AUSTRALIA'S ACCESSION TO THE *CYBERCRIME CONVENTION*: IS THE *CONVENTION* STILL RELEVANT IN COMBATING CYBERCRIME IN THE ERA OF BOTNETS AND OBFUSCATION CRIME TOOLS?

ALANA MAURUSHAT*

I BACKGROUND

At the annual Australian Computer Emergency Response Team ('AusCERT') computer security conference in 2009,[1] Federal Agent Nigel Phair of the Australian Federal Police ('AFP') stated that combating crime tools was important and that information on botnets was a priority item for the AFP. At the same conference, Alexander Seger, head of the Council of Europe's Economic Crime Division, urged Australia to accede to the *Council of Europe's Convention on Cybercrime* ('*Convention*').[2] In a joint media release of the Attorney-General and the Minister for Foreign Affairs on 30 April 2010, it was announced that Australia intends to accede to the *Convention*. According to the media release:

> The Convention, which entered into force in July 2004, is the only binding international treaty on cybercrime. It serves as both a guide for nations developing comprehensive national legislation on cybercrime and as a framework for international co-operation between signatory countries.
>
> Cybercrime poses a significant challenge for our law enforcement and criminal justice system. The Internet makes it easy for criminals to operate from abroad, especially from those countries where regulations and enforcement arrangements are weak.

* Lecturer, Faculty of Law, University of New South Wales; Deputy Director of the Cyberspace Law and Policy Centre, Faculty of Law, University of New South Wales; PhD Candidate, Faculty of Law, University of New South Wales. The author is completing a PhD in the area of regulatory botnets. The author is indebted to valuable comments from the two peer reviewers as well as Graham Greenleaf, Lyria Bennett Moses and Pauline Rappaport.

1 Nigel Phair, 'Cybercrime and the Legal Dimension' (Speech delivered at the AusCERT Asia Pacific Information Security Conference 2009, Gold Coast, 19 May 2009).

2 Alexander Seger, 'The Convention on Cybercrime – Meeting a Global Challenge' (Speech delivered at the AusCERT Asia Pacific Information Security Conference 2008, Gold Coast, 19 May 2008); *Council of Europe's Convention on on Cybercrime*, opened for signature 23 November 2001, 2296 UNTS 167 (entered into force 1 July 2004) ('*Convention*').

> It is critical that laws designed to combat cybercrime are harmonised, or at least compatible to allow for cooperation internationally.[3]

The *Convention* was negotiated and written in the earlier days of cybercrime – the late 1990s – with a final draft introduced in 2001. The *Convention* entered into force on 1 July 2004. Since then the craft and technologies involved in cybercrime have evolved so as to render many of the *Convention*'s provisions of limited relevance. Many cybercrimes are committed using modern cybercrime tools such as malicious software ('malware'), botnets, onion routing and others. These technologies are used with obfuscation, anonymity, computational power and deniability of traceback to the source in mind. The use of many forms of malware and botnets allows criminals to avoid technical controls such as antivirus software and internet filters, as well as to avoid law enforcement. The *Convention* entered into force the same year that the malware landscape became monetised and thus moved from the realm of the curious hacker to one of commercialisation and profitability. Organised criminal groups became involved in malware and botnets at this time. Later in 2004 new technologies were unveiled at technology conferences giving criminals such excellent tools as Tor (the ability to onion route allowing no traceback), TrueCrypt (a deniable encryption software) and virtual private network services. With money as an emerging motif in malware and botnet deployment along with the rapid advancement of obfuscation technologies, the ability to collect evidence and traceback to the perpetrator of an economic crime has become extremely difficult.

The *Convention* is premised on fighting cybercrime. Cybercrime is distinct from more traditional forms of crime in three ways. First, cybercrime is often transnational. It involves multiple jurisdictions where incidents are global. Dan Robel explains a global incidence as:

> Three primary situations can be defined as a global incident. The first is an incident where the country of origin from whence an attack or malicious activity originates differs from the country where the incident takes place. The next is an incident where all activity happens within one nation's physical borders, but assets (whether computers, data, etc) are owned by another nation. The last is where multiple nations are affected including the nation where the attack originated.[4]

Second, it is a novel area of crime with which *most* law enforcement agents, lawyers and judges are either unfamiliar or for which they have insufficient

3 Robert McClelland and Stephen Smith, 'Australia to Accede to International Cybercrime Convention' (Media Release, 30 April 2010) <http://www.foreignminister.gov.au/releases/2010/fa-s100430.html>.

4 Dan Robel, *International Cybercrime Treaty: Looking Beyond Ratification* (28 March 2007) SANS Institute, 6 <http://www.sans.org/reading_room/whitepapers/incident/>.

training.[5] Third, cybercrime involves digital evidence that is highly volatile and, therefore, subject to being expunged in court. The *Convention* has some relevance in addressing these three cybercrime attributes.

Cybercrime is a lucrative field that has, according to some sources, surpassed profits in the global drug trade.[6] One of the major reasons that cybercrime has escalated is due to the ability of criminals to avoid detection. While transnationalism, insufficient training and the volatility of digital evidence aid the cyber-criminal, the most significant contribution is the ability of a criminal to use obfuscation crime tools, which make traceback to the original source difficult or even impossible. For this reason, this article considers the *Convention*'s relevance against the backdrop of modern obfuscation crime tools.

The first part of the article explores what is meant by modern obfuscation crime tools. These include botnets, malware, Trojans, onion routing, fast flux and double fast flux, dynamic domain name hosting, virtual private network services, peer-to-peer (often known as 'P2P') channels, and encryption. These crime tools are used to commit many of the forms of cybercrime contemplated in the *Convention*: computer misuse and abuse, computer related fraud and forgery, and child pornography distribution. Intellectual property crimes will not be addressed in this article as such crimes do not typically exploit a full range of obfuscation technologies but most commonly use peer-to-peer file sharing programs. In the next sections, substantive, procedural and international cooperation elements of the *Convention* are explored and compared with Australian law. As the *Convention* requires procedural and international cooperation to occur in accordance with domestic law, this article will describe the Australian content warrant framework in conjunction with interception and real time evidence collection technologies and obligations for internet service providers ('ISPs') to use such technologies – this is the first article of its kind to do so. The last section will address the advantages and disadvantages of Australia acceding to the *Convention*.

I will use the example of a botnet as the main example of an obfuscation crime tool to demonstrate the relevancy of the *Convention*. Botnets have been singled out to keep the article a manageable size and due to the gravity of the

5 For example, in the case of *R v Caffrey* there was overwhelming evidence against the accused who launched a distributed denial-of-service attack against the Port of Houston. The logistics of the port, including ship docking, was severely affected. The defendant was a known hacker, with common hacking tools on his computer, had a grudge with the company and had announced his intentions in a number of chatrooms. Nonetheless, he was able to argue that his computer had been compromised and was part of a botnet being controlled by someone else. The jury acquitted. The case was not reported in law databases but was covered by the British media and is mentioned by several cybercrime researchers. See 'Questions Cloud Cyber Crime Cases', *BBC News* (online), 17 October 2003 <http://www.bbc.co.uk/2/hi/technology/3202116.stm>; Richard Clayton, *Complexities in Criminalising Denial of Service Attacks* (February 2006) 3–4 <www.cl.cam.ac.uk/~rnc1/complexity.pdf>; Peter Grabosky, *Electronic Crime* (Pearson Prentice Hall, 2007) 80–1; Susan W Brenner, Brian Carrier and Jef Henninger, 'The Trojan Horse Defense in Cybercrime Cases' (2004) 21 *Santa Clara Computer and High Technology Law Journal* 1, 1–7.

6 See John Leyden, 'Cybercrime "More Lucrative" Than Drugs' (29 November 2005) *The Channel Register* <http://www.channelregister.co.uk/2005/11/29/cybercrime/>.

threat that they pose, as recently demonstrated in the federal government's House of Representatives Inquiry into Cyber Crime entitled *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*.[7]

II OBFUSCATION CRIME TOOLS

There are many crime tools that allow criminals to remain anonymous online or to make traceback to the source of the crime challenging. Of these tools, botnets pose the greatest challenge for a number of reasons. For the purpose of this article, I will define these crime tools below and then, in order to keep the article a manageable size, I will use botnets as an example to analyse the potential ability of the *Convention* to deal with cybercrime. As such, I will provide a more detailed analysis of a botnet than the other types of obfuscation crime tools.

Malware can include a number of software programs such as viruses, worms and Trojans. Defined more technically, malware is:

> software, or a software component or feature, that comes by some means to be invoked on a device, and that, 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.[8]

In other words, it is software that becomes installed on a user's computer without the user's knowledge and does bad things once installed (like username and password theft, deleting files, stealing banking credentials and so forth).

Rootkits are:

> Literally software that allows an intruder to gain access to a device with the highest level of privileges available, ie associated with the root or system-administrator account. By extension: ... software that assists in obscuring the existence of malware on a device, and/or establishes an obscured environment within which malicious code can be executed.[9]

Rootkits are not visible on a computer. As such, the user cannot test or verify that the rootkit has been tampered with. The most damaging botnets often run with a default rootkit botnet that, if the main botnet goes down, the remote botnet waits to receive instructions from the default rootkit botnet. Rootkit botnets such as Mebroot have proven infallible. To date, no-one has been able to decrypt Mebroot or run any type of interference with its operations. Mebroot is one of many such botnets.

---

7 House of Representatives Standing Committee on Communications, Parliament of Australia, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime – The Report of the Inquiry into Cyber Crime* (2010) <http://aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf>. Invited submissions were received by the author, Microsoft, the Internet Industry Association ('IIA'), the Attorney-General's Department and the AFP – all of which highlighted the importance of tackling botnets within the context of combating cybercrime: at 122–5.

8 Roger Clarke, *Malware Glossary* (21 September 2009) <http://www.rogerclarke.com/II/MalCat-0909.xls>.

9 Ibid.

Trojans are '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'.[10] Many Trojans use keystroke logging. Keystroke logging captures everything that a person types into a computer. This, of course, includes usernames, passwords, financial details and other criminally useful identity details.

Onion routing is a proxy. More specifically, it is:

> a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes called onion routers. Each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated. This prevents these intermediary nodes from knowing the origin, destination, and contents of the message.[11]

The most common onion routing technology is Tor. It is used for both good and bad. People in countries with heavy internet censorship use this technology to access the greater world wide web.

Virtual Private Network services ('VPN') essentially allow for anonymous communication over the internet. VPN 'is a service where a customer requests multi-site connectivity services provided through a shared network infrastructure.'[12] VPN uses specialised tunnelling protocols that build on secured encryption techniques that provide data integrity, privacy and anonymity.

Dynamic Domain Name System ('DNS'), or dynamic DNS providers, allow users to register an account for free DNS hosting services. As leading botnet expert Gadi Evron describes:

> You can set up your domain name or use a 3LD with one they provide. Then point it to, for example, your home IP address (which changes every time you get on the Internet if it is dynamic). You could update the dynamic DNS information either via their Web page or using a tool they provide, which will automatically detect your new IP address and set your DNS records accordingly.[13]

This essentially involves the configuration of a domain to have several internet protocol ('IP') addresses.[14] If any one IP address is blocked or taken down, 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.

Fast flux is the name given to DNS records that change constantly. This could be every five minutes or every 15 days. 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

---

10 Ibid.

11 *Onion Routing* (19 June 2010) Wikipedia <http://en.wikipedia.org/wiki/Onion_routing>. Unlike other disciplines, Wikipedia is routinely sourced among technical scholars as authoritative.

12 US Patent No 7593395 (filed 22 September 2009). Definitions and backgrounds of VPN services and technologies are explored in this patent that is available online at <http://www.google.com.au/patents?hl=en&lr=&vid=USPAT7593395 >.

13 Craig A Schiller et al, *Botnets: The Killer Web App* (Syngress, 2007) 90.

14 A computer's IP address is the unique identifier of that machine, which identifies the machine to the network whenever that machine logs on to the internet.

and fast flux is the automation and rapidity of rotation with a fast flux botnet.[15] Some fast flux botnets rotate IP addresses every five minutes, others every hour. Botnets are explored below.

Encryption is the conversion of plain text into ciphertext. Encryption acts to conceal or prevent the meaning of the data from being known by unauthorised parties.

Obfuscation in the computer world refers to encoding and decoding drawing on conversion techniques that make it difficult to decipher data. For the purpose of this article I will also use the term to connote the broader sense of a technology that operates to evade technical parameters and to avoid law enforcement from tracing the crime back to its source.

Peer-to-peer communication 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 (such as servers or stable hosts).[16]

Distributed command and control (or superbotnets) is a type of botnet that draws on a small botnet comprised of 15–20 bots. The botnet masters may have anywhere from 10 000 to 250 000 bots at their disposal, but use select portions of small botnets within the larger botnet. The smaller botnet then issues commands to larger botnets (hence the term distributed command and control). Often the smaller superbotnet is located in the rootkit and is encrypted. Mebroot, for example, is a botnet that affects a user's rootkit. The program is encrypted. Noone in the world has yet to break this encryption.

Botnets are collections of remotely controlled and compromised computers known as bots, controlled by a bot master/botherder that installs software (typically malicious) on the bot's computer and performs acts, nearly always criminal, using the innocent bot computer.[17] Botnets may involve anywhere from a few hundred bots to several thousand to one documented case involving 13 million bots.[18] Bots receive their instructions from the bot master in the form of a bot (software). The bot must retrieve its instructions from what is known as the 'command and control' ('C&C') of the botnet. The C&C is often located in the Internet Relay Chat ('IRC') server or a set of designated domain names allowing a botmaster or a bot herder to control the bots remotely to perform activities that

15 Ken Dunham and Jim Melnick, *Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet* (CRC Press, 2009) 81.

16 *Peer-to-Peer*, Wikipedia (12 August 2010) <http://en.wikipedia.org.wiki/peer-to-peer>.

17 According to Clarke, above n 8, bots and botnets are explained as:

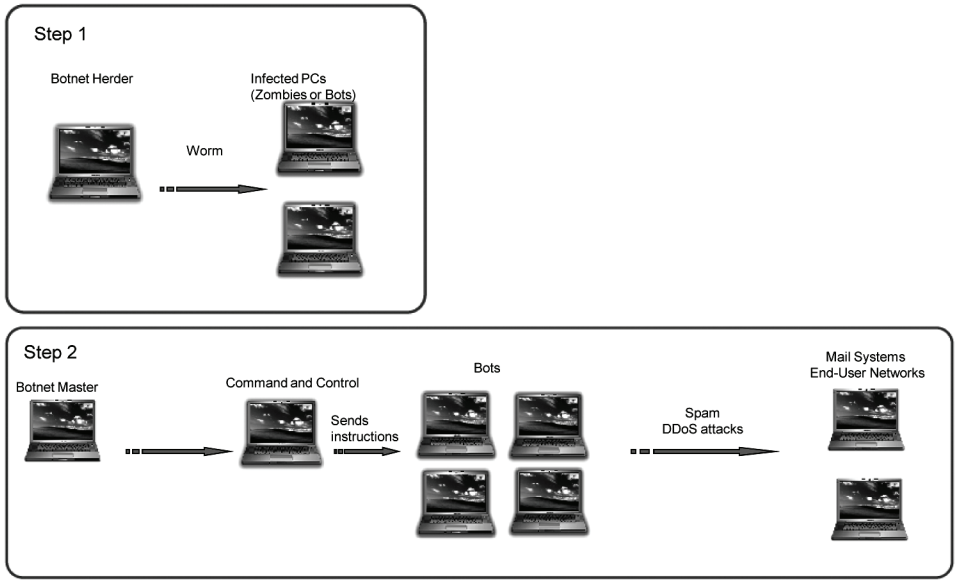
> (Generally, a program that operates as an agent for a user or another program. More specifically:) software that is capable of being invoked remotely in order to perform a particular function. (Typical functions include emailing spam or repetitively sending messages to a target device in order to overload it and thereby deny service; but also despatch of meta-data for files held on the device. A device on which a bot is installed is called a zombie. A set of devices on which bots are installed is called a botnet. Generally intended for largely automated operation, but under the control of a person who may be called a botnet master or botnet herder).

18 The Mariposa Botnet is said to have had 13 million zombies. See Jim Finkle, 'Spain Busts Hackers for Infecting 13 Million PCs' *Wired Threat Level* (2 March 2010) <http://www.wired.com/threatlevel/2010/03/spain-busts-hackers-for-infecting-13-million-pcs/>.

tend to be of a malicious nature. Other botnets leverage peer-to-peer networks and computer game consoles for their command and control locations.

The following diagram explains a botnet.

Diagram A: Steps in Procuring and Using a Botnet



In Step 1, the botnet herder needs to acquire bots to form part of his or her botnet. In Step 2, the botnet herder then uses software to command the bots to perform certain actions.

There are a number of methods to compromise a computer to become part of a botnet. This process will be referred to as bot acquisition. The principal methods are acquiring bots through operating system vulnerabilities, drive-by download and through social engineering techniques such as malicious web links and spam. These bot acquisition methods are systematically considered below.

Some botnet masters target software, hardware, and operating system vulnerabilities.[19] Many vulnerable computers are those that are unpatched,[20] use Windows and do not have a firewall.[21] Botnet masters often exploit vulnerable computers through port scans. A port scan is a process whereby requests are sent

19 A vulnerability is a feature or weakness that renders a computer or computer network susceptible to attack.

20 Operating system vendors issue patches. A patch is a set of computer code that purports to fix a vulnerability. Updating antivirus and anti-spyware is a form of a patch.

21 Yinod Yegneswaran and Paul Barford, 'An Inside Look at Botnets' in Mihai Christodorescu et al (eds), *Malware Detection (Advances in Information Security)* (Springer Science, 2007) 171. See also Roger Clarke and Alana Maurushat, 'The Feasibility of Consumer Device Security' [2009] *University of New South Wales Law Research Series* 5.

to networked computer ports in order to see which ports are open on a target computer. This is a way to assess vulnerabilities. Some commonly used ports are those related to Windows: port 42 WINS (host name server), port 80 HTTP, port 445 Microsoft-DS-Service, port 1025 Windows Messenger, and port 1433 Microsoft-SQL-Server.[22] Other botnets use social engineering techniques such as spam.

Botnet masters are increasingly resorting to new techniques for bot acquisition. Drive-by-downloads are becoming a more common way of acquiring bots.[23] The term drive-by-download is used in many ways. For our purpose, a drive-by-download means an authorised third party installation of malicious software where the installation occurs by visiting a website, clicking a deceptive advertisement, or clicking a link found in an email. The Torpig and Mebroot botnets, for example, utilised a drive-by-download technique. This is explained by Mebroot and Torpig researchers as:

> 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 (the drive-by-download server in the figure) 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. The installer then loads a kernel driver that wraps the original disk driver (disk.sys). At this point, the installer has raw disk access on the infected machine. The installer can then overwrite the MBR of the machine with Mebroot. After a few minutes, the machine automatically reboots, and Mebroot is loaded from the MBR.[24]

Social engineering techniques such as deceptive links, phishing and spam are common bot acquisition methods. Like in the drive-by-download instance, users are tricked into unknowingly installing malicious software onto their systems. Part of the malicious software is code designed to compromise the computer. Often many malicious programs are installed all at once. This could be adware, spyware, Trojans and keyloggers to steal usernames and passwords. The installations, therefore, can be multi-purpose. Once bot acquisition is successful, the compromised computer reports for duty by querying the command and control. Commands in the form of bot software are issued to the compromised computer.

---

22 Massimiliano Romano, Simone Rosignoli and Ennio Giannini, *Robot Wars – How Botnets Work* (8 November 2005) Window Security <http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html>.

23 Niels Provos et al, 'The Ghost in the Browser: Analysis of Web-Based Malware' (Paper presented at HotBots07 Conference, Cambridge, Massachusetts, 10 April 2007) <http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf>.

24 Brett Stone-Gross et al, 'Your Botnet Is My Botnet: Analysis of a Botnet Takeover' (Paper presented at the Association for Computing Machinery ('ACM') Conference on Computer and Communications Security 2009, Chicatgo, 9–13 November 2009) 635–6 (emphasis altered) (citations omitted).

The software instructs the bots to retrieve updates from the C&C of the botnet. The C&C may be located in domain names, in the IRC, in peer-to-peer channels, Google keywords and rootkits, or, more likely, a combination of several of the above. In a typical botnet, there will be several C&C locations to retrieve instructions. Many botnets will change the location of the C&C through dynamic DNS or fast flux rotation. For some botnets the C&C is changed every week, others every day and others every 20 minutes.[25] Many communications sent to the C&C are encrypted and thus not easily decipherable. Tracing back to an individual botnet master is extremely difficult. Where a C&C is shut down, most botnets are programmed to automatically receive its instructions from a new C&C location, or from a set default. Many botnets contain hundreds of thousands if not millions of infected bots.

The following is a list of functions that a compromised computer will perform once it becomes part of a botnet:

1) When a computer has been newly compromised one of its first duties is to report back to the C&C. It does this by joining a specified bot server such as the IRC or DNS text and waits for commands to be posted there. The commands are issued in the form of computer programs where the instructions are found in the payload of the bot.

2) The botnet master posts a command to the C&C that specifies instructions that the compromised computer then performs. Such instructions could be the downloading of several programs such as keylogging Trojans or adware. Other instructions may involve a denial of service attack whereby the target, type and time of the attack along with which compromised computers are to participate are all specified. This process may be aptly described as 'waiting for orders' and 'retrieving the payload'.

3) The compromised computer monitors the bot server where the C&C is located to verify whether any commands have been issued. Where there is a command the compromised computer proceeds to follow its instructions. Here the instructions found in the payload are carried out.

4) The compromised computer is programmed to routinely query the C&C to see if there are any new commands.[26]

Most compromised computers are programmed to compromise other computers. This is a form of recruiting other potential computers to join a botnet.

Why do botnets matter? Botnets are said to be involved in most forms of cybercrime and civil wrong ranging from sending spam, to denial of service attacks, child pornography distribution, worm propagation, click-fraud,

25 David Dagon et al, 'A Taxonomy of Botnet Structures' (Paper presented at 2007 Annual Computer Security Applications Conference, Miami Beach, 13 December 2007) <http://www.computer.org/portal/web/csdl/doi/10.1109/ACSAC.2007.44>.

26 Schiller et al, above n 13, 19.

keylogging technology and traffic sniffing (which captures passwords and credit card information), and mass identity theft.[27] In the words of leading botnet researcher Jeremy Linden of Arbor Networks, '[a]lmost every major crime problem on the Net can be traced to them.'[28] Internet security guru Vincent Cerf[29] has equated botnets to a pandemic, warning that a quarter of all personal computers have already become bots.[30] Botnets are perceived by many experts as a pandemic yet most users are unaware of the term or the threat that botnets pose to the internet.[31]

Particularly compelling is the description of botnets, compromised computers and related crimes from someone within the inner workings of the commercial child pornography industry. The article, 'An Insight into Child Porn',[32] was posted to the WikiLeaks website and is considered by many security experts and cybercrime researchers to be accurate and authoritative.[33] 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.[34]

---

27 Tomasz Rychlicki, 'Legal Issues of Criminal Acts Committed via Botnets' (2006) 12(5) *Computer and Telecommunications Law Review* 161.

28 Scott Berinato, 'Attack of the Bots' (November 2006) *Wired* <http://www.wired.com/wired/archive/14.11/botnet.html>.

29 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.

30 The statistics have been highlighted in a number of news reports and blog sites. See, eg, Nate Anderson, *Vint Cerf: One Quarter of All Computers Part of a Botnet* (25 January 2007) Ars Technica <http://www.arstechnica.com/news.ars/post/20070125-8707.html>.

31 David Barroso, 'Botnets – The Silent Threat' (Position Paper No 3, European Network and Information Security Agency, November 2007) 6.

32 Mr X, *An Insight into Child Porn* (26 February 2009) WikiLeaks <http://wikileaks.org/wiki/An_insight_into_child_porn>.

33 For example, see renowned security expert Bruce Schneier, 'The Techniques for Distributing Child Porn' on *Schneier on Security* (11 March 2009) <http://www.schneier.com/blog/archives/2009/03/the_techniques.html>.

34 Mr X, above n 32.

For those readers having difficulty with the technology, allow me to put it into layperson's terms. Once a computer is a bot, it can be used in every illegal function of the child pornography distribution chain. This includes spam botnets that may contain links to child pornography, links found within spam messages that trigger the downloading of malware. The malware infects an innocent user's computer and, without the user ever knowing, takes it over. The user's banking details are stolen. The user's email address is hijacked. Other items related to the user's identity are stolen (for example, usernames and passwords). The stolen identity (email and credit card details) is then used to register and purchase domain names, to launder money, to store and distribute child pornography. All of this is done typically in such a manner that the user has no idea the computer is a bot, not to mention that it is storing and distributing child pornography and other nefarious materials.[35]

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

There are approximately four methods of tackling botnets, which I will refer to as:

1) ISP and/or DNS registrar disconnection of C&C when located on web pages;[36]
2) infiltration and disruption of the C&C in IRC or peer-to-peer channels (typically by security organisations);
3) prosecution of the botnet herder(s); and
4) bot remediation (typically by the ISP).[37]

As this article deals with the *Convention* to investigate and prosecute cybercriminals, only prosecution of the botnet herders will be considered. The *Convention* plays no role in the other methods.[38]

---

35 Child pornography was found on the subdirectory of a Queensland dentist in Australia. It was revealed to the public when 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.

36 The country code top level domain name registry for Australia, the .au Domain Adminstration Ltd, has instigated legal action to terminate contractual agreements with domain name resellers over security lapses. See *Australian Style Pty Ltd v .au Domain Administration Ltd* [2010] VSCA 184 (23 July 2010). See also, Alana Maurusht, The Tole of DNS Registrars in Combating Botnets (working paper, copy on file with the author).

37 The IIA has issued a draft voluntary code that will implement a bot remediation program: Internet Industry Association, *Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security* (September 2009) <http://www.iia.net.au/images/resources/pdf/esecurity_code_consultation_version.pdf>. I have written 15 000 words on this bot remediation proposal. That paper is currently a working draft that will be submitted for publication in the near future. A copy of the working paper is available upon request. The Parliamentary Report on Cybercrime recommended that ISPs move swiftly to implement bot remediation programs along the lines of the current draft code: House of Representatives Standing Committee on Communications, above n 7, 137–48.

III THE *COUNCIL OF EUROPE CONVENTION ON CYBERCRIME*

The *Convention*, an agreement between member nations of the European Union is the only international agreement in the area of cybercrime. It is unique in that it is open for signature by non-European member states. The US, Canada and Japan have all signed the *Convention*, with the US also ratifying.

The *Convention* may be divided into 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;
2) computer related offences such as forgery and computer fraud;
3) content related offences, in particular the production, dissemination and possession of child pornography; and
4) offences related to infringement of copyright.

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.[39] Recent international gatherings in London and Venezuela were held to address economic cybercrime (computer offences, forgery and fraud). Only these first three categories will be considered in the analysis that follows, with intellectual property crimes excluded from the article.

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

1) expedited preservation of stored computer data;
2) expedited preservation and partial disclosure of traffic data;
3) production orders;
4) search and seizure of stored computer data;
5) real time collection of traffic data; and
6) interception of content data.

---

38 A detailed explanation of the other methods see Alana Maurushat, 'Zombie Botnets' (2010) 7 *SCRIPTed* 370.

39 Intellectual property has been excluded from analysis. Article 10 of 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 ('*TRIPS*'); *World Intellectual Property Organization Copyright Treaty*, opened for signature 20 December 1996, 2186 UNTS 121 (entered into force 6 March 2002). 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.

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 in terms of how a nation might negotiate some of the issues. These may broadly be categorised as:

1) extradition;
2) mutual assistance; and
3) designation of a 24/7 network contact.

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 yield the greatest concerns.

IV SUBSTANTIVE PROVISIONS RELEVANT TO BOTNETS

Table 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 following the table.

Table 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* that I will now address.

The *Convention*'s computer data provisions of 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 herder 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.[40] The *Criminal Code* references 'data',[41] 'data held in a computer',[42] and 'data storage device'.[43] 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 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.

---

40 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.

41 *Criminal Code Act 1995* (Cth) Dictionary (definition of 'data'):

> Data includes:
> (a) information in any form; or
> (b) any program (or part of a program).

42 *Criminal Code Act 1995* (Cth) Dictionary (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.

43 *Criminal Code Act 1995* (Cth) Dictionary (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'.

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 reference botnets to be included as a prohibited device.

The *Criminal Code* does not criminalise the misuse of a device. Devices used to commit internet crimes do not *obviously* (I will speculate below on how I think they might be caught under Australian legislation) appear to be contemplated within the legislation. Where a device is contemplated in the legislation, it is usually a specific type of device with reference to 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.[44] 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 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.

Under both the *Convention* and the *Criminal Code*, it remains ambiguous as to whether a person could lawfully have a botnet without attracting legal scrutiny. Most acquisitions of zombie computers are through unauthorised access, dishonest intent, or in a misleading and deceptive fashion. That said, there is speculation as to whether a consumer could consent to become part of a botnet. A user may use a website service that requires user consent through agreeing to terms of use. Users do not generally read terms of use agreements. Users click the 'I Agree' button only to find several software programs downloaded onto

44 *Criminal Code Act 1995* (Cth) s 100.1 (definition of 'tracking device').

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 manner such that users would not know their systems had been compromised. In Australia, the standard of consent is not one of informed consent.[45] Thus if a consumer clicks the 'I Agree' button, in most cases consent will be valid. A consumer cannot consent through terms of service to unknowingly aid and abet in the commission of a crime or illegal act.[46] Any subsequent use of a botnet for an illicit purpose such as sending some spam marketing illicit drugs or a distributed denial of service attack could not attract consent. However, consent could be granted for a computer to become a zombie for the use of *lawful* spam distribution. Thus, under both Australian law and the *Convention* the mere possession of a botnet, if acquisition is through lawful means and consent obtained, would not be criminalised.

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. 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,[47] 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.

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.

---

45 Simon Blount, *Electronic Contracts: Principles from the Common Law* (LexisNexis, 2009) 72.

46 This is not the same thing as knowingly or recklessly consenting to aid and abet in the commission of a crime. Here the consumer clicks on the 'I Agree' button and consents to vague and ambiguous terms to unknowingly aid and abet in the commission of a crime.

47 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' (25 February 2010) *Microsoft Malware Protection Centre – Threat Research & Response Blog* <http://blogs.technet.com/b/mmpc/archive/2010/02/25/dismantling-waledac.aspx>; Luis Corrons, 'Mariposa Botnet' (3 March 2010) *PandaLabs Blog* <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.

The *Criminal Code* child pornography provisions fully comply with the *Convention* with no differences. Child pornographic materials include written narratives, animated cartoons (such as manga), and fictional depictions of abuse. The recent decision of *McEwen v Simmons* establishes that under NSW and Commonwealth law depictions of sexual acts among the children characters of the American cartoon *The Simpsons* constitute child pornography.[48] A child is defined as a person under 18 years of age for both the *Convention* and *Criminal Code*.

V 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.

A 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 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 but most notably in its operation with the obligation to provide mutual assistance (examined in Part VI(A)).

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

48 (2008) 73 NSWLR 10.

1) enforcing the criminal law and laws imposing pecuniary penalties;
2) protecting the public revenue; and
3) safeguarding national security.[49]

A warrant is required before an ISP is compelled to assist law enforcement or a relevant authority.[50] ISPs are only 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.[51] Absent a warrant, the ISP has discretion as to whether they wish 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 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 as to 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. 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 herder where real time evidence can be collected and communications potentially intercepted. However, real time evidence collection and interception of communications require a warrant under Australian law. The *Convention* does not change this fact of domestic law. Real time evidence and interception requirements are considered in Part VI.

B Production Orders

Production orders often refer to compelling 'subscriber information', in particular in relation to subscription to an ISP or a DNS registrar. Private security organisations and researchers monitor malware and botnets through what is

49 *Telecommunications Act 1997* (Cth) ('*TA*') s 313.

50 In some instances, a certificate may offered 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: *Telecommunications (Interception and Access) Act 1979* (Cth) ss 16, 61 and 185A.

51 *Telecommunications Act 1997* (Cth) pt 13.

known as a virtual honeypot. A honeypot is used to collect samples of malware and botnets. Information is extracted by observing the operations of the botnet such as: how the botnet herder communicates to its zombies, what types of bot (code) it is running, and so on. The next step involves observing the C&C server addressing whether it is receiving its instructions through the IRC or peer-to-peer channels, or via designated websites. Security researchers can often then shut down the C&C of the botnet. The shutting down of a botnet is ideally accomplished with the following information:

- 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).[52]

There are several methods to take down a botnet: ISP and/or DNS registrar shut down, infiltration and disruption of C&C, zombie remediation and prosecution. Often a combination is used.[53]

In order to prosecute a botnet herder, one must first identify the botnet herder. 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 registrar (in the case of dynamic IP addressing, or where the C&C receives instructions from a webpage);
- 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 ascertain the identity of the botnet herder; 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.[54] 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 herder. Where the

52 Schiller et al, above n 13.

53 See, eg, Waledac botnet: Williams, above n 47.

54 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, 15.

botnet herder relies on peer-to-peer for its C&C there is no subscriber information. Production orders will only be useful in prosecution when dealing with lower level botnet herders 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 are explained and further explored in Part VII.

C 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 provisions 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 capacity is to ensure that domestic law enforcement cooperates with foreign law enforcement requests to search and seize a computer for an investigation abroad.

The *Convention* and Australian law are silent on how long law enforcement may seize a computer or a computer system without laying charges. There have been instances where police have confiscated computers, kept them for several months without ever laying charges, and significantly damaged the computers. The *Convention* does not discuss this type of potential abuse.

D Real Time Evidence Collection and Interception Capabilities

Many commentators have expressed fears of the *Convention* establishing an Orwellian system of electronic surveillance.[55] 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.

55 Gianluca Esposito, 'The Council of Europe Convention on Cyber-Crime: A Revolutionary Instrument?' in Roderic Broadhurst (ed), *Proceedings of the 2nd Asia Cyber-Crime Summit* (Centre for Criminology, University of Hong Kong, 2003). See also Jason Young, 'Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation' (2004) 9 *International Journal of Communications Law and Policy*.

Additionally, protection of civil liberties (privacy) and human rights[56] are safeguarded 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 is considered in Table B.

The value of real time forensics is perhaps best illustrated by way of analogy. For example, CCTV surveillance cameras are installed 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.

Real time forensics, operating on a similar premise, functions in two ways: general evidence collection without a suspect in mind, or specific evidence collection with a particular suspect in mind. Let us first consider general collection of real time evidence. ISPs routinely monitor their networks using technologies such as NetFlow. However, such monitoring is not typically done with identification of malicious actors in mind. NetFlow is used to check performance and to provide base data for billing and charging records. Where a crime is committed, a warrant may be issued allowing law enforcement agents to access ISP data logs (if any) stored at the time of the crime. The value of evidence collected post-crime is dependent on the monitoring and detection technologies used by the ISP. Many ISPs use medium packet inspection technologies such as NetFlow. NetFlow does not maintain data logs for long before deleting them.

Where more pervasive technologies such as deep packet inspection are deployed there is potentially more valuable 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 and deep packet inspection technologies are capable of collecting evidence in real time. The term 'real-time evidence' is not, without more, very useful. The importance lies in what type of information is collected by the packet inspection technologies, the length 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 often referred 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: perhaps the type of data collected was not useful; perhaps the type of data was useful but was not

56 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.

stored; or maybe the volume of data collected is too large a quantity to be of use in a timely 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 a content warrant. The communications of the suspect could then be intercepted. Depending on the type of warrant, this could include website contents and email 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 under the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*').

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).[57] Real time data collection allows the capturing of

> volatile information that would not normally be present in a postmortem 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 analyzing the system state.[58]

Without real time evidence, there is heavy reliance on the physical memory (commonly known as random access memory, or 'RAM') of a computer. 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 box to be captured, whether the information is local or remote.[59] Where real time data is stored, law enforcement agents are potentially able to peer at the email 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 people, or information conduits.

In Australia, ISPs were until recently required by law to have interception capabilities,[60] generally to be used for evidence gathering in connection with serious offences (crimes such as murder, terrorism, and child pornography).[61] Previously, interception obligations were limited to serious offences. A serious

---

57 Anthony Reyes et al, *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors* (Syngress 2007) ch 5.

58 Ibid 107–8.

59 Ibid 106.

60 *Telecommunications Act 1997* (Cth) s 324 required carriage service providers (which includes ISPs) to be able to intercept communications passing over the network or facility in accordance with a valid warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth). This provision has been repealed and amended several times. See amending Acts *Telecommunications Amendment Act 1997* (Cth), amending *TA*; *Communications Legislation Amendment Act (No 1) 2004* (Cth), amending *Telecommunications Act 1997* (Cth); *Telecommunications (Interception and Access) Amendment Act 2007* (Cth), amending *TIAA*.

61 *Telecommunications Act 1997* (Cth) s 5D.

offence included any criminal offence that would attract a minimum of seven 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.[62] As there was no minimum sentence specified and no case law 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. 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 as per *TIAA* sections 190 and 191.

Australian ISPs are not legally required to have the ability to collect evidence in real time. However, this obligation is ambiguously implied in section 9 of the *TIAA* stating that interception capabilities are required for 'interception made to or from a telecommunications service'. ISPs still have obligations to intercept communications but they do not have the direct obligation to collect evidence in real time or at least so it would seem. 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 therefore difficult to imagine 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 may not disclose the specifics of the technologies used or how they are implemented.[63] 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 performed in real time. However, the type of technology that is required to access stored communications requires the ability to take a snapshot of a suspect's email box (peer into the actual communication) or website. This is clearly a more pervasive collection of data. This is also real time data collection. To summarise, the *TIAA* and *TA* do mandate interception, but not 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 and interception, both of which require real time evidence technologies. There is therefore no argument that in Australia ISPs would be required to substantially commit additional resources to purchase and operate interception and real time evidence technologies once the *Convention* is acceded to; those capabilities should already exist.

Real time evidence is vital in many cybercrime investigations. In particular, the use of real time evidence technologies allows law enforcement the ability to

62 See *Criminal Code Act 1995* (Cth) 1995 div 477.

63 Enquiries made to several chief information officers of ISPs, as well as forensics experts working for the AFP, repeatedly stated that they were not authorised by law to disclose the types of technologies used for interception and real-time evidence collection. Emails on record with the author.

intercept and search encrypted information. This is perhaps the most distinctive advantage of the use of real time evidence techniques. In post-mortem 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. In a real time or live forensics instance, software (for example, the Pre-Deployed Agent model) can be remotely installed onto a computer system prior to an incident or software programs (for example, BestCrypt or ProDiscover Incident Response) can be initiated once a document is first opened. This 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'.[64] Where the entire system is encrypted, the complete content of the drive can be viewed since, '[s]imply put, because the drive is presently being used, it is unencrypted'.[65] It remains unclear whether ISPs have real time evidence technologies capable of performing the above acts because monitoring of a suspect's computer (and not specifically their email box) is not contemplated with a stored communication warrant. As well, the equipment warrant does not specify whether remote searches are allowed. In this instance a file would be downloaded remotely onto a computer and the entire content of the computer is imaged. Remote searches are considered in Part V(E).

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.[66] 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 ordre public.[67] This exemption would apply to all procedural and international cooperation provisions. Domestic law constraints, including warrants, are considered in Part VII.

E The *Convention* Is Silent on Transborder Remote Searches

'Transborder remote searches' refers to the situation where law enforcement agents in one jurisdiction will remotely install a keylogging program onto a suspect's computer in another jurisdiction. The *Convention* is silent on this point. Many jurisdictions such as the European Union have legalised overseas remote

64 Reyes et al, above n 57, 96.
65 Ibid 99.
66 *Convention* art 34.
67 Ibid arts 27(4), 29(5), 30(2).

computer searches.[68] Police in some European nations have been using remote searches without warrants for several years. The German Constitutional Court recently ruled that the practice of cyber-spying violates privacy rights.[69] German police will still be allowed to use remote searches but only in exceptional cases under the auspice of a judge. The German police have estimated that they will likely need to use remote searches approximately 10 times per year.[70] The European Union Council of Ministers will expand a statute permitting warrantless surveillance including remote searches of email, instant messaging and internet browsing history.[71] The Home Office of the UK have also authorised remote searches by police.[72] In jurisdictions such as the US, 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 § 1030 (1986), as well as 20 counts to conspire and a number of fraud counts.[73] The evidence was collected

68 Chatham House Rule: closed panel on Cybercrime at AusCERT Conference 2008. Law enforcement agents from the AFP, NSW, Germany and the FBI were present. Chatham House is the colloquial name for the Royal Institute of International Affairs in London, located in Chatham House. The Chatham House Rule is invoked at meetings to encourage free and unfettered discussions. According to the Chatham House website, the rule states that:

> When a meeting, or part therof, 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 Royal Institute of International Affairs, *Chatham House Rule*, <http://www.chathamhouse.org.uk/about/chathamhouserule>.

69 The state jurisdictions of Bavaria (Bayern), Rhineland-Palatinate (Rheinland-Pfalz) and (North Rhine-Westphalia Nordrhein-Westfalen) have enacted policing laws (Polizeirecht) that allow for remote searches. The Federal Constitutional Court of Germany has limited the law on remote searching: Bundesverfassungsgericht [German Constitutional Court], 1 BvR 370/07 and 1 BvR 595/07, 27 February 2008 reported in (2008) 120 BVerfGE 274.

70 Ibid. When questioned during the case challenging the constitutional limit of remote searching, the police responded that this type of search is necessary about 10 times per year. This does not mean 10 times per year in Germany, but 10 times per year in the state jurisdiction of North Rhine-Westphalia.

71 The operational measures to police cooperation in cyber crime were expanded to include cyber-patrols, joint investigation teams across borders and remote searches. The Council of Europe adopted this strategy in 2008: Europa, 'Fight against Cyber Crime: Cyber Patrols and Internet Investigation Teams to Reinforce the EU Strategy' (Press Release, 27 November 2008) <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827>.

72 David Leppard, 'Police Set to Step Up Hacking of Home PCs', *The Times* (online), 4 January 2009 <http://www.timesonline.co.uk/tol/news/politics/article5439604.ece>. See *Computer Misuse Act 1990* (UK) cl 18 s 1(1).

73 *United States v Gorshkov*, 2001 WL 1024026 (WD Wash, 2001) (23 May 2001).

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'.[74] 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.[75]

The content warrant framework, as will be seen in Part VII, 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. The mere identification of a botnet master by no means secures successful prosecution. In the recent investigation of the Mariposa botnet, it is possible that the botnet masters will not be successfully prosecuted. This is due to the tardiness of the Spanish government to enact computer misuse offences in spite of the fact that Spain ratified the *Convention* a decade ago. It remains to be seen if the evidence collected and obtained by security researchers will stand up in court or 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. The accused was an 18 year old male, Owen Walker, of New Zealand. Walker (known as Akill in the hacking world and suffering from mild autism) distributed a number of adware and spyware programs including DollarRevenue Software and was found guilty of accessing a computer system without authorisation under section 252(1) of the *Crimes Act 1961* (NZ). Walker was dismissed without conviction and fined NZ$9526.[76] The dismissal without conviction was due to Walker's lack of criminal intent as his motive stemmed from fascination with computers – all this despite the fact that Walker was paid thousands of dollars from adware and spyware companies.

---

74 Ibid. Gorshkov was sentenced to serve 36 months and ordered to pay US$690 000 in restitution: 'Russian Hacker Gets 3 Years in Jail', *MSNBC* (online), 4 October 2002 <http://www.msnbc.msn.com/id/3078748/ns/news-internet_underground/>.

75 Russell Smith, 'Impediments to the Successful Investigation of Transnational High Tech Crime' (2004) 285 *Trends & Issues in Crime and Criminal Justice* 1, 3–4.

76 *R v Walker* [2008] NZHC 1114 (15 July 2008) [38] (Potter J).

If more botnet masters are to be brought to justice, and in particular the ones tied to organised crime and serious fraud, law enforcement agents will need to be given the tools that security researchers use. Security researchers are able to gather intelligence through virtual honeypots, infiltrating 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 *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 that such a tool would have any significant impact on botnet investigations and prosecution but that 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 (for example, terrorism, child pornography, human trafficking, and 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 auspice 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.

F The *Convention* Does Not Make Traceback Any Easier

To continue with our example of a botnet, the greatest obstacle to 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 the large amount of resources and money required compared with the amount of damages suffered. Exploitation of this phenomenon is often described as the 'de minimis trap' or the 'salami technique'.[77] As David 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.[78]

---

77 According to Security Beyond Borders, 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': Security Beyond Borders, *Global Security Glossary – S* <http://www.securitybeyondborders.org/global-security-glossary-s/>.

78 David Wall, *Cybercrime* (Polity Press, 2007) 161.

In other words, these thieves steal a little bit of money from a lot of people who are located in many countries. The de minimis amount necessary to commence an investigation is not met. The capacity of law enforcement to investigate botnet related crimes in these situations is therefore limited.

Traceback is difficult predominantly due to the obfuscation methods deployed by malware actors – typically organised crime groups. Organised 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/multi-homing, fast flux DNS, distributed command and control (superbotnet), encryption, obfuscation and the move from open IRC channels to closed peer-to-peer channels. These tactics allow the host to roam and change intermittently as required to keep a botnet functioning. Malware operators employ the same stratagem to keep spam and illicit content rotating. These 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 Guillaume 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 (aka, 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 (aka, 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.[79]

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, betray who used a computer to perform a crime. If a computer is used by several people, identifying the botnet master will require additional evidence other than a mere IP address. The botnet master may only be targeted upon discovering where the C&C is occurring and tracing back through proxies to the original source. However,

79 Guillaume Lovet, 'Fighting Cybercrime: Technical, Juridical and Ethical Challenges' (Paper presented at the Virus Bulletin Conference 2009, Geneva, 23 September 2009) 65.

discovering the C&C point where a botnet receives its instructions from 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 that may or may not prove successful.

Even 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 money mule.[80] Money mules refer to those who, often innocently and unknowingly, launder money on behalf of criminals. The more effective method of traceback may be to follow the money trail.

VI 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'.[81] This cooperation is divided into three categories, considered below, with particular focus on mutual assistance provisions.

A Extradition

There has been much incorrect commentary surrounding the *Convention* over extradition and mutual assistance matters. This statement from Dan Manolescu's master's thesis 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.[82]

The *Convention* does not supplant existing provisions in extradition treaties. It deems articles 2–11 extraditable offences in existing treaties:[83] 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

80 Most cases where a botnet might have been used in Australia involve denial of service attacks by former disgruntled employees. In Australia, much cybercrime investigation is targeted on money mules: above n 68; the AFP and members of state police squads were present.

81 *Convention* art 23.

82 Dan S Manolescu, *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.

83 *Convention* art 24(2).

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 and are not likely to be done.[84] The *Convention* conveniently allows the incorporation of 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'.[85] Furthermore, parties do not have to impose criminal liability for copyright related offences where there are other effective remedies in place.[86] 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 herders has been sought anywhere in the world. In the case against Owen Walker extradition was not sought. He was tried in New Zealand despite the 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.

B 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*:

---

84 Broadhurst, for example, 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, 418.

85 *Convention* art 24(1).

86 *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.[87]

Yet the preamble to the *Convention* contains strong language of the importance of the needs of law enforcement with human rights and 'the rights concerning the respect for privacy'. The primary privacy complaint of the *Convention* is rooted in the false premise that the *Convention* does not allow for 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 in Part V(A) 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 analysed in Parts IV and VII. Moreover, parties may under the *Convention* require dual criminality for mutual assistance, as will be explored below.[88]

Dual criminality is allowed under the *Convention* with the exception of preservation of data. Stipulation of dual criminality is not allowed in mutual assistance requests for preservation of stored computer data.[89] Preservation of data obligations, however, do 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 (discussed in Part VII). 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.[90] 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 as to why preservation of stored computer data is 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

87 Adrian Bannon, 'Cybercrime Investigation and Prosecution: Should Ireland Ratify the Cybercrime Convention?' (2007) 3 *Galway Student Law Review* 115, 132.

88 *Convention* art 25.

89 Ibid art 29(3).

90 Lovet, above n 79, 68.

importantly, the particularly useful portion of data preservation consists in identifying connectivity points as a criminal 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.

C 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). One expert states that '[t]he establishment of this network is one of the most important provided by the *Convention*'.[91] The Convention further mandates that such network personnel must be trained and equipped.[92]

VII THE *CONVENTION* MUST BE APPLIED USING THE SAFEGUARDS PROVIDED IN DOMESTIC LAW

The *Convention* does not change the fact that content monitoring (whether the request is made by domestic or foreign law enforcement) must be done in compliance with domestic law. In Australia, this means that a warrant will be required.[93] The warrant framework may be used to compel an ISP or similar entity to collect, preserve and intercept communications. In theory, warrants could be issued to gather evidence about a botnet, the infected bots and to identify the botnet master. As will be seen in Part VIII below, 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

91 Broadhurst, above n 84, 421.
92 *Convention* art 35(3).
93 See Table B, below, for authority and explanation.

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 purview of the *TIAA*. Call charge records, by contrast, are regulated by the *TA*.[94] It is prohibited to monitor and disclose the content of communications without the customer's consent.[95] Unlawful collection and disclosure of the content of a communication attracts both civil and criminal sanctions.[96] The *TIAA* and *TA* expressly authorise a range of disclosures including to specified law enforcement and revenue protection agencies. The content warrant regime in Australia is inherently complex. Table B, below, maps the various types of warrants required in Australia for content monitoring and details the different requirements for each type of warrant.

Table B: Content Warrant Framework in Australia

Type of warrant	Legislation	Requirements and range of botnet activities
Part 2-2: Telecommunications Interceptions Warrant	*TIAA* Part 2-2	Issued by the Attorney-General under request of the Director of Security or ASIO in connection with national and foreign intelligence. Must be in writing, with specified duration, identification of suspected telecommunications system or named person, and reason (offence) the 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 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	*TIAA* Part 2-5	Not issued by the Attorney-General but by a judge or other agent nominated by the Minister. Requests are from the AFP, the state police and a number of commissions connected with policing (for example, Australian Criminal Commission). Required, for example, for collecting evidence of a denial of service attack of non-government website or server; any unauthorised access, modification or impairment of

94 *Telecommunications Act 1997* (Cth) pt 13.

95 *Telecommunications (Interception and Access) Act 1979* (Cth) s 7: prohibits disclosure of an interception or communications; *Telecommunications (Interception and Access) Act 1979* (Cth) s 108: prohibits access to stored communications.

96 Criminal offences are outlined in *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2-9 while civil remedies are outlined in *Telecommunications (Interception and Access) Act 1979* (Cth) *1979* pt 2-10.

		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	*TIAA* Part 2-3	May be requested by the police 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	*TIAA* Schedule 1.	Issued by the Attorney-General if request is from the Director of Security or ASIO. Issued by a judge or magistrate when requested by law enforcement. Application may be in writing or by telephone, with respect to a telecommunications system or named person, and must outline the grounds (offence) the application is based on. May only be issued to access stored communications and does not apply to communications in transit. Required, for example, for an examination of the content of an email or the entire collection of email messages if they are stored on the ISP's server – used to collect evidence once the identity of a botnet master is known.
B-Party Warrant	*Telecommunications (Interception) Amendment Act 2006* (Cth) ('*TIA 2006*') Schedule 2, amending *Telecommunications (Interception) Act 1979* (Cth) ('*TIA 1979*')	Issued by the Attorney-General if the request is from the Director of Security or ASIO (valid for three months). Issued by judge or magistrate when request from law enforcement (valid for six 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 offence is unknown. For example, examination of compromised machines/bots to see how they connect to the C&C.
Equipment based Warrant	*TIA 2006* Schedule 3, amending *TIA 1979*	Issued by the Attorney-General under request made by the Director of Security. Allows interception of telecommunications devices. Required, for example, for the examination of a piece of equipment (ie a computer), including imaging its entire content, not just the content of an email box. There exists indication if remote examination of the device is allowed by downloading software onto the suspect's computer.
No warrant required	*Telecommunications (Interception and Access) Amendment Act 2010* (Cth),	Carriage service (for example, an 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

	amending *TIAA*	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 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 botnet investigations 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 not even then the technical ability, depending on the department)[97] to perform many of the tasks required to gather intelligence on botnets. The *Convention* does not alter this.

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 with only one 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. This could means that they would require information about either the C&C, the botnet master, or the infected bot machines that form part of the botnet.

If law enforcement agencies had location information of the C&C of Dumb Botnet (for example, receiving instructions from <www.netar.com.au>)[98], 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 reveal 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>.

97 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.

98 This is a fictitious website name.

Law enforcement agents would need to make a request using the WHOIS protocol to access subscriber information for a domain name or IP address.[99]

ISPs send subscriber information to the WHOIS servers that keep a comprehensive database of subscribers' information. This protocol allows certain types of people (law enforcement in some instances) to obtain the subscriber's name along with contact details. The reality, however, is that fake identification details and stolen credit cards are often used to register ISP and domain name services. The subscriber information, therefore, whether it is found with WHOIS or through a production order will be of little use. 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 the C&C location was known (<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 infected bots, 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). At the end of the day, these types of traceback methods are likely to lead only to false subscriber information and are, therefore, of little utility.

If law enforcement only had information about which computers were infected as bots, 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 the police knew the IP address of the botnet master they could request a 'named persons' Part 2-5 Telecommunications Interception Warrant. They could then monitor 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 any 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 or her with the crime. It is possible that in a situation like that of Dumb Botnet existing content monitoring provisions are sufficient for law enforcement agencies to investigate a botnet master. The

99 Other protocols such as the Internet Registry Information Service ('IRIS') are being developed by the Internet Engineering Task Force to eventually replace the WHOIS protocol. It is hoped that IRIS will be less privacy invasive, reduce the use of databases for marketing, allow more efficient access by law enforcement and increase the accuracy of the contents of the database. See WHOIS Task Force 1, *Restricting Access of WHOIS for Marketing Purposes: Preliminary Report* (2010) Internet Corporation for Assigned Names and Numbers <http://gnso.icann.org/issues/whois-privacy/Whois-tf1-preliminary.html>.

problem with this example is that even the amateurs operate much more sophisticated botnets than the aptly named Dumb Botnet.[100]

In a *typical* botnet, there will be several C&C locations to retrieve instructions. Many botnets will change the location of the C&C every week, others every day. Web pages of C&C are typically registered with domain name registrars 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 cybercrime 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, whereby their IP address changes every 20 minutes. Additionally, many communications sent to the C&C are encrypted and thus not easily detectable. 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 location, or from a set default. Many botnets contain hundreds of thousands if not millions of infected bots. A B-Party warrant would be possible in this instance for an infected bot located in Australia, though not much information leading to prosecution of a botnet master may be gained from such a warrant.

In summary, warrants by law enforcement to investigate botnets are of limited use. The botnet Torpig is examined below to highlight this point.

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.[101] They used a virtual honeypot[102] 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, Computer Emergency Response Teams ('CERTs') and other security researchers.

The UCSB research team was able to infiltrate the Torpig botnet for 10 days. During this time, through a reverse engineering of the domain generation algorithm, they discovered that there were two C&C methods. The first C&C used encrypted hyper-text transfer protocol ('HTTP') protocol linking to domain names. The botnet was not detected by any antivirus or anti-spyware programs. The backup C&C was located in a separate botnet known as Mebroot located in 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

100 *R v Walker* [2008] NZHC 1114 (15 July 2008).

101 Stone-Gross et al, above n 24.

102 Thorsten Holtz and Niels Provos, *Virtual Honeypots: From Botnet Tracking to Intrusion Deletion* (Addison-Wesley, 2007). The authors describe a honeypot as a computing resource that they want to be probed, attacked and compromised in order to closely monitor the botnet or malware.

botnet switched C&C through a rapid fast flux of every 20 minutes.[103] UCSB recorded 180 000 unique hosts (compromised computers) connected to the botnet. The researchers infiltrated this botnet for exactly 10 days. During these 10 days they observed banking details from over 8310 accounts, 1660 credit cards, and 410 financial institutions reporting data back to the botnet master.

The researchers describe how the banking information was obtained:

> 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 (eg, 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 is shown in … [in which] 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.[104]

The researchers recorded the phishing scams noted that 14 per cent related to jobs and resumes, 7 per cent to money making, 6 per cent to sports fan sites, 5 per cent to exams and websites on worrying about grades, and (perhaps contrary to popular myth) only 4 per cent were related to sex.[105] The researchers reported that the banking information collected was sold to multiple parties in the underground economy. Researchers at the security corporation Symantec also followed the Torpig botnet noting that credit cards were fetching a rate between 10 cents and USD$25 while bank accounts were worth between USD$10 and

---

103 Richard A Kemmerer, 'How to Steal a Botnet and What Can Happen When You Do' (Speech delivered at Google Tech Talk, 10 September 2009) <http://www.youtube.com/watch?v=2GdqoQJa6r4>.

104 Stone-Gross et al, above n 24, 637 (emphasis altered) (citations omitted). URL stands for Uniform Resource Locator, and is a websites unique identifer. SSL is short for Secure Sockets Layer. SSL is a known encryption technology used in many electronic commerce applications. Phishing is a process of tricking recipients into sharing sensitive information with an unknown third party.

105 Kemmerer, above 103.

USD$100 with total profit estimates anywhere from USD$83 000 to USD$8.3 million.[106] Evidently, financial gain motivates Torpig's botnet master(s).

The researchers expressed concern firstly about being pursued by law enforcement and secondly about potential retribution victims, as they openly expressed strong beliefs that Torpig originated in Eastern Europe and is be linked to organised crime).[107] The researchers contacted the FBI during the timeframe that they infiltrated the botnet. Once notified, the FBI repatriated the data and sent it to the National Cyber-Forensics and Training Alliance. The FBI made requests to shut down the domain names of the documented C&C. The UCSB researchers note that the very instance that the FBI were notified, the C&C migrated from domain names to the rootkit botnet, Mebroot. As the researchers note, this is likely not a coincidence.[108] The Mebroot botnet is encrypted. No researcher has to date been able to crack Mebroot's encryption.

As highlighted in the Torpig botnet takedown, once law enforcement became involved in takedown, the C&C automatically shifted to a much more secure method using a newly 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.

VIII THE EFFECTIVENESS OF THE *CONVENTION*

There are many indications that the *Convention* has a long way to go before it will be an effective tool in combating transnational cybercrime. Many countries that have signed the *Convention* have yet to ratify it. Canada and Spain, for instance, while signatories, have not yet ratified.[109] As of March 2010, 46 countries had signed but only 26 had ratified the *Convention*.

There is indication that the procedural tools provided in the *Convention* have been under utilised. Research indicates that countries like Romania and the Ukraine, that have ratified the *Convention* and are hotbeds of cybercrime activity, have received a paucity of international requests under the *Convention*.[110] The Ukraine also has yet to have designated a 24/7 network contact.[111] The *Convention*'s requirement of a 24/7 contact duplicates previous initiatives by

106 Symantec, *Report on the Underground Economy* (November 2008) <http://www.symantec.com/content/en/us/about/media/pdfs/Underground_Econ_Report.pdf>. Many statistics and research about cybercrime and cyber security is conducted by security corporations that specialise in anti-virus and other types of security software.

107 Kemmerer, above n 103.

108 Ibid.

109 Council of Europe, *Convention on Cybercrime* (1 September 2010) <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

110 Lovet, above n 79, 69.

111 Ibid.

Interpol and the Group of Eight to establish similar international contact networks. Multiple points of network contacts may be confusing and ineffective.

The *Convention* is the only international instrument of direct relevance to botnets. The *Convention* has been criticised as repugnant to privacy protection, in particular to free and anonymous speech online.[112] 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 like the US or Canada. By contrast, any *Convention* provisions adopted in Canada that may be repugnant to civil liberties may be challenged under the *Canadian Charter of Human Rights and Freedoms*;[113] the same safeguards are not present in Australia. There is therefore a need to be particularly cautious in adopting procedures that impact on civil liberties. It does not follow, however, that absent a Bill of Rights, Australia should not accede to the *Convention*.

The substantive provisions in the *Convention* are similar to Australian law though some changes are needed to enable Australia to comply with the *Convention*, should it become a signatory. The misuse of a device provision should be added to the *Criminal Code*, along with the specific exemption for security researchers. Botnets should be specifically referenced as a device. As this paper has demonstrated, this type of provision is to likely to be one of the most important provisions for successful prosecution of a botnet herder. Additionally, Australia may have to adopt specific provisions for computer related forgery and fraud though we have seen that under the *Criminal Code* the current provisions are sufficiently broad as to include their computer related counterparts.

From a domestic perspective, the procedural requirements under the *Convention* do not alter Australian law. Australian ISPs already have interception and real time evidence collection capabilities. Preservation of data, production orders and search and seizure of computer systems are already required under Australian law for the purpose of criminal investigations. The provisions compel law enforcement and ISPs to fulfil similar duties as they would if a local criminal investigation extended such duties to those law enforcement agents abroad 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 become potentially 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.

112 Young, above n 55.

113 *Canada Act 1982* (UK) c 11, sch B pt 1 ('*Canadian Charter of Rights and Freedoms*').

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 precondition 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 absent a valid warrant.

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 foreign 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 herder. Ratifying the *Convention* could also allow law enforcement to use live forensics investigations to follow and preserve evidence of illegal bot activity.

The *Convention*'s mutual assistance provisions are highly diluted as countries with significant cybercrime industries, like Russia, are not party to the *Convention*. Even if nations such as Russia were to sign the *Convention*, there remains scepticism that sufficient resources would be allocated to law enforcement to enable investigation. The fact is that in many nations, cybercrime and e-commerce are under enforced. Priority inevitably goes to crimes where the victims are local. The *Convention* does not alter this.

The popularity of botnets as a cybercrime tool did not fully emerge until 2004, which saw a shift to monetisation of malware and botnets. Many of the emerging obfuscation technologies render traceback of botnet herders difficult and the likelihood of the prosecution of sophisticated botnet herders is rather unlikely. Nonetheless, the *Convention* remains of some utility to law enforcement. Where information may be gathered about a botnet herder (perhaps through following the financial trail or through information trading when prosecuting other malicious actors in order to strike a better deal), identification of the botnet herder 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 cybercrime illegal.

As seen with the Mariposa botnet takedown, there is needed a more public and coordinated effort between the security companies, ISPs, researchers, DNS registrars, and law enforcement to both takedown botnets and prosecute botnet herders. 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 bear 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 behind whose legal loopholes botnet herders can hide. From a policy perspective, it is my view that Australia should accede to the *Convention* with the knowledge that the *Convention* will not significantly aid law enforcement to tackle cybercrime. The use of modern obfuscation tools impacts on law enforcement's ability to combat many forms of cybercrimes. Much work needs to be done.

Interpol has been an underutilised 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 track, mitigate and eventually prosecute botnet herders. 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.

Cybercrime will need to be addressed through changes to protocol, education and training of end users and businesses, more secure practices by business, continued efforts by software and hardware companies to produce more secure products. Governments must be called upon to regulate internet governance structures such as DNS registrars and to impose codes of conduct for ISPs where the industry has not performed satisfactorily in helping to better protect users from cybercrime.