Export (IPFIX) Oct. 2004.

"McAfee Virtual Criminology Report: Cybercrime: The Next Wave" 2007.

"McAfee Virtual Criminology Report: Organized Crime and the Internet" December 2006.

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).

[SAC025]: Fast Flux Hosting and DNS (SAC025) (January 28, 2008) available at http://www.icann.org/committees/security/sac025.pdf (last accessed January 31, 2011).

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).

ZHAO, X., HOWE, D., NISSENBAUM, H., and MAZERES, D., "Phantom Access Agent: a Client-Side Approach to Personal Information Control" available at http://www.nyu.edu/projects/nissenbaum/papers/paa.pdf (last accessed June 30, 2010).

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).

DE VILLIERS, M., "Information Security Standards" (2009) *University of New South Wales Law Research Paper Working Paper* 34.

Free Press, DPI.

"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).

Interpol Constitution and General Regulations (Interpol Constitution).

LIVINGOOD, J., MODY, N. And O'REIRDAN, M. of Comcast, Internet Engineering Task Force Working Draft, *Recommendations for the Remediation of Bots in ISP Networks* (September 2009)

LOZUSIC, R. "Fraud and Identity Theft" Briefing Paper No 8/03.

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).

MANOLESCU, D., *Is It Possible to Regulate the Internet Globally?: A Comparative Case Study of Cybercrime Framework in Canada and Romania* (Masters Thesis, University of Alberta, 2009).

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>

U.S. Department of Justice Press Release: California Man Pleads Guilty in "Botnet" Attach 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).

BARLOW, J.P., "The Economy of Ideas" (March 2994) *Wired* Issue 2.03 available at http://www.wired.com/wired/archive/2.03/economy.ideas.html (last accessed November 10, 2010).

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).

CARTER, M., "Spam King Pleads Guilty to Felony Fraud" (March 15, 2008) *The Seattle Times* available at http://seattletimes.nwsource.com/html/localnews/2004283998_spamking15m.html (last accessed October 29, 2010).

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., "Web Snooping Policy Shrouded in Secrecy," *The Age*, June 17, 2010, http://www.theage.com.au/technology/technology-news/web-snooping-policy-shrouded-in-secrecy-20100617-yi1u.html.

MSNBC, "One of the World's Top 10 Spammers Held in Seattle" (May 5, 2007) available at http://www.msnbc.msn.com/id/18955115/ (last accessed October 26, 2010).

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).

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).

VAMOSI, R. "FBI Warns of New Storm Worm Variant" (2008) available at http://new.cnet.com/8301-1009_3-10002760-83.html (last accessed June 24, 2010).

ZDnet, "Berner-Lees says no to Internet 'snooping'", March 11 2009 available at http://news.ndnet.co.uk/security/01,000000189,39625971,00.htm (last accessed April 16, 2009).

Conference/workshop seminars and papers

ALLMAN, M., BLANTON, E., PAXSON, V. And SHENKER, S. "Fighting Coordinated Attackers with Cross-Organizational Information Sharing" *Records of the 5th Workshop on Hot Topics in Networks*, Beckman Centre 2006.

BARAKAT, A., and KHATTAB, S., "A Comparative Study of Traditional Botnets Versus Super-Botnet" in *INFOSEC 2010*.

BENDRATH, R. "Global Technology Trends and National Regulation: Explaining Variation in the Governance of Deep Packet Inspection" *International Studies Annual Conference Paper* (Feb. 2009) available at http://userpage.fu-berlin.de/~bendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf (last accessed May 25, 2009).

Closed panel sessions at *AusCERT 2008 Conference, AusCERT 2009 Conference*, and Internet *Security and Intelligence Operations 5 Workshop 2007*, Estonia.

DAGON, D. and DAVIS, C., "Botnet Population and Intelligence Gathering Techniques" (2008) *Blackhat Conference* available at http://www.blackhat.com/presentations/bh-dc-08/Dagon-Davis/Presentation/bh-dc-08-dagon-davis.pdf (last accessed June 28, 2010).

DAGON, D., GRIZZARD, J., SHARMA, V., NUNNERY, C., and BYUNGHOON KANG, B., "Peer-to-peer Botnets: Overview and Case Study" (2007) *Hotbots Conference* available at http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard_html/#uniq (last accessed June 30, 2010).

DAGON, D, GU, G., LEE, C. and LEE, W., "A Taxonomy of Botnet Structures" *Twenty-Third Annual Computer Security Applications Conference* (ACSAC 2007) pp. 325-339.

DAGON, D., ZOU, C., and LEE, W. "Modeling Botnet Propagation Using Time Zones" (2006) *Proceedings of the 13th Network and Distributed System Security Symposium* (NDSS).

DUNKLIN, P. and ELLSMORE, N., "Anti-Virus is Dead" *Australian Information Security Association Meeting*, August 19, 2009.

ESPOSITO, G. 'The Council of Europe Convention on Cyber-Crime: A Revolutionary Instrument?' in BROADHURST, R. (ed) (2004) *Proceedings of the 2nd Asia Cyber-Crime Summit* (Centre for Criminology, the University of Hong Kong, 2003).

GOVIL, J., "Examining the Criminology of Bot Zero" *Information, communications & Signal Processing 6th International Conference on (2007)* available at http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4449633&tag=1 (last accessed December 2010).

GUPTA, A. and DUVARNEY, D., "Using Predators to Combat Worms and Viruses: A Simulation-based Study" (2004) *Proceedings of the 20th Annual Computer Security Applications Conference*, ACM Digital Library.

IANELLI, N. and HACKWORTH, A., "Botnets as a Vehicle for Online Crime" Dec. 1 2005 *US CERT* available at http://www.first.org/conference/2006/papers/ianelli-nicholas-slides.pdf (last accessed March 18 2011).

IETF's Internet Architecture Board workshop on "Unwanted Internet Traffic", summarized in RFC 4984, available at http://www.isi.edu/in-notes/rfc4948.txt (last accessed January 29, 2010).

JANG, D., KIM, M., JUNG, H-C, N, B-N, "Analysis of HTTP@P Botnet: Case Study Waledac" (2009) *Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications.*

JUDGE, P., APLPERVITCH, D., and YANG, W., "Understanding and Reversing the Profit Model of Spam" (2005) *Fourth Workshop on the Economics of Information Security* available at http://infosecon.net/workshop/pdf/49.pdf (last accessed December 2010)

KIM, D-H., LEE, T., IN, P., and JEUNG, H.C., "Botnet Damage Propagation Estimation Model" (2009) *KSII The First International Conference of Internet (ICONI)* available at http://www.embedded.korea.ac.kr/ecel/paper/international/2009/12200910.pdf (last accessed December 2010).

LIAO, Q., STRIEGEL, A., and LI, Z., "Botnet Economics: Uncertainty Matters" (2008) *WEIS Conference 2008*, available online at http://www.weis2008.econinfosec.org/papers/Liao.pdf (last accessed July 5, 2010).

LOVET, G., "Fighting Cybercrime: Technical, Juridical and Ethical Challenges" (Paper presented at the *Virus Bulletin Conference* 2009, Geneva, 23, September 2009).

MAURUSHAT, A., "The Limits of 'Permitted Self-Help' in Internet Security and Intelligence" *ISOI conference*, Estonia.

MAURUSHAT, A."Standing Behind Technical Promises" (2008) *AusCERT Asia Pacific Information Security Conference.*

NEWTON, J. (2004), "Interpol and the cards industry: global partnerships to deliver local solutions", in Broadhurst, R. (Ed.), *Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology*: University of Hong Kong, Hong Kong.

PERLOTTO, R. "Conficker" *AusCERT Online Crime Symposium* (2009). Presentation available online at https://www.auscert.org.au/download.html?f=318 (last accessed November 10, 2010).

Presentation by FBI (2008), *AusCERT Conference.*

Presentation given at the *World Economic Forum* 2007.

PROVOS, N., MCNAMEE, D., MAVROMMATIS, P., WANG, K., and MODADUGU, N., "The Ghost in the Browser: Analysis of Web-based Malware" (2007) *HotBots07 Conference*, Cambridge Massachusetts, USENIX.

PURDY, A. "Fight Cybercrime Like We Mean It" AusCERT 2009 available at http://conference.auscert.org.au/conf2009/presenter.php?presenter_id=AP (last accessed June 12, 2010).

PURDY, A. and PLESCOE, R., "National Cyber-Forensics Training Alliance" (2009) *AusCERT Security Conference.*

RAMACHANDRAN, A. and FEAMSTER, N., "Understanding the Network-Level Behaviour of Spammers" (2006) *SIGCOMM*.

ROMANOSKY, S., TELANG, R., and ACQUISTI, A. "Do Data Breach Disclosure Laws Reduce Identity Theft? *Seventh Workshop on the Economics of Information Security*, June, 2008.

SANTORELLI, S., "The Future of Botnets" (2008) *AusCERT Conference*.

SCOTTBERG, B., YURICK, W. And DOSS, D. "Internet Honeypots: Protection or Entrapment" *Internet Symposium on Technology and Society* (2002) available at www.ieeexplore.ieee.org/xpls/abs_all.jsp?arnuber=1013842&tag=1 (last accessed November 6, 2010).

SKINNER, W. AND FREAM, A., "A Social Learning Theory Anlaysis of Computer Crime Among College Students" (1997) 34 Journal of Research in Crime and Delinquency 495

STEWART, J. "Protocols and Encryption of the Storm Botnet" *Blackhat Computer Security Conference* available at https://www.blackhat.com/.../BH_US_08_Stewart_Protocols_of_the_Storm.pdg (last accessed June 25, 2010).

STONE-GROSS, B., CAVALLARO, L., GILBERT, B., SZYDLOWSKI, M., KEMMERER, R., KRUEGEL, C., and VIGNA, G., "Your Botnet is My Botnet: Analysis of a Botnet Takeover" (2009) *CCS, ACM* 978-1-60.

TEAM CYMRU, "Confickr" (2009) *AusCERT Security Conference*.

TEAM CYMRU presentations at *AusCERT Security Conference* (2007 and 2009). Closed sessions on cybercrime.

VAN DER GEEST, Thea, PIETERSON, Willem and DE VRIES Peter: Informed Consent to Address Trust, Control, and Privacy Concerns in User Profiling, *Workshop on Privacy-Enhanced Personalization, 10th International Conference on User Modeling*, Edinburgh (2005). Available online: http://www.isr.uci.edu/pep05/papers/InformedConsent.PDF.

VOGT, R., AYCOCK, J., and JACOBSON, M., "Army of Botnets" (2007) *Network And Distributed System Security Symposium (ISOC)* available at http://www.74.125.155.132/scholar?q=cache:x9cPT4RLO0J:scholar.google.com/&hl=en&as_sdt=2000 (last accessed June 29, 2010). THAT LINK DOESN'T WORK – TRY THIS ONE INSTEAD: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.67.6519&rep=rep1&type=pdf

WOUTERS, P., "Defending Your DNS in a Post-Kaminsky World" (2009) *Black Hat Computer Security Conference* available at http://www.blackhat.com/presentations/bh-dc-09-Wouters/BlackHat-DC-09-Wouters-Post-Dan-Kaminsky-slides.pdf (last accessed June 30, 2010).

ZENZ, K., "Cyber Crime Within the Russian Federation" presentation at *AusCERT 2008*.

ZHUANG, Li., DUNAGAN, J., SIMON, D.R., WANG, H.J., and TYGAR, J. D., "Characterizing Botnets From Email Spam Records" *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats* (2008)

Online videos and podcasts

"Anonymous to Australia" available at http://www.youtube.com/watch?v=eEc80U46hIQ (last accessed January 13, 2011).

INSIGHT, "Stolen ID" (December 14, 2008) available at http://news.sbs.com.au/insight/episode/index/id/30 (last accessed February 11, 2011).

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).

Risky.biz Podcast, "RB2: AusCERT Podcast: Interview with Moscow-Based Cybercrime Analyst Kimberly Zenz" (May 20, 2009).

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).