Australian Government
Australian Institute of Criminology

House of Representatives Communications Committee Inquiry into Cyber Crime

Submission by the Australian Institute of Criminology

The Australian Institute of Criminology's cyber crime research
In May 2009, the House of Representatives Communications Committee commenced an inquiry into cyber crime and its impact on Australian consumers. The Australian Institute of Criminology (AIC) welcomes the opportunity to contribute to the inquiry and wishes to draw the Committee's attention to the following research findings and publications.

The AIC first undertook research into cybercrime in 1996 when it received a grant from the Telstra Fund for Social and Policy Research in Telecommunications to examine current and emerging forms of criminality involving telecommunications systems as the instruments and/or the targets of criminal activity; organizational and regulatory shortcomings which facilitate the commission of the illegality in question; difficulties which tend to arise in the detection, investigation, and prosecution of the illegal activity; typical outcomes of the legal process; and countermeasures which will minimise future risk of the illegality in question, without inflicting collateral harm. This research led to the publication of the path-breaking book in Australia, *Crime in the Digital Age* (Grabosky and Smith 1998) and a series of associated AIC papers and journal articles.

Two other works then followed, *Electronic Theft* (Grabosky, Smith and Dempsey 2001) and *Cyber Criminals on Trial* (Smith, Grabosky and Urbas 2004) which examined economic crimes perpetrated using computers, and the processes of prosecution, trial and sentencing of cyber criminals, respectively. Institute staff also acted as consultants to the *Inquiry into Fraud and Electronic Commerce* conducted by the Victorian Parliament, Drugs and Crime Prevention Committee (2004), which was a major review of financial crime involving information and communications technologies.

The AIC continues to work closely with the Australian Government Attorney-General's Department and a number of key Attorney-General's portfolio agencies including the Australian Federal Police (AFP), with respect to cybercrime issues. In September 2003, the Australian Institute of Criminology was engaged by the then newly established Australian High Tech Crime Centre to conduct research into issues relating to key criminal justice issues concerning cybercrime in the context of an evolving international and domestic legal and law enforcement framework, and to identify the crime risks which will arise out of the environment in which Australians use information and communications technologies (ICT). As part of this research, a number of publications were released.

More recently, the AIC undertook the first national survey of Australian businesses from a range of industry sectors and including all sizes of business across Australia during February – April 2008. This survey sought to determine the prevalence and nature of computer security incidents that businesses had experienced, the areas in which business systems were vulnerable to such incidents, and the cost, types and effectiveness of approaches Australian businesses used to prevent them. The study was funded from the Proceeds of Crime Act 2002, which is administered by the Australian Government Attorney-General's Department (Richards 2009).

In November 2007, the Attorney-General's Department commissioned the AIC to search for, locate and report on the existing international academic and policy-relevant literature concerning the use of social networking sites for grooming children for sexual purposes, the extent and nature of the problem, and effective ways in which to address it. The results of this research were published in a report in July 2009 (Choo 2009).

The importance and relevance of cyber crime for Australia

Information and communications technologies (ICT) such as the new media have become an important element in our day-to-day activities as interaction, collaboration and knowledge-sharing among participants become easier and more widespread. This creates not only benefits for the community but also socio-economic challenges and risks of criminal exploitation of ICT – cybercriminal activities.

In our increasingly interconnected world, threats to national security can come from unexpected sources and directions. Cyberspace provides criminal actors with a safe haven that enhances their organisational and operational capabilities. Information security and associated laws and policy are also less well-developed in emerging economies, thus providing an environment in which criminal activities can be conducted with reduced chances of detection.

Threats from cyberspace are increasingly important and strategically relevant in Australia (see Rudd 2008) and overseas. A 2008 report of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency noted: 'we began with one central finding: The United States must treat cybersecurity as one of most important national security challenges it faces' (CSIS 2008). A National Office for Cyberspace will be established within the Executive Office of the President under the United States Information and Communications Enhancement Act of 2009 to deal with the emerging cybersecurity threats. The office is tasked to coordinate cybersecurity response between the Department of Homeland Security, the Department of Defense, the National Security Agency and the private sector. On 29 May 2009, the President of the United States of America Barack Obama referred to the importance of cyberthreats faced in today's digital age.

> This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history.
>
> So cyberspace is real. And so are the risks that come with it.
>
> It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox -- seen and unseen -- is something that we experience every day (Obama 2009).

The nature and prevalence of e-security risks and implications of these risks on the wider economy

Cybercrime often involves transnational crime in which offenders may be located in a number of jurisdictions. This creates difficulties for law enforcement in terms of detection, investigation and extradition of offenders. Cybercrime is becoming increasingly pervasive and sophisticated, and appears to be growing in volume and impact. Although some have

questioned the existence of organised criminal activities in cyberspace, several studies have identified a relationship between organised crime and cyberspace in recent years. McCusker (2006: 257), for example, suggested that 'cybercrime has become an integral part of the transnational threat landscape and conjures up pressing images of nefarious and increasingly complex online activity'. Choo (2008) also outlined three categories of organised crime groups that operate in cyberspace:

- Traditional organised crime groups which make use of ICT to enhance their terrestrial criminal activities;
- Organised cybercriminal groups which operate exclusively online; and
- Organised groups of ideologically and politically motivated individuals who make use of ICT to facilitate their criminal conduct.

Data breaches

Almost every business in developed economies makes use of the internet. As businesses continue to engage in electronic commerce, they will become increasingly globalised and interconnected and the level of data being created by society is set to increase. In terms of the future threat landscape, it is argued that the increased variety and volume of attacks is inevitable given transnational crime networks' desire to obtain personal and confidential information. Non-physical data breaches due to computer or network intrusions are a cause for concern. According to the data breach investigations conducted by Verizon Business from 2004 to 2008, for example, only 9 per cent of the data breaches are attributable to physical attacks. In the Verizon investigations, hacking was found to be one of the leading causes of data breaches (64% of cases). 'Unauthori[s]ed access via default, shared, or stolen credentials constituted more than a third of the entire Hacking category and over half of all compromised records' (Verizon 2009: 16).

The involvement of organised crime groups in computer or network intrusions such as hacking and unauthorised access to obtain sensitive information, emphasises the importance of large-scale profit-driven incentives. In one American case, for example, two accused persons (and others known and unknown) 'allegedly participated in a scheme to steal funds from bank and brokerage accounts by hacking into those accounts through the internet, using personal financial information obtained through computer viruses' (*United States of America v Alexander Bobnev and Alexey Mineev*). The accused persons subsequently sent a portion of the stolen funds to their associates in Russia using money remittance services after keeping a portion of the funds for themselves.

Internet frauds, scams and phishing

In online or internet scams, cybercriminals abuse the internet to reach out to potential victims across the globe by sending unsolicited messages purporting to originate from legitimate organisations in order to deceive individuals or organisations into disclosing their financial and/or personal identity information. Information obtained from phishing and other illegal means is invariably used to facilitate the commission of crimes such as financial fraud and identity theft. A survey of 4,988 American adults conducted by Gartner in 2008, for example, found that the top causes for financial fraud against consumers were data breaches at a retailer, government agency or other organisation, and third party phishing (Litan 2009). The biennial KPMG fraud survey of 420 organisations in Australia and New Zealand reported similar findings.

> Within the financial services sector, credit card fraud accounted for 39 percent of the value of fraud attributable to external parties. Fraudulent access to financial services' accounts [by adopting the identity of the account holder by

> ‘phishing’ or ‘trojan horse’ attacks over the internet] amounted to 31 percent of the total value attributable to external parties (KPMG Forensic 2009: 13).

Several researchers and security practitioners have also suggested the involvement of organised crime groups in phishing scams (see McCombie 2007; Choo & Smith 2008; Choo, Smith & McCusker 2007a). In recent years, phishing messages are increasingly targeting top executives of organisations or members of specific groups—known as spear phishing or whaling (Garretson 2007; McMillan 2008).

Organised crime groups have also been known to use identity fraud either to conceal their identities in order to evade detection and protect their assets from confiscation, or as an enabler to commit various frauds and other crimes (SOCA 2008). Internet frauds and scams include a variety of advance fee scams including Nigerian scams, lottery scams and inheritance frauds, online auction frauds, and other identity-related and payment card frauds. In the United States, out of 275,284 complaints to the Internet Crime Complaints Center between 1 January and 31 December 2008,

- Online auction fraud accounted for 25.5% of the 72,940 cases referred to US law enforcement agencies and 16.3% of the total reported dollar loss
- Payment card fraud accounted for 9% of the 72,940 cases referred to US law enforcement agencies and 4.7% of the total reported dollar loss
- Nigerian advance fee scam accounted for 2.8% of the 72,940 cases referred to US law enforcement agencies and 5.2% of the total reported dollar loss

The total dollar loss from all cases of internet fraud and scams referred to United States law enforcement agencies in 2008 was US$264.6 million – an increase of 10% from the previous year (NW3C 2009).

The Australian Bureau of Statistics (2008)’s National Personal Fraud Survey, conducted throughout Australia during July to December 2007, estimated that nearly A$1 billion was lost as a result of personal fraud. The survey found that

- A total of 806,000 Australians reported to be victims of at least one incident of personal fraud in the previous 12 months.
- Nearly half a million Australians reportedly experienced a form of identity fraud.
- Nearly six million Australians were exposed to a range of selected scams and 329,000 people fell victim to at least one type of scam by responding to or engaging with the unsolicited offer. The three main categories of selected scams were lotteries (84,100 victims), pyramid schemes (70,900) and phishing and related scams (57,800).

Malware creation and dissemination

The McAfee (2008)’s virtual criminology report indicated that cybercriminals are increasingly exploiting vulnerabilities in software and using social engineering techniques to spawn a broad range of threats including spyware, phishing, adware, rootkits, spam, and botnets. In 2008, Symantec reported that ‘the number of new malicious code (also known as malware) signatures increased by 265 percent over 2007; over 60 percent of all currently detected malicious code threats were detected in 2008’ (Symantec 2009: 15).

In the AICs Australian Business Assessment of Computer User Security (ABACUS) survey, responses from 4,000 Australian businesses indicated that 14% of the respondents had experienced one or more computer security incidents during the 2006–07 financial year. According to the survey, the most common type of incident reportedly experienced by the respondents was a virus or other malware code and the most common effect was corruption of hardware and software; and the total financial loss as a result of computer security

incidents against businesses in Australia during the 2006–07 financial year was estimated at between $595 and $649 million (Richards 2009).

Malware including worms, viruses, backdoors, keyloggers, and Trojans, is designed to install other malicious code that will cause damage and or capture personal data without the computer user's consent and knowledge. The 2008 UK Threat Assessment report observed that 'most new malware is designed to steal financial data (such as credit card details, bank account details, passwords, PIN numbers) as a precursor to various frauds and other deceptions' (SOCA 2008:9). An example of information stealing malware is keylogging programs (keyloggers). These are designed to monitor user activity including keystrokes. They can be used by cybercriminals to steal passwords or credit card details, which can then be used for malicious purposes such as identity/online fraud. Cases involving the use of keyloggers include the attempted theft of more than £229m from Sumitomo Matsui Banking Corporation in London. Three individuals were reportedly extradited to the UK under European Arrest Warrants from Belgium and Spain and '[a]pproximately £1.5m in assets was [reportedly] restrained and will be the subject of further action under the Proceeds of Crime Act' (SOCA 2009: 19).

McAfee (2005) estimated that the number of potentially malicious threats emerging each month increased from approximately 300 to 2,000 between 2003 and 2005, largely due to the growing incidence of bot malware. Sophos (2006) also pointed out that an unpatched computer with neither antivirus protection nor a firewall installed would have a 50 percent chance of becoming a zombie within 30 minutes of being connected to the internet. Bot malware is often surreptitiously forwarded to victims by various means, such as via email attachments, via peer-to-peer (P2P) networks, and visits to an infected website. Bot malware typically takes advantage of system vulnerabilities and software bugs or hacker-installed backdoors that allow malicious code to be installed on computers without the owners' consent or knowledge. They then load themselves into such computers, often for nefarious purposes.

Bots – individual computers infected with bot malware – are then turned into zombies. The shift in motivation from curiosity and fame-seeking to illicit financial gain has been marked by a growing sophistication in the evolution of bot malware (Choo 2007), as illustrated by recent examples of detected bot malware such as Conficker. Conficker has received a considerable amount of media attention worldwide in recent months, and has been widely reported to have successfully 'infiltrated government sites, military networks, home PCs, critical infrastructure, small networks, and universities, around the world' (Porras, Saidi & Yegneswaran 2009). According to analysis of Conficker and its variants (Conficker B and Conficker C) by Sophos – an IT security company – and the Malware Threat Center at SRI International, Conficker and its variants are designed to provide a secure binary updating service that effectively allows the bot malware designer instant control of millions of personal computers (PCs) worldwide and have a number of sophisticated defensive mechanisms.

- The use of cryptography such as binary encryption methods to prevent other individuals such as bot malware designers and law enforcement investigators from taking over the Conficker botnet.
- The use of compiler-level code obfuscation to hinder the malware from being detected by anti-malware software and make reverse engineering more difficult for investigators analysing the malware (Porras, Saidi & Yegneswaran 2009; Fitzgibbon & Wood 2009)

Compromised computers – zombies – can then be used as remote attack tools or to form part of a botnet under the control of the botnet controller (Choo 2007). According to Symantec (2009: 19), 'bot networks were responsible for the distribution of approximately 90 percent of all spam email [in the calendar year 2008]'. A 2008 report by McAfee also pointed

out that '[r]ecent figures suggest that the number of compromised zombie PCs in botnets has quadrupled in the last quarter alone and that these are capable of flooding the Internet with more than 100 billion spam messages per day … [and] are increasingly switching to phishing, distributed denial of service (DDoS) and website attacks which are capable of causing a huge amount of damage and are a growing threat to the security of nations, the national information infrastructure, and the economy.' (McAfee 2008: 5). Data from Symantec (2009) further suggested that in 2008, botnets were responsible for the distribution of approximately 90 percent of all detected spam email.

As Schaffer (2006) and many other security researchers have pointed out, bot malware is just as dangerous as more familiar cyberthreats, e.g. viruses, worms, Trojan horses and network intrusions. Moreover, advances in modern technologies offer criminals more opportunities to commit economic crimes with larger payoffs and fewer risks. The identities of the bot criminals are preserved when they carry out concerted attacks since zombies (attack sources) are not owned by the attackers. Known financially-motivated cyber criminal groups using malware as vehicles for cybercrime include:

- The 'Russian Business Network' (RBN), an allegedly Russian-based group, identified by VeriSign to be a criminal internet service provider of child abuse materials, phishing sites designed to fool visitors into handing over their banking details, and repositories of Trojan code and other malware (Miller 2007). RBN also allegedly 'runs a protection racket that extorts as much as US$2,000 a month in fees for "protective Web services" from borderline sites' (Keizer 2008).
- The botnet-for-rent Loads.cc group, which is reportedly 'responsible for the distribution and installation of massive amounts of malware: Spambots, keyloggers, DDoS bots, adware and rootkits' (Goodin 2008).

In recent years, increased attention on the part of law enforcement agencies has led to a number of arrests.

- The 'M00P virus-writing gang': three suspected members of the gang were arrested by the London Metropolitan Police Computer Crime Unit, the Finnish National Bureau of Investigation and the Finnish Pori Police Department, in connection with a conspiracy to infect computers with malware to create a botnet (Jaques 2006). Botnets can then be rented out to willing parties to facilitate other criminal activities such as spam. For example, a member of the 'botmaster underground' pleaded guilty to computer fraud and spam offences connected to his dealings in botnets. The defendant created new variants of the 'rxbot' and distributed these variants to establish several botnets. He then offered to hire out the botnets to others for the purposes of sending spam and launching distributed denial-of-service (DDoS) attacks17, thus earning thousands of dollars. It was also alleged that the defendant used the botnets to generate income from the surreptitious installation of adware on the zombies. In May 2006, the defendant was sentenced to 57 months in federal prison (US DoJ 2006).
- On 29 July 2008, an individual was arrested by Dutch authorities and according to the indictment, the individual had participated in a conspiracy along with others to use, maintain, lease and sell an illegal botnet consisting of more than 100,000 computers worldwide. It was also alleged that the individual used the botnet, paid for the servers on which the botnet was hosted, and agreed with another unindicted co-conspirator to broker the sale of the botnet and underlying bot code to a third party for 25,000 Euros (FBI 2008).
- On 4 March 2009, an individual was sentenced to 48 months in federal prison after pleading guilty in 2008 to accessing protected computers to conduct fraud, disclosing illegally intercepted electronic communications, wire fraud and bank fraud. According

> to court documents, the individual reportedly admitted that he illegally accessed and remotely controlled these hundreds of thousands of compromised machines – zombies – in the United States. The individual then used his botnets to search for vulnerabilities in other computers, intercept electronic communications and engage in identity theft. The individual also admitted that he and others installed malware on zombies to capture electronic communications as they were sent from these compromised computers (e.g. online financial transactions). Usernames and passwords to accounts mined from these intercepted communications were used to make purchases and/or transfer funds without the consent of the victims (FBI 2009).

Although malware is still disseminated using conventional tools such as email, cybercriminals have turned to exploiting browser plug-in and webserver vulnerabilities in recent months. Various reports have indicated that a large number of commercial, government, university and other high profile and high traffic websites worldwide have been successfully compromised by infecting unwitting visitors with malware (see Leyden 2009; McMillan 2009; Moses 2009). For example in May 2009, the UK regional director of Finjan, an IT provider of secure web gateway solutions, noted that a botnet discovered by the company in February 2009 reportedly contained 1.9 million infected computers in 73 government domains (Raywood 2009).

In a recent study, researchers from Harvard University and the University of Cambridge examined the use of search engines to locate potentially vulnerable computers – a technique known as search engine optimisation. The study suggested that the cybercriminals are compromising web servers to host phishing websites using search engine optimisation.

> At least 18% of website compromises are triggered by these searches. Many websites are repeatedly compromised whenever the root cause of the vulnerability is not addressed. We find that 19% of phishing websites are recompromised within six months, and the rate of recompromise is much higher if they have been identified through web search. By contrast, other public sources of information about phishing websites are not currently raising recompromise rates; we find that phishing websites placed onto a public blacklist are recompromised no more frequently than websites only known within closed communities (Moore & Clayton 2009: unpaginated).

McAfee (2009: 3) has reported similar findings. In the first quarter of 2009, the company reported an increase in the number of malicious websites created and 'sites that host malware—with thousands of new sites appearing daily'. McAfee Avert Labs also reportedly 'uncover(ed) a massive search engine–optimization ring that targeted the top Google search terms. The attackers not only stole copyrighted materials from popular sites, but they also abused other popular sites, such as Democrats.org, to bump up their Google rankings. The goal of the attackers in optimizing search results was to install rogue anti-virus software. This was a case of a rogue Facebook application, leading to rogue search results, leading to rogue security software' (McAfee 2009: 3).

Business, government and individual householders need to be aware of risk mitigation strategies (see Moore & Clayton 2009) and to ensure that these strategies are implemented and updated, as search engine optimisation will continue to be one of the most sought after attack vectors by criminals.

The underground economy

Extraterritoriality, the notion that cyberspace has no geographic boundaries, has driven the e-commerce revolution. Unfortunately, organised criminal groups operate online under the same free market principles. Researchers from Carnegie Mellon University, University of California Berkeley and University of California San Diego (Franklin et al. 2007) highlighted the emerging trend of underground economy for the buying and selling of security

vulnerabilities, stolen credit card and other online credential information; and the sale of compromised hosts established on public IRC servers. To evade the scrutiny of law enforcement agencies, organised cybercrime groups have been reportedly building their own encrypted instant-message (IM) programs such as CarderIM designed to establish a 'secure' channel to sell stolen financial and personal information.

Although there are no known published statistics involving monthly subscription-based services for malware updates being offered at such underground economy sites, it is likely that such services will become increasingly popular. The emergence of an underground economy as the provider of illicit information is thought to indicate the level of professionalism and commercialisation present in the transnational crime sector – see Table 1.

Table 1: The underground economy

Digital assets	Prices (US$)
Credit card information	$0.06 – $30
Bank account credentials	$10–$1000
Email accounts	$0.10–$100
Email addresses	$0.33/MB–$100/MB
Proxies	$0.16–$20
Full identities	$0.70–$60
Mailers	$2–$40
Cash out services	8%–50% or flat rate of $200–$2000 per item
Shell scripts	$2–$20
Scams	$3–$40/week for hosting, $2–$20 design

Source: Symantec (2009)

Just like entrepreneurs, cybercriminals are always on the lookout for new markets and, with the rise of online gaming, a new outlook for exploitation has just appeared. Data from Symantec (2009: 15) also indicated that '[m]alicious code that targets online games accounted for 10 percent of the volume of the top 50 potential malicious code infections, up from 7 percent in 2007'.

Byron defines online gaming as: 'a digital game that uses a live network connection in order to be played', which usually means the Internet. So, this includes games played on the Internet, from simple games (e.g. puzzles or word games) to massively multiplayer online role playing games (MMORPGs) like World of Warcraft, but also those played online through consoles, across mobile phones or via peer-to-peer networks' (Byron 2008: 191). Online gaming is a growing industry with the online gaming market worldwide expected to exceed $US13 billion by 2012 (Ong 2008). Research by Gartner, highlighting a similar trend in mobile gaming, predicted that end-user revenue will increase to $US9.6 billion in 2011 (Nguyen, Ekholm & Ingelbrecht 2007).

The virtual worlds, massively multiplayer online games (MMOGs) and MMORPGs provide an environment in which people communicate with each other using a virtual persona – an avatar – and allow strangers who do not necessarily speak the same language to establish relationships in the virtual worlds. To participate in the games, players have to exchange real cash for virtual currency from the gaming sites (e.g. LindeX™, the official Second Life currency) or from third-party trading sites (e.g. www.ige.com). Using these virtual currencies, players can purchase virtual properties, virtual accommodation and virtual merchandise in the virtual worlds. At 3 June 2009, the reported virtual exchange rate on LindeX™ was L$260 to $US1.

A 2008 study by researchers from Peking University in China and University of Mannheim in Germany identified six types of actors in the Chinese underground economy involved in the compromise, trade and exploitation of virtual assets in online gaming.

- Virus writers are individuals who write malicious software (malware) for profit.
- Website masters/crackers: website masters are individuals who attract potential victims with freebies and redirect them to malware-infected sites and website crackers are individuals who compromise websites by exploiting vulnerabilities in these websites. The study suggested that the current market price is approximately 40 to 60 RMB per ten thousand visits.
- Envelope stealers, individuals with limited technical knowledge, typically buy ready-to-use malware and other malware kits from virus writers and/or website traffic from Website Masters/Crackers in order to steal login credentials and other account information. The harvested login credentials and other account information are then resold to Virtual Asset Stealers for profits.
- Virtual asset stealers, individuals with limited or no technical knowledge but possess a good understanding of the underground market, purchase login credentials and other account information in order to steal valuable virtual assets such as online gaming accessories and online gaming currency (e.g. QQ coins). The stolen virtual assets are then resold for profit.
- Virtual asset sellers are individuals who buy virtual assets from the underground market at a very low price before selling to other legitimate players on the public marketplaces at a profit.
- Players are individual participants of online games (Zhuge et al. 2008).

Risks of money laundering may also develop as players in MMOG and MMORPG sites deal in virtual currency (Choo 2008; Choo, Smith & McCusker 2007a). For example, money launderers could purchase virtual currency or properties using illicit cash and exchange the virtual currency and properties back to physical cash. Alternatively, colluding avatars (controlled by criminals) could launder illicit proceeds in the form of gifts or barter arrangements. In the 2008 national drug threat assessment report, the United States National Drug Intelligence Center warned that drug traffickers may exploit virtual currency to launder their drug proceeds.

- Selling virtual game accessories to other players for a credit to their account and the credit can be cashed with the gaming operator and a legitimate cheque will be issued to the account owner (e.g. launderer).
- Accepting virtual currency in exchange for illicit drugs.
- Maintaining multiple gaming accounts for the purpose of buying and selling of merchandise to themselves to create a false sense of trade legitimacy.
- Selling virtual currency in exchange for real money to other players (US NDIC 2007).

Cyberbullying

According to Muir (2005), advances in ICT have outpaced our understanding of their social impact, particularly involving their negative aspects. In recent years, a new form of bullying, including harassment targeting children and young users, has emerged which makes use of ICT such as blogs, email, text messaging, chat rooms, mobile phones, mobile phone cameras and social networking sites. Cyberbullying can also include online fights, denigration, impersonation, trickery, and cyberstalking. Reeckman and Cannard (2009) argued that ‘[t]here are notable differences between cyberbullying and traditional and face-to-face bullying … [as c]yberbullies can remain anonyomous’. Thomas also highlighted similar concerns.

> The anonymity provided by the internet introduces a new element: The victim may have no way to identify the bully. Neither parents nor school officials may know how to intervene to stop the harassment. Children may be reluctant to report incidents, for fear their computer privileges will be curtailed (Thomas 2006: 1015).

The anonymous nature of the internet also allows offenders to masquerade as the victim and post fabricated and malicious information online with the intention of stalking, harassing or embarrassing the victim. In a recent case, for example, an individual allegedly 'engaged in a course of conduct consisting of malicious postings to MySpace, Facebook, Craig's List and other Internet social sites in which he caused the personal identity information of [the victim] – including her home address – to be publicly displayed. At the time, the indictment says, [the defendant] had been served with a restraining order forbidding contact with [the victim] … [the defendant also] allegedly posed as [the victim] and distributed Web site invitations to visit [the victim's] residence for sexual gratification' (US DoJ 2008).

Unlike traditional face-to-face bullying, victims of cyberbullying may find it harder to escape as explained by a young respondent – a student aged between 12 and 20 years in the city of Gothenburg, Sweden – in the study by Slonje and Smith:

> One participant reflected on the impact cyberbullying outside school may have: "I believe that cyberbullying most often can be worse for the victim. Partly because the bullies spend so much energy on the bullying, but also because the bullying takes place outside school, in other words when the victim is at home. Home is usually a sanctuary for most people. But the bullies take this sanctuary away from the victims by cyberbullying them." (Slonje & Smith 2008: 151).

The extent of the problem

As is the case with most forms of cybercrime, it is difficult to determine with accuracy the actual extent to which individuals particularly children and young people are bullied or harassed online. Quantification of the extent of the problem is exacerbated by the illegal nature of such activities, which makes self-reporting and detection unlikely to occur. Whitty (2008: 1843-4) 'argued that the online environment could produce a greater number of stalkers and harasses than offline … [as] people can often be more easily located online. Slonje and Smith (2008: 148) agreed and indicated that 'the opportunity for cyberbullying may increase with age as older pupils more often will have mobile phones or access to the internet'. In both Australia and the United States, research has sought to document the extent to which bullying takes place online.

Australia

More than a fifth of respondents (aged between 15 and 20 years) in the 2008 youth poll, initiated by Senator Natasha Stott Despoja in 1992, reportedly experienced being 'upset or felt threatened by someone they came into contact with online (Despoja 2008: 13).

Of the 91 student respondents enrolled in the Youth Unit at Northern Melbourne Institute of TAFE (NMIT), 63% reported experiences of being cyberbullied although only 9% reported being cyberbullied by another NMIT student (Reeckman & Cannard 2009). A significant percent (58%) of the respondents admitted to be a cyberbully.

In the Australian Covert Bullying Prevalence Study (ACBPS) conducted by Edith Cowan University, a total of 20,832 Australian students aged 8 to 14 years from over 200 schools and 456 school staff were interviewed. The ACBPS found that:

- 27% of Year 4 to Year 9 (Australian) student respondents reported being bullied every few weeks or more often overtly, covertly or both during the last term at school;
- 61% of students reported being bullied in any way had also experienced covert bullying (either on its own or in conjunction with overt bullying). Of students who had reportedly experienced covert bullying, 24% had been physically hurt, and 13% had been sent nasty messages on the internet. 53% of student respondents who indicated that they had bullied others had engaged in covert bullying (either on its own or in conjunction with overt bullying);
- 16% of student respondents reported being bullied covertly every few weeks or more often in the term the survey was conducted. Year 5, 6 and 8 student respondents were most likely to report being bullied covertly (18-20%) and those in Year 9 least likely (12%). This form of bullying was experienced slightly more often by girls (18%) compared with boys (15%) and in Government schools (17%) more often than non-Government schools (14%);

Despite the high number of reported incidences of bullying experienced by student respondents in the ACBPS, the study indicated that '[t]he vast majority of Year 4 through Year 9 students had not [reported] experience[ing] cyber bullying, with only 7-10% of students reporting they were bullied by means of technology over the school term' (Cross, Shaw, Hearn, Epstein, Monks, Lester & Thomas 2009: xxiii). This extensive study also found that '[s]lightly higher rates of cyber bullying were found among secondary students and students from non-Government schools [and c]yber bullying was not observed by or reported to as many staff members as other forms of bullying, but was not rare (20%)' (Cross, Shaw, Hearn, Epstein, Monks, Lester & Thomas 2009: xxiii).

United States

Between 2 and 15 February 2006, the National Crime Prevention Council (2007) in the United States conducted a study in which approximately 46 percent of a nationally representative sample of 824 middle and high school students aged 13 through 17 reported that they had experienced some form of cyberbullying in the last year.

In the study by Williams and Guerra (2007), 3,339 youths in Grades 5, 8 and 11 in 78 school sites in Colorado were first surveyed in late 2005, and 2,293 respondents in the original sample participated in a follow-up survey in 65 school sites in 2006. The study found that 9.4 percent of the respondents experienced internet bullying.

Responding to cyberbullying

The question of how best to create a safe online environment for children and young people is not easily answered. The ACBPS, for example, pointed out that '[w]hile pedagogical and legal policies, like the National Safe Schools Framework, have assisted in creating positive, supportive environments for the reduction of face-to-face bullying that occurs on school grounds, the virtual nature of cyber bullying means it may occur both within the school environment or off-campus, blurring the boundaries for supervision and responsibility, and introducing a number of unprecedented legal and educational concerns for schools' (Cross, Shaw, Hearn, Epstein, Monks, Lester & Thomas 2009: 38).

Children and young people are generally more technologically savvy and at ease with the use of web 2.0 (social networking sites) than their parents, teachers and other individuals tasked with taking care of them. The virtual/digital generations are increasingly communicating in ways unfamiliar to adults in virtual venues only dimly grasped by them. It is not surprising that adults are not up-to-date with recent advances in ICT used by the virtual/digital generations and, therefore, also have difficulty in coping with or responding to online risks faced by their children. However, some countries have sought to address this

educational need such as the initiatives announced by the Deputy Prime Minister The Hon Julia Gillard MP (Gillard 2009).

Besides focusing preventive strategies on children, parents should also be included in the educational programs. For example, parents should ensure that children and young people are subject, to some degree, to family rules that limit the frequency and their connection time, and be familiar with the communication technologies (e.g. instant messaging programs and social networking sites) to reduce their child's risk behaviour in the longer term. The issue of adult awareness is crucial when it comes to effective action by parents and schools against cyberbullying. Both parents and teachers should be aware of the various types of online risks (including online child grooming) and of what actions can be taken. The ThinkUKnow Australia website (http://www.thinkuknow.org.au/site/index.asp) – a joint effort by the UK Child Exploitation and Online Protection Centre, the Australian Federal Police, Microsoft Australia and the Australian Communications and Media Authority – is one of the recent additions to a list of educational programs designed to educate both parents and children about online dangers. On the website, there are simple-to-follow useful programs for teachers, parents or guardians that explain the different ways in which children are using the internet, give practical advice on how to protect children and provide useful first-warning signs in how the behaviour of young people may change if they are being targeted by offenders.

The internet is a shared community and coordinated efforts are needed by parents, schools, communities, organisations and governments to ensure that a safe online environment is available for children. Funding for educational outreach programs such as promoting safe use of the internet among children (e.g. advising children about the risks associated with meeting online friends) in various media, informing the public of the risks linked to the use of online technologies and conducting educational road shows tailored to the needs of children, parents, teachers and other individuals tasked with taking care of children should be encouraged.

The principal social networking sites such as MySpace have also been proactive in working with law enforcement agencies to protect children and young people against sexual offenders online (Choo 2009). Terms of use on social networking sites prohibit users from abusing the sites for activities such as harassment of other users and dissemination of objectionable materials. Users who violate these terms may have their accounts deactivated and in situations of a criminal nature, may be reported to appropriate law enforcement agencies.

Cyberstalking

The wealth of personal information and pictures online could potentially be used by individuals and sexual predators to identify, locate, contact, stalk and harass their victims. Cyberstalking behaviours include:

- Sending repeated unwanted messages using email and SMS or posting messages on blogs, profiles on social networking sites, etc.
- Ordering goods and services on the behalf of victims, which could potentially result in legal, reputation and financial losses to the victims
- Publicising private information about the victim
- Spreading false information
- Gathering information about a victim online
- Encouraging other individuals to harass the victim
- Unauthorised access into the victim's computer(s) or internet accounts (e.g. email and social networking site accounts) (Mullen, Pathé & Purcell 2009).

In the Media and Communications in Australian Families 2007 study commissioned by the Australian Communications and Media Authority (ACMA), 751 Australian families with children aged between eight and 17 years were surveyed nationwide from 20 March to 12 May 2007. A total of 1,003 children aged between eight and 17 years in these families completed time-use diaries that indicated their online activities. The study found that:

- approximately 70 percent of girls aged between 14 and 17 years, and 50 percent of boys of the same age group had a personal profile on MySpace or other similar online sites
- approximately one in eight respondents aged between 14 and 17 years reportedly posted videos online (ACMA 2007).

The study by Cox Communications (2007) highlighted that people with a public profile are more likely to be bullied and harassed online, and to receive personal messages via email, instant messaging, chat or text messages from strangers when compared with respondents without a public profile. Smith (2007: 2) also reported that '[t]hose who have posted photos of themselves and created profiles on social networking sites are more likely to have been contacted online by people they do not know' and 'girls are significantly more likely than boys to be contacted by someone they do not know when other factors are held constant'. However, 58 percent of the respondents in the Cox Communications (2007) study did not think that posting personal information and photos on public networking sites was an unsafe practice, 47 percent were not worried about other people using their personal online information in ways they did not want them to, and 49 percent were unconcerned that the posting of personal information online might negatively affect their future.

In the 2006 US-based Youth Internet Safety Survey (YISS-2), the 1,500 youths aged between 10 and 17 years who were interviewed reported frequent exposure to unwanted sexual material, sexual solicitations and harassment online (Wolak, Mitchell & Finkelhor 2006). Some four percent of all young respondents to the survey indicated that people they met online requested nude or sexually explicit photographs of them (Wolak, Mitchell & Finkelhor 2006), and respondents aged between 14 and 17 years were reportedly more likely to receive sexual solicitations online than other age groups (Wolak, Mitchell & Finkelhor 2006).

In the Growing Up with Media survey, 1,588 youths aged between 10 and 15 years were surveyed between August and September 2006 (Ybarra, Espelage & Mitchell 2007). The respondents were required to be able to read English and to have used the internet at least once in the previous six months prior to the survey. The study found the following results:

- Internet harassment or unwanted sexual solicitation
    - 35 percent reported being the victim of either internet harassment or unwanted sexual solicitation
    - 21 percent reported perpetrating either internet harassment or unwanted sexual solicitation
- Internet harassment only
    - 34 percent of all youth reported being the victim of internet harassment at least once in the previous year while eight percent reported being targeted monthly or more often
    - 21 percent reported perpetrating internet harassment of others at least once in the past year and four percent reported doing so monthly or more often

Although only a minority of the respondents in the Growing Up with Media survey were frequently involved in internet harassment or sexual solicitation as victims or perpetrators, the various associated psychosocial problems (e.g. elevated rates of substance use,

involvement in offline victimisation and commission of sexual aggression) highlighted the need for early intervention and prevention programs for this group of young people.

In the Survey of Children's Use of the Internet that was carried out between December 2005 and January 2006, 848 students aged between nine and 16 years in 21 Irish schools were interviewed (Webwise 2006). The survey found that 19 percent of the respondents indicated they had been harassed, upset, bothered, threatened or embarrassed by someone when chatting online.

Legislative responses to cyberstalking

Traditionally, courts have accepted jurisdiction if a person against whom legal proceedings are brought is physically present in the geographical territory (i.e. country or state) in which the court operates, or is a citizen of the territory, or if there is some other sufficient 'territorial nexus'. Such a connection might arise if the alleged victim of a crime is in the territory, or some other effect of the crime, sufficient to exercise jurisdiction, is present. For crimes involving physical acts, rules of jurisdiction have largely been relatively easy to apply, but the situation is more complicated for online activity as illustrated by a recent media article.

> The man behind a vicious website used by cowards to harass Victorian teenage girls has dared authorities to take action. Melton website designer Andrew Pallant claims his site, which has more than 1300 posts containing unsubstantiated and often vulgar allegations, is designed to protect freedom of speech. The site, which has been operating for more than a year despite repeated complaints, invites people to vent their fury about everyone from ex-girlfriends, to teachers, police and police informants, the Herald Sun reports. Many of the victims are teenage girls who have had their name, photo and phone numbers posted, accompanied by invitations to bombard them with abusive phone calls and text messages or ask them for sex. Mr Pallant boasts the site, which has caused chaos in western Victoria, gets about 3000 hits a month. But although police have received complaints from parents and victims, they are powerless to prosecute Mr Pallant or to close the site down …. Yesterday Mr Pallant admitted to the Herald Sun his site was often used for bullying (Healey and Murphy 2009).

Inspector John Manley, head of Victoria Police's E-crime squad has suggesting that 'Victoria Police do not have any authority to take any blanket action against this type of site regardless of the location of the server'. A former chief justice of the Family Court of Australia observed 'that current legislation was extremely limited and had failed to keep up with advances in technology [for cyberbullying]' and that 'without specific legislation to address cyber bullying, lawyers had to make do by adapting other legal mechanisms such as anti-stalking and harassment laws' (Smith 2007b).

In the case of cyberstalking, it is possible to stalk a person far removed from one's physical location and this may result in:

> some jurisdictional complications in applying the law. For example, in DPP v Sutcliffe [2001] VSC 43, the Victorian Supreme Court held that a Melbourne man accused of stalking an actress in Canada by means including email was subject to prosecution under s21A of the Crimes Act 1958 (Vic), which has since been amended to make clear that it extends to cyberstalking which crosses jurisdictional boundaries (Urbas & Choo 2008: 31).

In a recent example, an Australian female reportedly plead guilty in the Victorian County Court today to four counts of stalking a female American Idol contestant over the internet

(AAP 2009). In May 2009, she was sentenced to 26 months imprisonment, with a non-parole period of 12 months (Hadfield 2009).

McEwan, Mullen and MacKenzie (2007) highlighted some of the difficulties in drafting anti-stalking legislation. For example, not all of the above mentioned behaviours are criminal. For example, mining for information about a victim online using publicly available information (e.g. profiles on social networking sites and online resumes with addresses and other contact details) is not illegal, nor is posting of messages of a non-threatening nature. However when these "innocuous" 'activities are repeated over an extended period of time in an unwelcome manner these seemingly inoffensive acts develop into a course of conduct with menacing overtones for the target', argued McEwan, Mullen and MacKenzie (2007: 208).

Urbas and Choo (2008) referred to provisions relating to offensive communications which could be used to deal with misuse of the internet to stalk or harass others. For example, section 474.17 of the *Criminal Code Act 1995* (Cth) creates an offence of using a carriage service to menace, harass or cause offence, which means using the carriage service in such a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive. This provision can be applied to such uses of the internet as the posting of pornographic, defamatory or racist material on websites. Penalties for cyberstalking vary considerably between states and territories – maximum penalty ranges from two years to 21 years imprisonment, as illustrated in Table 2.

Table 2: Summary of cyberstalking offences in Australian states and territories

Juris-diction	Provision	Maximum penalty
ACT	*Crimes Act 1900*, s35	Five years imprisonment if (i) the offence involved a contravention of an injunction or other order made by a court; or (ii) the offender was in possession of an offensive weapon; two years imprisonment otherwise.
Cth	*Criminal Code Act 1995*, s474.17	Two years imprisonment.
Qld	*Criminal Code Act 1899*, s359B	Seven years imprisonment if, for any of the acts constituting the unlawful stalking, the person (a) uses or intentionally threatens to use, violence against anyone or anyone's property; or (b) possesses a weapon within the meaning of the Weapons Act 1990; or (c) contravenes or intentionally threatens to contravene an injunction or order imposed or made by a court or tribunal under a law of the Commonwealth or a state; five years imprisonment otherwise.
NT	*Criminal Code Act*, ss189	Five years imprisonment if (i) the person's conduct contravened a condition of bail or an injunction or order imposed by a court (either under a law of the Commonwealth, the territory, a state or another territory of the Commonwealth); or (ii) the person was, on any occasion to which the charge relates, in the possession of an offensive weapon; two years imprisonment otherwise.
SA	*Criminal Law Consolidation Act 1935*, s19AA	Five years imprisonment for an aggravated offence or three years imprisonment for a basic offence.
Tas	*Criminal Code Act*	Except in capital cases, all sentences are left to the

	1924, s192	discretion of the judge of the court of trial, who may in any case impose a sentence of imprisonment up to 21 years (Blackwood & Warner 1993). Criminal Code Act 1924, s454 states that: except as is otherwise expressly provided, references in any enactment to a sentence of imprisonment passed on any person for a term not less than or exceeding a specified term are to be construed as including references to a sentence of imprisonment passed on that person for the term of his or her natural life.
Vic	*Criminal Code Act 1958*, s21A	10 years imprisonment.

Source: Urbas and Choo (2008: Table 3)

Mitigating cyber security risks

Cybercrime is one of the most rapidly expanding forms of criminality that knows no borders. Protecting consumers from cybercrime is a complex and difficult task. Cybercrime, however, if left unaddressed can have a more severe economic impact than many traditional crimes, and affect the financial security of online business in addition to causing social harm to individuals and social cohesion (Morris 2004; Choo & Smith 2008; Choo, Smith & McCusker 2007a). The widespread incidence of identity theft, for example, is a major challenge since such theft is a common precursor offence that requires a broad-based prevention effort (White & Fisher 2008). According to the United States Federal Trade Commission (cited in US GAO 2009: 3), 'in 1 year, as many as 10 million people—or 4.6 percent of the U.S. adult population—discover that they are victims of some form of identity theft, translating into reported losses exceeding [US]$50 billion'.

The threat of cybercrime has given rise to a growing demand for new strategies of response. These include the need to reduce the opportunities for cybercrime to occur, to make cybercrime more difficult to commit, and to increase the risks of detection and punishment associated with committing cybercrime.

Adopting a coordinated and collaborative approach

Australia's national information infrastructure comprises computerised control systems that support critical infrastructure in both the public and private sectors. These are vital to our national security, economic development, and national public health and safety. Security is only as strong as the weakest link. Tight couplings between different areas of critical infrastructure may result in rapid escalation of seemingly modest disruptions within one sector to others. If unsecured sectors are compromised, these sectors can be used as launching pads to attack other critical infrastructure sectors. A successful attack on the information technologies and communications infrastructure that supports many of the other critical infrastructures could disrupt supply chain management systems, financial sector networks or power grids. Consequences of these attacks could continue to have a reverberating impact well after the immediate damage is done.

Many sectors are privately owned and therefore, instituting an effective coordination with private sector organisations including public-private crisis management plays a pivot role in mitigating cybersecurity risks. Such partnerships can potentially when the industry participates in the sharing of sensitive information and could provide the following assistance:

- Building resilient systems (e.g. building resilient supply chains) and also cybersecurity protection.

- Providing training and enhance security awareness of the industry, in particularly small and micro businesses.
- Identifying risks which can aid in the development of effective measures and mitigation controls: controls required to mitigate individual risk might vary among different types of systems. For example, requirements for critical control systems usually differ from typical IT systems on aspects such as performance, availability, and risk management requirements.

Collaboration between the public and private sectors will also form strategic alliances outside our borders for risk management.

IT security in environments with high bandwidth and open systems such as universities needs to be bolstered (Choo, Smith and McCusker 2007). Examples of incidents involving security breaches at educational institutions include the 2009 May incident at the University of California, Berkeley. The university reported that the databases containing individuals' social security numbers, health insurance information and non-treatment medical information, such as immunization records and names of some of the physicians they may have seen for diagnoses or treatment might have been exposed to hacker(s) who broke into the university's computer systems (Gilmore 2009). There had been other instances of computers in environments with high bandwidth and open systems being compromised and used to facilitate other cybercrime such as in botnet-facilitated attacks.

Leveraging technologies

Although technologies on their own cannot solve problems of cybercrime, data mining and authentication technologies can be useful in combating financial crime and reducing incidences of fraud and identity theft.

Data mining

Data mining technologies such as transaction monitoring systems are designed to process and analyse large volumes of data, and identify and understand complex patterns of data (e.g. financial transactions). For example, transaction monitoring systems can be designed to prevent a transaction or generate an alert when a financial transaction above a threshold amount from an internet location in a pre-defined foreign country to a payee account with a suspicious address is processed.

Authentication technologies

Although Sullivan (2008) highlighted several studies demonstrating that the Europay, MasterCard and Visa standards consortium (EMV) smart cards may be circumvented by technically competent criminals, it is acknowledged that smart cards when implemented correctly can help to reduce card fraud and reduce identity theft incidences. Chairwoman Yvette D Clarke of the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Committee on Homeland Security in her prepared statement also pointed out that private sectors should continue exploring feasibility of ‘deploying new technologies – like chip and PIN – to fight fraud that could lead to organized crime and terrorism’ (Clarke 2009).

Social network analysis tools

Any individual can create multiple online identities or have multiple avatars (virtual representations of themselves in virtual worlds) and be a member of more than one social networking site at any one time. There are various types of relationships (or degrees of linkage) between individual user identities in online social networking sites such as MySpace and Friendster. These virtual relationships in online social networking sites can be broadly categorised into direct linkages between two online user identities (e.g. friends), quasi-direct linkages between two online user identities (e.g. friends’ friends), and indirect linkages between two online user identities (e.g. user identities who are ‘somehow’ connected to a

particular user identity via quasi-direct linkages). Social network analytical tools such as mapping tools can be extremely useful for law enforcement investigators when establishing virtual relationships and connections between offenders and their potential victims (e.g. in online child exploitation, cyberbullying and cyberstalking cases), understanding these relationships and connections, and analysing their implications in online social networking sites. van der Hulst (2009) also pointed out the importance of such tools to analyse criminal networks in order to gain a more thorough understanding of criminal behaviour.

Government has driven much of the response to technology-enabled crime but the private sector plays a crucial role. This is in part due to the design of the personal computer and the global adoption of the internet being largely in the hands of private sector forces that are less focused on security than on functionality. Thus the burden of protection against misuse of the technology has fallen to individual users. There is a flourishing industry of computer security products and services, such as antivirus software, intrusion detection devices and encryption tools, servicing the increasing desire of individuals and businesses to protect themselves against computer-related threats.

Commercial off-the-shelf (COTS) products form the backbone of many of our existing systems and networks. Such products, however, notoriously contain security vulnerabilities. Poorly designed, executed and maintained security protocols, programs, processes and devices leave computer networks open to attack. In 2007 IBM reported that the number of detected security vulnerabilities had increased by almost 40 percent from 2005 to a total of 7247 in 2006 (IBM 2007). 3534 vulnerabilities were reportedly documented by IBM in the first six months of the 2008 calendar year, which is an increase of five percent from the first half of 2007 (IBM 2008). A total of 6,098 vulnerabilities were reported to the United States-based CERT coordination centre in the first three quarters of 2008 (http://www.cert.org/stats/cert_stats.html#vulnerabilities). What is more concerning is that the number of ‘high severity vulnerabilities continued to rise in number and overall percentage [in the first half of 2008’ (IBM 2008: 4). As highlighted in the earlier section, such vulnerabilities could be exploited by criminals.

Many such risks can be minimised by the industry developing more secure hardware and software. It would, however, be insufficient to reduce software vulnerabilities and the overall defect content in software and hardware components. Security should also be integrated into the software and system development life cycle, as retrofitting security implementations to a released system typically require significant architectural or coding changes. Making late changes can be technically challenging and costly. Although several international standards have been designed to facilitate and ease the secure development of applications (also known as SDA), there does not appear to be widespread adoption of SDA (by software and hardware vendors). This could, perhaps, be attributed to competitive market forces dictating that software and hardware products with sophisticated functionalities have to be delivered at accelerated speeds (Viega et al. 2001). Consequently, less thorough code reviews and vulnerability testing are conducted resulting in less robust software and hardware applications that contain security flaws and bugs.

Industry has been making efforts to integrate security within the software and system development life cycle, in particular during early requirement analyses. Several industry initiatives aiming to design more trustworthy systems and to provide security mechanisms at the device interface have been established. For example, the Trusted Computing Group was formed to develop and promote open, vendor-neutral industry specifications and industry-wide codes of conduct for trusted computing. The Trusted Computing Group also plays a significant role in promoting best practice. Manufacturers need to be made aware that they could achieve marketing and competitive advantages if they produced new products with higher levels and more innovative types of security that would help combat technology-

enabled crime. Organisations actively seeking to go beyond mere compliance with existing legislation would generate greater consumer trust and confidence in the new world of informed consumers. Moreover, vendors of secure software and hardware would spend less time and resources on fixing and releasing patches for vulnerabilities. Law enforcement and security researchers could contribute to a stronger technology security environment by notifying manufacturers and vendors of weaknesses discovered in technologies to enable fixes to be formulated, by publicising weaknesses discovered during investigations and research, and by working with industry to identify potential new and emerging risk areas.

An effective legal and policy framework for cybersecurity

Law enforcement operates at three broad levels: crime prevention, investigation and prosecution (Choo, Smith and McCusker 2007a). It can reasonably be anticipated that cybercrime prosecutions involving multiple jurisdictions will continue to arise in the years ahead. Because online offending transcends borders so easily, numerous territories can simultaneously assert jurisdiction, particularly when an attack transits multiple jurisdictions with different regimes for preserving evidence. Investigations by law enforcement agencies and private investigators will also be hindered by the global distribution and increasingly corporate ownership of internet and cyberspace infrastructure and services. Trails of evidence may pass through innumerable hosts, each requiring legal authority to access evidence, while gambling at each step on evidence retention versus business demands for data storage.

Timely access to evidence located in one or more foreign jurisdictions may be difficult or impossible, as it would normally require the assistance of authorities in the foreign jurisdiction(s) that for various reasons may be unwilling or unable to assist. When the suspect is located abroad, these difficulties are compounded. It will be necessary for the international community to urgently address problems of multiple jurisdictions. This may poses a challenge for traditional criminal law and as explained by Brenner and Schwerha,

> [l]aw is at base territorial; criminal laws are promulgated and enforced by nation-states, which use them to control crime and maintain the baseline of internal order that a society requires to survive. Criminal law therefore has been purely domestic; external threats to order that came from nation-states were dealt with by the military, not by law enforcement. (Brenner and Schwerha 2008: 19).

The use of cybercrime legislation often seeks to proscribe transnational criminal activity. Recent legislation deals with this by enabling prosecutions to take place where the accused or victim are located in different jurisdictions as long as there remains a sufficient connection with the place in which the prosecution is commenced. Where an accused is located in another country, however, it may be necessary to seek extradition. Australia, for example, may request the extradition from other countries of persons who have committed acts online that adversely affect Australian citizens or interests for them to be returned to Australia to face prosecution (as governed by the *Extradition Act 1988* (Cth)). The *nullum crimen sine lege* principle is relevant in most legal systems. Satisfying the criterion of dual criminality – the alleged misconduct must constitute an offence under both the laws of the extradition country and Australia – is invariably necessary in both extradition and mutual assistance requests.

Only five years ago Smith, Grabosky and Urbas (2004: 156) observed when discussing crime in the digital environment that ‘those who fail to anticipate the future are in for a rude shock when it arrives’. Countering these risks requires effective international coordination and there is a continuing need to enhance cross-jurisdictional law enforcement and judicial cooperation in the fight against cybercrime as emphasized in a recent report by the

Commission of the European Communities (2008). Rita M Glavin – Acting Assistant Attorney General of the United States Department of Justice – also pointed out in her testimony before the House of Representatives Homeland Security Committee Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology that

> As illustrated by the array of cases I have mentioned, carders operating in carding forums on the Internet reside in different countries, collaborate freely across borders, and can immediately and widely distribute stolen identity information around the globe. In addition, online carding forums provide networking opportunities for criminals interested in joining together to perpetrate other financial fraud or criminal activity on a global scale. As a result, coordination and cooperation from foreign law enforcement is vital to the success of carding investigations and prosecutions. In this regard, the Identity Theft Task Force's Strategic Plan also recommended that the Department of Justice and other departments and agencies take specific steps to improve coordination and evidence sharing with foreign law enforcement agencies (Glavin 2009: 8).

In addition, achieving some measure of legislative uniformity will help to minimise the risk of so-called 'jurisdiction shopping' in which offenders seek out jurisdictions from which to base their activities that have the least severe punishments or which have no extradition treaties current. More recently, the European Commission has considered introducing harsher penalties for cybercriminals so that 'all 27 EU member states [are] in line with countries like the UK, France and Germany, which have longer sentences for cybercrime' (Ashford 2009).

The human dimension

It is generally understood that human actors are one of the weakest links in attempts to secure systems and networks. Choo, Smith and McCusker (2007a: 99) noted that '[i]nformation security awareness training courses inform end-users about their accountability for ensuring the integrity, confidentiality, privacy and availability of IT assets within the organisations. For example, in 2007 Microsoft investigated targeted attacks against Microsoft Word using a vulnerability in Microsoft Office 2000 and Office XP that allowed remote code execution when users opened an infected document'. There is growing awareness among end-users of the need for basic security online, constant and ongoing promotion of a culture of security for information systems and networks among end-users is essential to ensure employees (and also the public) are kept abreast of technology-enabled crime developments and how new security measures can be used to their advantage (Choo, Smith and McCusker 2007b).

A 2006 survey, however, indicated that 53 percent of respondents identified inadequate staff training / education in security practices and procedures as one of the most common weaknesses within organisations and one they believed contributed to electronic attacks (AusCERT 2006). The escalating complexities of the end-user environments underline the need for continuing training requirements. The Australian Bureau of Statistics estimated that, as at 30 June 2006, approximately 43.8 percent of the population in Australia was aged 40 and above (ABS 2006). This particular group might not be as IT literate as the younger generation and hence, might be an easier target for criminals. Constant and ongoing training programs are essential in educating this ageing population about the transnational nature of technology-enabled crime. Responses from 4,000 Australian businesses in the more recent ABACUS survey also signalled a worrying trend – a significant (79%) of businesses are unaware of any computer security awareness-raising initiatives (Richards 2009).

There is, therefore, a need for coordinated action by government agencies to ensure the most effective crime prevention advice is provided to the community. User education through

dissemination of media releases by authoritative institutions, such as SCAMwatch (http://www.scamwatch.gov.au/), would enable users to maintain current knowledge of the latest scams and the best fraud prevention measures available (Choo, Smith and McCusker 2007a).

Technological expertise, computer forensic capabilities, and sufficient investigative powers within government agencies are also important. A focus on training a few experts no longer suffices: both generic and specialist training with common standards are now demanded. The need for training in technology-enabled crime legislation, particularly concerning evidence and procedure, will increase as countries enact new legislation to deal with emerging threats. Initiatives such as the recent announcement by the Australian Federal Police (AFP) to train all AFP officers in forensic technology over the next 18 months to improve their ability to deal with cyber crime (and enable them to search and access computers at a crime scene without compromising information) (Sharma 2009) should be extended to other state and territory police forces within Australia .

Conclusions

As the internet and other forms of ICT continue to advance, the opportunities for criminal exploitation of online systems will increase. It is unlikely that traditional organised crime groups will shy away from using cyberspace to facilitate and/or to disguise illicit proceeds of real world based crimes as organised crime groups are very market driven and reflect many of the features of contemporary commerce (Choo, Smith & McCusker 2007a,b). The 2008 UK threat assessment, for example, explained that:

> global migration and ever more widespread information and communications technology (particularly the Internet) means that more and more criminals will have the contacts and capabilities to operate without boundaries, and those directing criminal activity find it easier to maintain their anonymity and reduce their risks (SOCA 2008:25).

The next wave of technology-enabled security threats will be targeted attacks aimed at specific organisations or individuals within enterprises. Organisations in the financial services industries and their top executives will be targeted more heavily than others (e.g. in spear phishing and whaling cases), with financial gain being the ultimate goal. The reasons for commercially motivated cybercrime will also change from greed and cupidity to politically or ideologically motivated activities. For example, the AusCERT (2006) survey and the DTI Information Security Breaches survey (PwC 2006) found an increase in the views held by the businesses surveyed that electronic attacks are more often motivated by illicit financial gain than in the past, both in Australia and around the world. The DTI Information Security Breaches survey (PwC 2006) further suggested that information security breaches cost British companies across several industry sectors £10 billion per annum. The United States Department of Justice’s national computer security survey estimated that cyber attacks cost American businesses US$314 million (Rantala 2008).

Choo, Smith and McCusker (2007a) cautioned that households and consumers are also likely to be targeted as a vector to support intrusions of more valuable targets. Criminals and malware authors are also targeting remote client machines as a means of attack (Kerr 2007). Thus prevention at both the consumer and business levels remains of equal importance. In addition to existing threats, new attacks will come from people, not just with programming experience but also with business and systems (process) and legal experience. There is a significant shift, therefore, in offender focus with more attacks targeting specific businesses and specific systems internal to those businesses. Cyber criminals will probe for weak and poorly guarded or unsecured computer networks within commercial organisations whose ability to detect and respond to fraud or other thefts is slow, imprecise and limited.

The need for further research

The "2007 inquiry into the future impact of serious and organised crime on Australian society" noted that 'the increasing use of technology, transnational connections and fluidity of organised crime groups will make law enforcement's task of policing organised crime's illicit activities more difficult' (PJCACC 2007:28). In the inquiry, Mr Alastair Milroy, *then* CEO of Australian Crime Commission, 'called for a greater involvement and contribution by academia to the body of research informing Australia's policy and operational choices in fighting organised crime' and suggested that:

> …a lot more work could be done to fill in some of the gaps…[such as] the value of organised crime markets, which is about the revenue derived by organised crime in pursuit of illegal activity…To deal with organised crime, to assist in forming policy and to have better operational responses, you have to look at the problem itself and understand organised crime markets (PJC ACC 2007:78).

A key issue, therefore, is the need to fill gaps in the knowledge base concerning cybercrime. Research efforts also need to entail greater collaboration within the international research community, which will allow law enforcement agencies, policy makers and other key stakeholders to understand and manage potential cybercrime threats more effectively.

References

All URLs were correct at 10 July 2009

Ashford W 2009. EC plans tougher sentences for cybercrime. *Computerweekly* 15 June. http://www.computerweekly.com/Articles/2009/06/15/236417/ec-plans-tougher-sentences-for-cybercrime.htm

AusCERT 2006. *Computer crime and security survey* Brisbane: AusCERT. http://www.auscert.org.au/images/ACCSS2006.pdf

Australian Associated Press (AAP) 2009. Aussie admits stalking American Idol star. *News.com.au* 20 May. http://www.news.com.au/story/0,23599,25511831-1243,00.html?from=public_rss

Australian Bureau of Statistics (ABS) 2006. *Population by age and sex, Australian states and territories*. ABS cat. no. 3201.0. http://www.abs.gov.au/ausstats/abs@.nsf/cat/3201.0

Australian Bureau of Statistics 2008. *Personal fraud, 2007* Canberra: ABS. http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/$File/45280_2007.pdf

Australian Communications and Media Authority (ACMA) 2007. *Media and communications in Australian families 2007*. Canberra: ACMA. http://www.acma.gov.au/WEB/STANDARD/pc=PC_310893

Australian Institute of Criminology (AIC) 2005. Child exploitation. *High tech crime brief* 2. Canberra: AIC. http://www.aic.gov.au/publications/htcb/htcb002.html

Blackwood J & Warner K 1993. *Tasmanian criminal law: text and cases*. Hobart: University of Tasmania

Brenner SW 2002. Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina journal of law and technology* 4(1). http://jolt.unc.edu/sites/default/files/brenner_.pdf

Brenner S 2006. Cybercrime jurisdiction. *Crime, law and social change* 46(4-5): 189-206

Byron T 2008. *Safer children in a digital world: the report of the Byron review*. Nottingham: DCSF Publications

Center for Strategic and International Studies (CSIS) 2008. *Securing cyberspace for the 44th presidency*. Washington, DC: Center for Strategic and International Studies.

Choo K K R 2007. Zombies and botnets. *Trends & issues in crime and criminal justice* no 333. Canberra: Australian Institute of Criminology.

Choo K K R 2008. Organised crime groups in cyberspace: a typology. *Trends in organized crime* 11(3): 270–295

Choo K K R 2009. Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences. Research and public policy series no. 92. Canberra: Australian Institute of Criminology.

Choo K K R & Smith R G 2008. Criminal exploitation of online systems by organised crime groups. *Asian journal of criminology* 3(1): 37–59

Choo K K R, Smith R G & McCusker R 2007a. *Future directions in technology-enabled crime: 2007–09*. Research and public policy series no. 78. Canberra: Australian Institute of Criminology.

Choo K K R, Smith R G & McCusker R 2007b. The future of technology-enabled crime in Australia. *Trends & issues in crime and criminal justice* no. 341. Canberra: Australian Institute of Criminology.

Clarke Y D 2009. *Prepared statement: Chairwoman Yvette D Clarke of the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Committee on Homeland Security*. http://hsc.house.gov/SiteDocuments/20090331141915-60783.pdf

Commission of the European Communities 2008. Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan. Commission staff working document SEC(2008) 511

Cox Communications 2007. *Teen internet safety survey, wave II*. http://www.cox.com/TakeCharge/includes/docs/survey_results_2007.ppt

Cross D, Shaw T, Hearn L, Epstein M, Monks H, Lester L & Thomas L 2009. *Australian covert bullying prevalence study (ACBPS)*. Perth, WA: Child Health Promotion Research Centre, Edith Cowan University

Despoja NS 2008. *Youth Poll 2008*. http://www.natashastottdespoja.com/cms_resources/Youth%20Poll%20May%202008.pdf

Federal Bureau of Investigation (FBI) 2008. Brazilian man charged in conspiracy to infect more than 100,000 computers worldwide with malicious software. *Media release* 21 August.

Federal Bureau of Investigation (FBI) 2009. Information security consultant sentenced to 4 years in prison in federal wiretapping and identity theft case. *Media release* 4 March. http://losangeles.fbi.gov/dojpressrel/pressrel09/la030409usa.htm

Fitzgibbon N & Wood M 2009. *Conficker.C: a technical analysis*. http://www.sophos.com/sophos/docs/eng/marketing_material/conficker-analysis.pdf

Franklin J, Paxson V, Perrig A & Savage S 2007. An inquiry into the nature and causes of the wealth of internet miscreants. In: Ning P, di Vimercati SDC, Syverson PF (eds) Proceedings of the 14th ACM conference on Computer and communications security, ACM CCS 2007, Alexandria, Virginia, USA, October 28–31, 2007. ACM, New York, pp 375–388

Gilmore J 2009. Hackers attack campus databases, steal social security numbers, other data. *Media release* 8 May. http://datatheft.berkeley.edu/news.shtml

Glavin RG 2009. *Statement of Rita G Glavin, Acting Assistant Attorney General Criminal Division United States Department of Justice before the House of Representatives Homeland Security Committee Subcommittee on Emerging Threats, Cybersecurity, and Science & Technology*. http://hsc.house.gov/SiteDocuments/20090331141958-47850.pdf

Garretson C 2007. Whaling: Latest e-mail scam targets executives. *Computerworld* 16 November. http://www.computerworld.com.au/index.php?id=1342062697&eid=-255

Goodin D 2007. TJX agrees to pay banks $41m to cover Visa losses. *Channel register* 3 December. http://www.channelregister.co.uk/2007/12/03/tjx_settlement_agreement/

Grabosky P N & Smith R G 1998. *Crime in the digital age: Controlling telecommunications and cyberspace illegalities* Sydney: Federation Press / New Brunswick: Transaction Publishers.

Grabosky P N, Smith R G, & Dempsey G 2001. *Electronic theft: Unlawful acquisition in cyberspace* Cambridge: Cambridge University Press.

Hadfield S 2009. Woman jailed for Idol cyber-stalking. *News.com.au* 29 May. http://www.news.com.au/story/0,27574,25555510-29277,00.html

Healey K & Murphy P 2009. Call to shut down teen 'revenge' website. *Herald sun* 19 June. http://www.news.com.au/technology/story/0,28348,25658569-5014239,00.html

IBM 2007. IBM X-Force 2006 trend statistics report. *IBM report* January. http://www.iss.net/documents/whitepapers/X_Force_Exec_Brief.pdf

IBM 2008. *IBM Internet security systems X-Force® 2008 mid-year trend statistics*. *IBM report* January. http://www-935.ibm.com/services/us/iss/xforce/midyearreport/xforce-midyear-report-2008.pdf

Jaques R 2006. European police nab zombie hackers. *Vnunet* 27 Jun. http://www.vnunet.com/vnunet/news/2159221/euro-police-nab-zombie-hackers

Keizer G 2007. Porn sites serve up Mpack attacks. *Computerworld* 25 June. http://www.computerworld.com.au/index.php?id=610295694&eid=-255

Kerr J 2007. Cyber crime battle. *Australian national security magazine* February: 21–23

Kirk J 2007a. Facebook sues Canadian porn company over hacking. *Computerworld* 18 December. http://www.computerworld.com.au/index.php?id=1056262081&eid=-255

Kirk J 2007b. Symantec: Chinese hackers grow in number, skills. *Infoworld* 18 May. http://www.infoworld.com/d/security-central/symantec-chinese-hackers-grow-in-number-skills-208

KPMG Forensic 2009. *Fraud survey 2008*. Australia: KPMG

Leyden J 2009. Indian embassy website hack part of wider assault: ad ranking scam or massive malware attack?. *The register* 29 January. http://www.theregister.co.uk/2009/01/29/indian_embassy_website_hack/

Litan A 2009. *2008 data breaches and financial crimes scare consumers away*. Stamford, CT: Gartner

McAfee 2005. *McAfee virtual criminology report*. Santa Clara CA: McAfee

McAfee 2008. *McAfee virtual criminology report: cybercrime versus cyberlaw*. Santa Clara CA: McAfee

McAfee 2009. *McAfee threats report: first quarter 2009*. Santa Clara CA: McAfee

McCombie S 2007. Organised cybercrime & phishing: the godfathers of the internet. Presentation at the Technology Trends 2007 seminars, CSIRO ICT centre, Australia, 12 February. Available at: http://www.ict.csiro.au/MU/Trends/

McCusker R 2006. Transnational organised cyber crime: distinguishing threat from reality. *Crime, law and social change* 46(4-5): 257-273

McMillan R 2008. Criminals hack ceos with fake subpoenas. *PC world* 14 April. http://www.pcworld.com/businesscenter/article/144548/criminals_hack_ceos_with_fake_subpoenas.html

McMillan R 2009. Paris Hilton's web site being used in web attack. *Computerworld* 13 January. http://www.computerworld.com.au/article/272877/paris_hilton_web_site_being_used_web_attack?eid=-144

Miller N 2007. From Russia with malice: criminals trawl the world. *The age* 24 July. http://www.theage.com.au/news/business/from-russia-with-malice-a-criminal-isp/2007/07/23/1185043032049.html

Moore T & Clayton R 2009. Evil searching: compromise and recompromise of internet hosts for phishing, in Proceedings of 13th International Conference on Financial Cryptography and Data Security. February 23-26, 2009: Barbados. http://people.seas.harvard.edu/~tmoore/fc09evil.pdf

Moses A 2009. Spammers hack into government jobs website. *The age* 26 January. http://www.theage.com.au/news/technology/security/id-theft-alert-as-job-site-hacked/2009/01/26/1232818299147.html

Morris S 2004. *The future of netcrime now: part 1 – threats and challenges*. http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf

Mullen P E, Pathé M & Purcell R 2009. *Stalkers and their victims (2nd ed)*. Cambridge: Cambridge University Press

Muir D 2005. *Violence against children in cyberspace*. Bangkok: ECPAT International

National Crime Prevention Council 2007. *Teens and cyberbullying*. http://vocuspr.vocus.com/VocusPR30/Temp/Sites/2623/57d586957e1d404ca0f0d5f6d0b18996/Cyberbullying-Exec%20Summary-FINAL.doc

National White Collar Crime Center (NW3C) 2009. *2008 internet crime report*. http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf

Nguyen TH, Ekholm J & Ingelbrecht N 2007. *Dataquest insight: More growth ahead for mobile gaming*. Stamford, CT: Gartner

Obama B 2009. *Remarks by the president on securing our nation's cyber infrastructure*. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

Ong B H 2008. In the real world, virtual gaming spells big business. *Straitstimes* 28 April. http://www.straitstimes.com/Free/Story/STIStory_231774.html

Parliament of Victoria, Drugs and Crime Prevention Committee 2004. *Inquiry into fraud and electronic commerce*, Final report, (Consultants: R. G. Smith and J. Walvisch) Melbourne: Government Printer.

Parliamentary Joint Committee on the Australian Crime Commission (PJCACC) 2007. *Inquiry into the future impact of serious and organised crime on Australian society*. Canberra: Parliament House

Porras P, Saidi H & Yegneswaran V 2009. *An analysis of Conficker C*. http://mtc.sri.com/Conficker/addendumC/

Rantala R R 2008. *Cybercrime against businesses, 2005*. http://www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf

Raywood 2009. Botnet discovered by Finjan contained 73 government domains. *SC magazine* 1 May. http://www.scmagazineuk.com/Botnet-discovered-by-Finjan-contained-73-government-domains/article/135953/

Reeckman B & Cannard L 2009. Cyberbullying: a TAFE perspective. *Youth studies Australia* 28(2): 41 – 49

Richards K 2009. *The Australian business assessment of computer user security: a national survey*. Research and public policy series no. 102. Canberra: Australian Institute of Criminology.

Rudd K 2008. *The first national security statement to the Australian parliament: Address by the Prime Minister of Australia The Hon. Kevin Rudd MP*. http://www.alp.org.au/download/now/national_security_statement_to_the_australian_parliament.pdf

Schaffer G P 2006. Worms and viruses and botnets, oh my!. *IEEE security & privacy* 4(3): 52–58

Serious Organised Crime Agency (SOCA) 2008. *The United Kingdom threat assessment of serious organised crime*. http://www.soca.gov.uk/assessPublications/downloads/UKTA2008-9NPM.pdf

Serious Organised Crime Agency (SOCA) 2009. *Serious Organised Crime Agency annual report 2008/09*. http://www.soca.gov.uk/assessPublications/downloads/SOCA_AR_2009.pdf

Sharma M 2009. Cyber crime courses for police. *Australian IT* 16 June. http://www.australianit.news.com.au/story/0,24897,25641259-15319,00.html

Sidambaram S 2000. *The role of police, prosecution and the judiciary in the changing society - the Singapore approach*. Resource material series no. 55: 303–335. Tokyo, Japan: United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders

Slonje R & Smith P K 2008. Cyberbullying: Another main type of bullying?. Scandinavian journal of psychology 49(2): 147–154

Smith A 2007. *Teens and online stranger contact*. Washington, DC: Pew Internet and American Life Project. http://www.pewinternet.org/PPF/r/223/report_display.asp

Smith B 2007. Law 'lags behind' cyber bullying. *The age* 17 May. http://www.theage.com.au/news/national/law-lags-behind-cyber-bullying/2007/05/16/1178995236283.html

Smith R G, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press

Sophos 2006. *Stopping zombies, botnets, and other email-borne threats*. Abingdon: Sophos

Straits Times 2009. Warning on malware 'market'. *Straits times* 17 June. http://www.straitstimes.com/Breaking%2BNews/Tech%2Band%2BScience/Story/STIStory_391534.html

Sullivan RJ 2008. Can smart cards reduce payments fraud and identity theft?. *Economic review* Third Quarter issue: 35–62. Kansas City MO: Federal Reserve Bank of Kansas City. http://www.kc.frb.org/PUBLICAT/ECONREV/PDF/3q08Sellon.pdf

Symantec 2009. *Symantec global internet security threat report trends for 2008: volume xiv*. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

Thomas T 2001. Supervising child sex offenders in the community: some observations on law and practice in England and Wales, the Republic of Ireland and Sweden. *European journal of crime, criminal law and criminal justice* 9(1): 69–90

United States Department of Justice (US DoJ) 2006. “Botherder” dealt record prison sentence for selling and spreading malicious computer code. *Media release* 8 May. http://www.usdoj.gov/criminal/cybercrime/anchetaSent.htm

United States Department of Justice (US DoJ) 2007. Six defendants indicted for stealing money from bank customers accounts through the internet. *Media release* 7 May. http://www.usdoj.gov/usao/cae/press_releases/docs/2007/05-07-07FriendInd.pdf

United States Department of Justice (US DoJ) 2008. KC man indicted for cyberstalking. *Media release* 9 May. http://kansascity.fbi.gov/dojpressrel/pressrel08/cyberstalking050908.htm

United States Government Accountability Office (US GAO) 2009. *Identity theft: governments have acted to protect personally identifiable information, but vulnerabilities remain*. Washington, DC: United States Government Accountability Office

United States National Drug Intelligence Center (US NDIC) 2007. *National drug threat assessment 2008*. Johnstown, PA: National Drug Intelligence Center

van der Hulst R 2009. Introduction to Social Network Analysis (SNA) as an investigative tool. *Trends in organized crime* 12(2): 101–121

Verizon 2009. *2009 data breach investigations report*. http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Viega J et al. 2001. Trust and mistrust in secure applications. *Communications of the ACM* 44 (2): 31–36

Websense Security Labs 2006. Malicious website/malicious code: fradulent YouTube video on MySpace installing Zango Cash. *Media release* 6 November. http://www.websense.com/securitylabs/alerts/alert.php?AlertID=689

White M & Fisher C 2008. Assessing our knowledge of identity theft: the challenges to effective prevention and control efforts. *Criminal justice policy review* 19(1): 3-24

Whitty M T 2008. Liberating or debilitating? An examination of romantic relationships, sexual relationships and friendships on the Net. *Computers in human behavior* 24(5): 1837–1850

Williams K R & Guerra NG 2007. Prevalence and predictors of internet bullying. *Journal of adolescent health* 41(6) Supplement 1: S14–S21

Wolak J, Mitchell K & Finkelhor D 2006. *Online victimization of youth: five years later. Alexandria, VA: National Center for Missing and Exploited Children*. http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=2530

Ybarra M L, Espelage D L & Mitchell K J 2007. The co-occurrence of internet harassment and unwanted sexual solicitation victimization and perpetration: associations with psychosocial indicators. *Journal of adolescent health* 41(6) Supplement 1: S31–S41

Zhuge J, Holz T, Song C, Guo J, Han X & Zou W 2008. Studying malicious websites and the underground economy on the Chinese web. In: Proceedings of the 7th Workshop on the Economics of Information Security, WEIS 2008, Hanover, New Hampshire, June 25–28, 2008