Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Inquiry into Cyber Crime

Submission to the Standing Committee on Communications on the inquiry into cyber crime and its impact on Australian consumers

Alana Maurushat
Lecturer and PhD Candidate, UNSW Faculty of Law
Deputy Director
Cyberspace Law & Policy Centre, UNSW Faculty of Law

September 9, 2009

1.0 Introduction

Thank you for the invitation to make a submission on the inquiry into cyber crime and its impact on Australian consumers.

This submission is by researchers at the Cyberspace Law & Policy Centre (CPLC) <http://www.cyberlawcentre.org/>, University of New South Wales Faculty of Law. CPLC is a public interest centre focused on representing the user's perspective in public policy. Alana Maurushat, the Centre's Deputy Director, is finishing a PhD in the area of Internet Security and Cybercrime. A portion of this submission is taken from her graduate research, **"The Malware Matrix: Combating the Commercial Malware Industry Through Security Policy".** The Centre is indebted to student research interns Shannon Kalish for her work on the submission, and to Pauline Rapaport and David Vaile for their comments.

In the following pages we make a number of submissions on aspects of cybercrime. We have made an effort not to duplicate submissions made by other organizations. We are supportive of most of the submissions made by other organizations, and would like to acknowledge in particular the excellent and accurate submissions of the ABA and isoc-au. Our submission is written from the perspective of the consumer and is focused on proactive techniques, unlike the current reactive techniques used predominantly within the fight against cybercrime. Our submission addresses:

b) Botnets;
d) i) Education Initiatives; and
e) Future Initiatives to Mitigate E-Security Risks

2.0 Summary

2.1 Botnets

Botnets are the predominant vehicle for cybercrime. Any new policy efforts in the cybercrime area need to address emerging botnet techniques. Policy needs to be proactive as opposed to reactive. Prosecution in this area should be limited and targeted. There exist a number of significant challenges to prosecution: victims often unknown, collection of digital evidence, evaluating damages, continual propagation of botnet, and the ability of organized crime to take over a dormant botnet. Australia should remain active in its current initiatives at the OECD level and AISA but extend its type of data collection relevant to these studies.

2.2 Education Initiatives

The Australian government has launched a series of education campaigns on Internet safety. To date, there has been no transparent consideration of where education campaigns are likely to succeed and where they will be ineffective based on the type of techniques used in cybercrime. Education will play a pivotal role for ***some*** types of cybercrime such as some forms of social engineering, Eg. the Nigerian lotto scams. For other types of cybercrime (phishing, web-base malware) user education will play no role for consumers. It is important to look at the types of cybercrime that education may offer benefits, and others, where education of consumers will not present any gain based on evidence-based research.

2.3 Future Initiatives

There is a strong need for a type of centre similar to the United State's **National Cyber Forensics and Training Alliance (NCFTA)** run by Ron Plescoe (and Andy Purdy). The NCFTA acts as a cybercrime hub or a clearing house for information on cybercrime. They liase with organizations who are victims of cybercrimes such as fraud, DDOS, and corporate espionage – much of their work is with financial institutions. The NCFTA operates as an intelligence hub. In doing so, they also work with appropriate law enforcement agencies to bring forth *targeted prosecution* and work with organizations to mitigate attacks. We recommend something a similar clearing house or intelligence hub for cybercrime be formed or that an existing centre such as the Australian High Tech Crime Centre perform this function.

3.0 Botnets

3.1 Botnets as the Predominant Vehicle for Cybercrime

Botnets are a major vehicle for the commission of cybercrime. **Botnets are said to be involved in most forms of cybercrime and civil wrong ranging from sending spam, to denial of service attacks, to child pornography distribution, to worm propagation, to click-fraud, to keylogging technology and traffic sniffing which**

captures passwords and credit card information, and to mass identity theft. [1] In the words of leading botnet researcher Jeremy Linden of Arbor Networks, "Almost every major crime problem on the Net can be traced to them."[2] One must stop and reread this: almost every major online crime may be traced to botnets. Internet security guru Vincent Cerf[3] has equated botnets to a pandemic, warning that a quarter of all personal computers have already become bots.[4] The most accurate figures on botnets may be found by the non-commercial organization **Shadowserver** http://www.shadowserver.org/wiki/. They are a group of voluntary security experts from around the globe who perform detailed analysis of botnets and malware. Their statistics and methodologies are well respected in the field, partially as they do not have a commercial interest.

The "command and control" (C&C) of the botnet often occurs in the IRC server or network allowing a botmaster or a bot herder to control the bots remotely to perform activities which tend to be of a malicious nature. Most botnet dismantling and prosecution of botnet herders is based on older forms of botnets who operate in teh IRC channel. Botnets, however, are now leveraging peer-to-peer networks and what will likely be on the horizon in the near future, mobile phones – **p2p and mobile phone mediums present additional challenges to shutting botnets down, mitigating harm, and collecting digital evidence for prosecution.** Any new policy efforts in this area will need to address emerging botnet technology and its related challenges.

3.2 Select and Targeted Approach to Botnet Prosecution

In any event, we feel that only select and targeted prosecutions of botnet herders should be pursued. **The emphasis, instead, should be squarely placed on proactive measures as opposed to reactive measures.** Put another way, offensive manoeuvres as opposed to defensive manoeuvres. **It follows that any cybercrime policy should place a significant emphasis on the disruption and dismantling of botnets, as opposed to mere prosecution of botnet herders.**

To date there have been no public prosecutions in Australia of botnet herders. In fact, there is a paucity of prosecutions on the international front as well. Those botnet herders who have been prosecuted tend to come from the lower end of the cybercrime chain, and do not represent botnets run by organized crime groups.

The United Nations has funded a project targeted at understanding the motivation and possible deterrents of computer hackers. The Study, "Profiling Hackers"[5], provides an ongoing and detailed survey of computer hackers around the globe. The findings are not only

---

[1] Rychlicki, T. "Legal Issues of Criminal Acts Committed Via Botnets." (2006) Computer and Telecommunications Law Review 12(5), p. 163.
[2] Quote taken from Berinato, S. "Attack of the Bots" Wired Magazine Issue 14.11 (November 2006).
[3] 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.
[4] Presentation given at the World Economic Forum 2007. The statistics have been highlighted in a number of news reports and blog sites. See, for example, Anderson, N. "Vint Cerf: one quarter of all computers part of a botnet" (January 25, 2007) Ars Technica available at http://www.arstechnica.com/news.ars/post/20070125-8707.html.
[5] Chiesa, R., Ducci, S. And Ciappi, S. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* (UNICRI, CRC Press, 2009).

interesting but directly relevant or helping governments to develop a targeted approach to prosecution. The Study divides hackers into nine groups: wannabe lamer, script-kiddies, cracker, ethical hacker, skilled hacker, cyber warrior, industrial spy, government agent, and military hacker. The Study directly asks about the deterrent effect of laws, sentences and technical difficulties. The law provided had a deterrent effect for only two of these groups: script kiddies and ethical hackers. The law did not deter professional hackers from engaging in hacking and cybercrime in general. This is another reason why prosecution seems to warrant a lower priority than disruption.

An analysis of two prosecutions of script kiddies is provided below:

Two botnet herders, highlighted below, were arrested under the FBI-initiated "Operation Bot Roast". They were both tried for their botnet activities. Robert Bentley, a 21 year-old male from Florida pleaded guilty (when?) to accessing a computer without authorization (known as LSDigital). Bentley illegally installed DR software on a number of European computers using his botnet. He is currently serving a 41-month sentence and was fined $65,000 USD for his activities. While such arrests may appear promising, as investigating officer Duckin admits, "Bentley doesn't count as 'Mr. Big' in the world of cybercrime."[6]

The other arrested botnet herder 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 DR Software and was found guilty of accessing a computer system without authorization under section 252(1) of the *Crimes Act (NZ)*. . Walker was dismissed without conviction and fined $9526 NZD.[7] 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. The court identified four factors relevant to the assessment of an appropriate sentence: 1) the reason for the offending; 2) whether the harm was to a business enterprise or suffered by individual victims; 3) whether the actions would likely cause a loss of confidence in computer systems in general; and 4) whether there was a possibility of harm continuing after apprehension of the offender. The judge found that no aggravating factors were found in the case. In the judgment, there was notice that Walker was offered a position with large computer corporations as well as interest from the New Zealand police subsequent to his arrest. [8]

These are just two of a number of cases internationally which throw doubt on the viability of this sort of prosecution as an effective measure.

3.3 Impediments to Prosecution and Perpetual Nature of Botnets Once Dismantled

If Australia begins to pursue botnet herders, it is important to know that any botnet convictions would likely be fraught with the same impediments as those in the Bentley and Walker trials.

---

[6] The judgment has is unreported. Details from the case may be found in news articles. The quote in question is from Sopho, "Sopho Assists Computer Crime Unit in Bringing Botnet Master to Justice" June 12, 1008 available at http://www.sophos.com/pressoffice/news/articles/2008/06/bentley-imprisoned.html

[7] *R. v. Walker* HC HAM CRI2008-0750711 [2008] NZHC 1114 (15 July 2008)

[8] Chiesa, R., Ducci, S. And Ciappi, S. Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking (UNICRI CRC Press, 2009).

Firstly, it is extremely difficult to prove actual damages. In Walker's case, only the University of Pennsylvania was able to bring evidence forth of $13000 in damages in spite of the fact that the illegally installed software from the botnet infected 22 million computers. Admittedly, the portion attributable to Walker's activities is unknown. The University of Pennsylvania is often the entity who claims damage for such actions as they host the world's largest computer security research centres, are host to the US CERT and is also home to the National Cyber Forensics and Training Alliance (this expanded in 5.0 Below). **Finding defendants for botnet prosecution imposes an additional challenge.**

Second, the resulting harm does *not* stop once the botnet herder ceases to operate a botnet. Most botnets are self-replicating like worms. Worms self-replicate, are self-sustaining, and are capable of operating independently for an indefinite period. Once the botnet is up and running, it continues to infect machines. Any form of prosecution must be followed up by a "cleaning-up process" to disinfect bots.

Third, dormant botnets are susceptible to being taken over by other botnet herders. A common botnet program takes over an already infected computer rendering the bot part of a new botnet, or the herder merely infiltrates the already established botnet and begins initializing new command and controls. Botnets run by amateurs such as Walker and Bentley are susceptible to being taken over by organized crime groups.

For these reasons, it is important to focus on disrupting active bots and cleaning up dormant bots.

3.4 Australia's Role in OECD Malware Initiatives

We are encouraged to see Australia playing a leading role in the various OECD Malware Initiatives.

In particular, the study underway by the **OECD Economics of Malware: Addressing the Security Externality of End Users** is precisely the type of funded empirical research desperately missing in the field. The Study, announced in 2009, has a few principle objectives which are outlined below:

1) Quantitatively and qualitatively analyze the degree and ways in which ISPs manage side effects (*i.e.* the externalities) generated by some types of end user behaviour. By analyzing a large data set of malicious traffic emanating from ISP networks worldwide, the study can assess the security performance of ISPs and determine the factors that influence their relative performance (such as size, geographic location, types of security measures adopted, etc.).

2) Quantitatively and qualitatively analyze the degree and ways in which financial service providers mitigate end user externalities. By collecting and synthesizing the fragmented data currently available in OECD member countries on internet-based financial fraud as well as its countermeasures, the study can assess the degree to which financial service providers mitigate end user externalities.

By measuring outbound spam, statistics relating to spambots will likewise be generated. The outcomes of these types of studies should prove beneficial for Australia in adopting a proactive approach to botnets and malware.

3.5 Internal Australian Botnet Initiatives

The ACMA developed the **Australian Internet Security Initiative (AISI)** in 2006 to involve ISPs in tackling botnets. ACMA delivers botnet data to the ISPs involved in the project. The ISP can then elect to inform the customer that their computer has been compromised, and perhaps resolve the problem. **To date, there is no publicly available information assessing the program's success.** In short, we do not know how many consumers were actually contacted by ISPs to disinfect their computer (bot), whether such attempts were feasible from a consumer's perspective, the likelihood of re-infection, and what types of costs ISPs absorbed in time and effort to disinfect machines. Such projects that encourage a "cleaning up of one's backyard" approach should be encouraged while more statistics should be generated from these types of projects.

4.0 Education Initiatives

Education will play a pivotal role for ***some*** types of cybercrime. For other types of cybercrime, user education will play **no role** for consumers. **While there are a number of education initiatives underway by the Australian government as identified in other submissions, it is important to look at the types of cybercrime that education may offer benefits, and others, where education of consumers will not present any gain.** This may be somewhat counterintuitive in an environment where consumer and industry education are often characteristics of the problem here which throw doubt on the relative potency of such programs.

4.1 Where Education will Have a Limited Effect

Many people believe that phishing may be successfully combated with user education and training. The empirical evidence, however, suggests that education and training will have little to no effect on phishing. This suggests that any national approach to cybercrime which is over-reliant on user education and training is likely to be deficient.

4.1.1 Social Engineering and Phishing Studies:

1) A study conducted by the School of Computer Science, Carnegie Mellon University Hong Kong University was done to test participants' ability to identify phishing web sites before and after training. It was found that the training made participants more cautious and paranoid but did not make them more effective in combating phishing.

http://www.ecom-icom.hku.hk/seminar/20080527/CombatingPhishingAttacks.pdf

2) The same outcome was found in a study conducted by the School for Informatics, Indiana University. Their study showed that education does affect the subject's judgment, but more in terms of making them more suspicious than in improving their ability to distinguish phishing from legitimate emails.

http://www.informatics.indiana.edu/markus/papers/phish6.pdf

3) However the School of Computer Science, Carnegie Mellon University Hong Kong University did have some success improving users' ability to identify phishing sites when education which appealed to human nature and people's general intuitiveness was utilized. The test participants were asked to play an animated online game Carnegie Mellon researchers invented called "Anti-Phishing Phil". Players move Phil the fish around the screen to examine bait and identify URLs as phishing or legitimate. Correct answers are praised and incorrect answers are explained by a popup message. 4,517 people participated in an online study and results showed people made better decisions after playing the game versus reading online training materials. Results also showed that the game makes users more knowledgeable about techniques they can use to identify phishing web sites. Reasons explaining why the game works are that unlike other more banal educational materials, it appeals to human nature – it's fun and people like to win at things.

http://cups.cs.cmu.edu/soups/2007/proceedings/p88_sheng.pdf

4) Another study conducted by the School of Computer Science, Carnegie Mellon University Hong Kong University was known as PhishGuru or Embedded Training. Users were sent periodic training emails that look like phishing attacks. If a user clicks a "phishing" link, they are shown succinct and engaging information on protecting themselves from phishing. Although the user study results show that sending training materials through normal email is ineffective, it did show that users are motivated to learn after falling for fake phishing attack. Also that study showed that users retained and transferred knowledge better when trained after falling for fake phishing attack versus getting training materials in normal email.

http://www.ecrimeresearch.org/2007/proceedings/p70_kumaraguru.pdf

5) "Mainstream advice for web users about phishing can be misleading, and phishers are changing tactics, making that advice obsolete" Markus Jakobsson, Associate Professor of Informatics at Indiana University

http://www.washingtonpost.com/wp-dyn/content/article/2007/10/10/AR2007101000614.html

6) "Education is not proving successful either, despite the efforts of some governments. Education is possibly the least effective method of stopping phishing. Education does not deter fraud. All it does is strengthen consumer confidence and you cannot trust consumers to make the right choices all the time." Uriel Maimon, Senior Researcher, Chief Technology Office, Consumer Solutions Business Unit, RSA.

http://www.itnews.com.au/News/84723,no-quick-tech-fix-for-phishing.aspx

7) Montclair State University Computer Science School conducted research which showed that the phishing IQ test and the session evaluation survey reveal that the current student body of the university was mostly oblivious to phishing threats. Upon being exposed to the topics and shown how to analyze a message for phishing characteristics, students were able to correctly identify most of the threats.

http://delivery.acm.org/10.1145/1150000/1140187/p237-robila.pdf?key1=1140187&key2=5145032521&coll=GUIDE&dl=GUIDE&CFID=50589473&CFTOKEN=20558106

8) The School of Computer Science, Carnegie Mellon University Hong Kong University present the results of a user study they conducted to test the effectiveness of existing online training materials that teach people how to protect themselves from phishing attacks. They found that these training materials are surprisingly effective when users actually read them. Their results contradict the conventional wisdom that training users to avoid phishing attacks do not work. Further work is needed to determine the most effective way of delivering training materials so that people will read them, as well as ways to improve existing training materials to make them even more effective.

http://www.cylab.cmu.edu/research/techreports/cmucylab07003.pdf

9) Jakob Nielsen, a web usability guru, has argued that educating users about security simply does not work.

http://www.useit.com/alertbox/20041025.html

10) A paper which tested user education in the form of documentation for the extended validation feature in IE7 [23] concluded that user education is ineffective. [not sure how relevant]

http://usablesecurity.org/papers/jackson.pdf

11) The conventional wisdom seems to be that training users not to fall for phishing attacks is pointless.

http://www.cylab.cmu.edu/research/techreports/cmucylab07003.pdf

4.2 Types of Evolving Threats Which Cannot Be Tackled Through Education

4.2.1 Web-based Malware

Malicious software may be broadly characterized as network attacks, social engineering attacks and website application attacks (also known as web-base malware). The latest evolution of malware – website application attacks are undetectable to the human eye. Examples include 'drive-by downloads' or 'drive-by infections', 'iframe injections' or 'iframe exploits', and 'cross scripting' – to name but a few.[9] Essentially, these types of attacks involve the insertion of unauthorized computer language which alters the original website or redirects traffic unknowingly to a rogue website. **In 2009, nearly one newly-infected webpage is discovered approximately every five seconds by security**

[9] At its most basic, an 'iframe' is the insertion of unauthorized third party computer language, which alters the original website. In this instance, a hacker sources their content into your website as opposed to directly manipulating a database. An 'iframe' is associated with a type of attack known as an SQL injection (Structure Query Language) or a sequel injection. This injection technique allows for web application exploits on client-supplied data. The SQL allows a website to provide dynamic and changing content. The data is backed-up and fed to the website via SQL. The attacker is able to directly manipulate your database. An 'iframe' may be inserted via the SQL injection. The last use of 'iframe' is the most common. It is a combination of the above uses.

companies.[10] Of new web-based applications being developed in the past year, 60 percent have malicious applications. Anti-virus and anti-spyware programs are only able to detect 80 percent of these new applications.[11] Many forms of traditional network attacks may be reduced by the use of a firewall coupled with up-to-date security software patched at frequent intervals and modest changes to network configuration. Social engineering attacks may be reduced through spam filters, as well as through education and recognition of potentially luring patterns. **Conventional security products, education and safe practices, however, do not adequately protect the end-user from web-base malware.**[12] The lack of traditional preventative measures together with the alarming rate of increase of this type of attack raise concerns. The best countering strategy is not evident.

Web-based malware has a core set of attributes:

- most often targets browser vulnerabilities;
- triggers automatic downloads;
- often uses luring content to entice end-users to initiate drive-by-downloads;
- often uses botnets as a distribution mechanism to plant unwanted content; and
- often initiated through adware, spyware and Trojans, commonly inserted through a technique known as an iframe.

Most web-based malware is not triggered by visiting a website itself. Often, the website merely acts as a landing site and it is the advertisements found on the website that contains a malicious component. In such instances, when a user clicks on the offending advertisement, they are redirected to the site containing malicious content. In other instances, a website may have been infiltrated by hackers who have placed malicious applications directly onto a trusted third party commercial website such as CNN. Malicious websites also operate by penetrating a search rank result such as Google. Malicious scripts may be injected into a webpage to steal session cookies, access privilege contents, change profile settings, record usernames and passwords, redirect traffic and/or generally misuse an account. Users are, thus, impacted in a variety of ways, including compromised authentication (access content in database), unauthorized access to personal data (enabling credit card fraud, and identity theft), misuse of bank accounts (unauthorized ordering of goods online via third party), pop-up advertisement flooding, spyware installation, bot acquisition and data theft where information is transferred to the attacker.[13] Website owners as opposed to users are also affected. Their content may be altered, as is the case with iframe injections, where the altered content may initialize malicious applications or customers may be redirected to other sites with malicious applications. The foregoing may result in the erosion of customer trust.

---

[10] Sophos reports 1 new infected webpage every 4.5 seconds. See Sophos, "Security Threat Report: 2009) available at http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf (last accessed April 27, 2009).

[11] Hines, M. "Malware flood driving new AV" Info World (Dec. 14, 2007) available at http://www.infoworld.com/article/07/12/14/Malware-flood-driving-new-AV_1.html. The journalist interviewed Carey Nachenberg, a research fellow with Symantec. Nachenberg's team performed a study which looked at the number of new application over a one week period in Nov. 2007. Apparently, out of the 65,000 new applications, 60% were malware.

[12] Mijatovic, N. and Mosse, B. "Web 2.0 Insecurity" conference paper presented at AusCERT 2008.

[13] Jim, T., Swamy N., and Hicks, M. "Defeating Script Injection Attacks with Browser-Enforced Embedded Policies" ACM Proceedings of the 16th international conference on World Wide Web available at http://portal.acm.org/citation.cfm?id=1242654

4.2.2 Infiltrated Google Search Ranking Pages

Infiltrated Google search ranking display pages represent an example of web based malware. For instance, a user looking for ways to better secure their personal computer may type 'anti-virus software' into Google. A number of fake criminal websites masquerading as legitimate anti-virus companies (spamlinks) will appear within the first few pages of the Google search hit, as well as in the advertisement space. Pandalabs, a developer of anti-malware software, has documented over one million malicious spamlinks regarding Ford and Nissan that are accessed through compromised Google search engine rankings.[14] The problem is so acute that Google has announced that it will change its infamous and secret search algorithm.[15] As will be demonstrated, sites that serve up malware are often an involuntarily part of a malware distribution network. A distribution network often includes a landing site, an iframe script originating from a remote site, and the remote site or distribution site that hosts the malicious content. These networks link together in a complex web of relationships, including individual adware programs placed on computers through botnets or distributed by adware brokers - many of which are connected to organized crime. One cybercrime expert describes the gravity of the situation as a 'global [adware] conspiracy.'[16]

4.3 Regulatory Challenges of Malware

The relationship between adware, spyware, spam, phishing, search engines, botnets, money mules, and organized crime in general is an *inherently complicated structure*. The connection between many of these supposed legitimate activities such as adware, and malicious applications, is not well documented. Regulatory and policy analysis has typically focused on one or two elements such as spam and phishing, or, in another common example, botnets and DDoS attacks.[17] The artificial categorization of attacks without comprehension and acknowledgement of how the pieces fit together has led to ineffective and wrongly targeted approaches to policy.

The Centre is currently working on a case study of the Netherlands adware company Dollar Revenue, tracing its roots back to organized crime and botnets, and comparing the legal framework of the Netherlands with that of Australia. Cybercrime provisions and governing structure of cybercrime responsibility in the Netherlands have led to successful prosecutions and fines in the area. **There are a number of loopholes in the Australian system which would make such an investigation difficult if not impossible. Graduate Researcher, Alana Maurushat, would be happy to share this case study with the Inquiry panel if so desired.**

---

[14] Correll, S-P. "Targeted Blackhat SEO Attack Against For Motors" Pandalabs April 14, 2009 available at http://pandalabs.pandasecurity.com/ (last accessed April 20, 2009)

[15] Miller, J. "Blackhat SEO Spammers Force Google's Hand" April 25, 2009 available at http://www.webpronews.com/topnews/2009/04/20/google-set-to-change-ranking-algorithm (last accessed April 27, 2009)

[16] Source cannot be named nor his/her affiliation. Presentation at closed workshop with Chatham House Rules.

5.0 Future initiatives that will further mitigate the e-security risks to Australian internet users.

There is a strong need for more private and public sector cooperative initiatives. The ABA's submission highlights this need well. In particular, we wish to strongly support a type of centre similar to the United States' **National Cyber Forensics and Training Alliance (NCFTA)** run by Ron Plescoe (and Andy Purdy). The NCFTA acts as a cybercrime hub or a clearing house for information on cybercrime. They liase with organizations who are victims of cybercrimes such as fraud, DDOS, and corporate espionage – much of their work is with financial institutions. The NCFTA operates as an intelligence hub. In doing so, they also work with appropriate law enforcement agencies to bring forth *targeted prosecutions* and work with organizations to mitigate attacks. We recommend something a similar clearing house or intelligence hub for cybercrime be formed or that an existing centre perform this function.

It is important to encourage active engagement with researchers in various disciplines within Australia and internationally, and to put in place measures to support their participation, such as agreed modes of cooperation.

Thank you for the opportunity to make this submission.

Yours Sincerely,

Alana Maurushat
Lecturer and PhD Candidate, Faculty of Law, UNSW
Deputy Director, Cyberspace Law and Policy Centre, UNSW
a.maurushat@unsw.edu.au +61 2 9385 8027