TILES

Briefing Paper No. 6 June 2008

Contact:
Associate Professor
Roberta Julian
Institute Director
University of Tasmania
Private Bag 22
Hobart Tasmania
Australia 7001
Telephone
+61 3 6226 2217
Facsimile
+61 3 6226 2864
Email
Roberta.Julian@utas.edu.au
tiles@utas.edu.au
Website
www.utas.edu.au/tiles
ISSN: 1832-701X

TASMANIAN INSTITUTE OF LAW ENFORCEMENT STUDIES

UTAS

Cyber-Victimisation in Australia: Extent, Impact on Individuals and Responses

Dr Lynne Roberts
Lecturer, School of Psychology,
Curtin University of Technology

The Tasmanian Institute of Law Enforcement Studies (TILES) publishes regular Briefing Papers on topics related to the Institute's research program. Our sixth Briefing Paper is prepared by Dr Lynne Roberts and is based on TILES' first public lecture at the University of Tasmania on 31 October 2007. At the time of this presentation, Lynne was a Research Fellow with the Crime Research Centre at the University of Western Australia. This Briefing Paper introduces readers to the impact that cyber-crime has on its individual victims, its prevalence and how we, as a society respond.

Roberta Julian, Director

Introduction

Over the last decade Australians have embraced new information and communication technologies. The majority of Australians now have access to computers and the Internet. By the beginning of 2007 there were 5.67 million households in Australia with home internet access(1), with many more individuals accessing the Internet through their work or studies. The Internet; while providing a range of benefits to individuals, organisations and governments; also provides new opportunities for criminal activities to emerge. These online criminal activities are commonly referred to as 'cyber-crimes'. While cyber-crime has received considerable media and some academic attention, the focus has largely been on the crime rather than offenders or victims.(2) The focus of this briefing paper is on individual victims of cyber-crimes.[i] Key questions to be addressed are:

- What is cyber-crime?
- How prevalent are cyber-crimes?
- What impact do cyber-crimes have on victims?
- How do we, as a society, respond to cyber-victimisation?

This paper begins with a brief overview of cyber-crime. This is followed by an exploration of the prevalence of cyber-crime and the impact on victims, focusing on three broad categories of cyber-crime: identity theft, the sexual exploitation of children online and cyber-harassment. The paper ends with an examination of legal, technical, regulatory, educational and professional responses to cyber-crime and cyber-victims.

[i] Organisations or governments can also be the victims of cyber-crime. Australian information on organisations as victims of cyber-crime can be found in the *2006 Australian Computer Crime and Security Survey* (http://www.auscert.org.au/render.html?it=2001

TASMANIAN INSTITUTE OF LAW ENFORCEMENT STUDIES

What is Cyber-Crime?

While there is no one generally accepted definition of cyber-crime, for the purposes of this paper the term 'cyber-crime' is used to refer to "any crime that is facilitated or committed using a computer, network or hardware device".[3] Information and communication technologies such as networked computers provide cheap, fast, secure, anonymous communication with multimedia capacity. They may be used as a means of communication and organisation to support existing criminal activities, to provide new ways of conducting criminal activities, to extend the geographic reach of criminal activities or to create new types of criminal activity.[4]

Computers may be used as the target or intermediary of cyber-crimes. Examples of computers as the target of cyber-crimes include data theft (e.g. copying of trade secrets) and breaches of data security. As the intermediary of crime, computers act as a buffer between offenders and victims, affecting how an offence is executed. For example, stalking can be conducted by repeatedly following or harassing another individual in person, but it can also be conducted using networked computers to engage in activities such as repeatedly sending harassing emails. While computers may be used as a mechanism for committing or organising criminal activity, they can also provide protection against detection and punishment through the additional layers of anonymity that offenders can utilise.

Cyber-crimes can be broadly divided into two categories: property cyber-crimes and interpersonal cyber-crimes. Property cyber-crimes are focused on achieving financial gain (i.e. fraudulent activities based on identify theft, scams and phishing emails). Interpersonal cyber-crimes are criminal activities conducted online that take the form of an 'assault' against the individual, their integrity or reputation. This can include acts such as cyber-harassment, cyber-bullying and cyber-stalking.

Cyber-crime is not a static category of crime. The increasing convergence of technologies means that crimes will change and new cyber-crimes (or variations on existing cyber-crimes) will emerge. The introduction of each new information and communication technology potentially expands the range of criminal opportunities and potential victims. For example, the introduction of third generation (3G) mobile telephones provides the potential for wide-spread mobile Internet access and increases security risks through possible intrusion by unauthorised persons, bandwidth leeching, exploitation of network access and increased risk of loss or theft.[5]

It is not possible in a paper this length to provide an adequate coverage of all types of cyber-crimes. Instead, this paper focuses on one type of property cyber-crime and two broad types of interpersonal cyber-crime. Identity theft has been selected as illustrative of a rapidly expanding property cyber-crime both within Australia and internationally. The online sexual exploitation of children and cyber harassment have been selected as two broad types of interpersonal cyber-crime that receive considerable attention in the media. Each of these types of cyber-crime is briefly described below.

Identity theft

Identity theft involves the online misappropriation of identity tokens (e.g. email addresses, webpages and the combination of username and password used to access systems), typically for financial gain. Other identity-related information that can be readily harvested online include names, contact details and, in the United States, Social Security Numbers. The combination of these identifiers is sufficient to obtain a credit card.[6]

Methods used to perpetrate cyber identity theft include hacking, phishing, pharming, traffic redirectors, advance-fee frauds, fake taxation forms, keyloggers and password stealers.[7] Phishing involves the use of emails and 'fake' websites to 'fish' for personal information such as credit card numbers, bank account information and passwords. Phishing emails often direct individuals to a specially created website that may 'spoof' a reputable organisation in order to fool individuals into providing confidential information. Social engineering techniques (e.g. scare tactics, such as threat of imminent closure of a bank account) are used to encourage compliance.[8] While early phishing attempts were amateurish, they now involve increasing sophistication such as the use of spyware and the installation of keyloggers on victims' computers to record keystrokes (including passwords and logins). Phishing is more effective when the phishing message appears to originate from a member of the recipient's social network.[9] The practice of phishing is widespread. In December 2007, 25,328 unique phishing websites were detected and remained online for an average three days. The most targeted industry sector is financial services.[10]

Online Sexual Exploitation of Children

The Parliamentary Joint Committee on the Australian Crime Commission on Cybercrime identified three main areas of concern in relation to the online sexual exploitation of children: pornographic child sex imagery; the sexual grooming and solicitation of children by paedophiles and children accessing unsuitable material online.[11] Each of these is briefly described below.

The Internet has enabled the fast transmission of child pornography across and between countries, increasing the market and visibility of child pornography through increasing the ease of producing and distributing digital material.[12] (The increased ease of access to child pornographic images is of particular concern given that recent laboratory research has demonstrated that exposure to pornographic images of underage-looking models increases viewers association of sex and sexuality to subsequent nonsexual images of youth.[13]

Children may be groomed for later sexual encounters or directly sexually solicited online. Two models of paedophilia operating in cyberspace have been identified.[14] The first model, the 'trust based seductive model', operates where a paedophile works to gradually obtain a child's trust before attempting to 'seduce' the child into sexual activity. The second model, the 'direct sexual model', dispenses with the stage of building trust and from the beginning is openly sexual.

Exposure to pornographic material online by children and youth may be planned or inadvertent. The Internet facilitates youth access to pornographic material through access to large quantities of free sexually explicit material, the limited age-related restrictions in place and the directed marketing of this material through pop-ups, spam and traffic forwarding.[15] Inadvertent exposure is of particular concern giving the paucity of research on the impact of this on children and youth.[16]

It should be noted that while these three areas of concern (pornographic child sex images, the sexual grooming and solicitation of children by paedophiles and children accessing unsuitable material online) have been grouped into the category of the online sexual exploitation of children, each represents a separate activity that is not necessarily related to the others. For example, while it is possible for a predator to provide potential 'targets' with pornographic material as part of the grooming process, many adolescents may access or be exposed to pornographic material online without any contact from a predator.

Cyber-Harassment

Individuals may be subjected to a range of harassing activities online. The Internet provides a wide range of opportunities for individuals to interact with strangers, expanding the potential 'pool' of victims for harassing activities.

Cyber-bullying is a term used to refer to bullying behaviour conducted online through media such as email, newsgroups, bulletin boards, instant messaging, websites and online games. Cyber-bullying behaviours encompass online postings, conversations or messages that are designed to harass, humiliate and intimidate the receiver. This may include threats, insults and teasing. Multimedia capacity extends the range of bullying material to videos and images (such as 'photo-shopping' a victim's face onto pornographic images). The potential audience for cyber-bullying activities is far larger than for its offline counterpart[17] and the bullying may be more concrete than verbal harassment.[18]

Cyber-stalking is a term used to refer to stalking activities conducted online utilising a range of tools and virtual environments. While the most commonly used methods of cyber-stalking are email and instant messages[19], the types of stalking activities engaged in range from threats, harm to reputation ('cyber-smearing'), damage to data or equipment to attempts to access confidential information and computer monitoring.[20,21] Cyber-harassment, cyber-bullying and cyber-stalking are terms that appear to be used interchangeably in the literature without clear definitional differences. The term cyber-bullying tends to be used when talking about the harassment of children and the terms cyber-stalking or harassment used when talking about the harassment of adults. The use of these terms in relation to online harassment has been questioned. Wolak, Mitchell and Finkelhor argued that most online incidents that are labelled as cyber-bullying do not involve both repeated aggression and a power imbalance between the victim and aggressor (the generally accepted defining features of bullying), and recommended the use of the term 'online harassment' be utilised to describe harassment that does not include offline components.[22] Similarly, a contentious issue in the cyber-stalking literature is whether this behaviour is best conceptualised as a new form of deviant/criminal behaviour or as simply an extension of offline stalking behaviours.[23,24,75]

How Prevalent are Cyber-Crimes?

The prevalence and incidence of cyber-crimes affecting individuals in Australia is largely unknown. To date, there has been no comprehensive population survey undertaken to provide reliable estimates across types of cyber-crimes.[ii] In this section information is provided on estimates of the frequency of the three types of cyber-crime that are the focus of this paper: identity theft, the sexual exploitation of children online and cyber-harassment.

Identity Theft

Information and communication technologies increase the ease and reduce the costs (time, financial and location) of identity token and data acquisition, expanding the range of potential victims and the scale on which identity theft can be perpetrated.[8,25,26] For example, hacking was used to obtain account information for 40 million credit card customers held by Card Systems Solutions.[27] A recent estimate suggests that approximately 40% of all identity frauds are facilitated online.[28] The use of traditional methods is declining with the increased use of information and communication technologies. For example, Hoskin, commenting on the changing nature of fraud in government welfare payments in Australia, noted that stolen identities are replacing the creation of false identities, enabling fast, repeated and difficult to trace fraudulent activities.[29]

It is very difficult to disentangle the amount of fraud that is due to cyber-identity theft as a large proportion of victims do not know how their identifying information was stolen. Fraud associated with identity theft is a major source of reported cyber-crime internationally. Survey research suggests that in the United States alone, 8.4 million Americans were the victims of identity fraud in 2006, with the total cost of this fraud estimated at $49.3 billion.[30]

[ii] The exception to this is the personal fraud victimisation survey conducted by the Australian Bureau of Statistics on behalf of the Australasian Consumer Fraud Taskforce. The results of this survey are due to be released later this year.

In Australia identity theft itself is not a criminal offence, although the use of stolen identities in fraudulent activities is. Survey research commissioned by the Federal Office of the Privacy Commissioner, reported that 9% of survey respondents stated they had been the victim, 17% knew of somebody that was a victim, and 60% were concerned that they would become a victim of identity theft.[31]

Online Sexual Exploitation of Children

Establishing the prevalence of child pornography online is hampered by differing definitions of child pornography and the absence of reliable estimation methods. It is known that some covert groups who use the Internet to exchange child pornography have extreme membership requirements. For example, the Wonderland Club required potential members to submit 10,000 new child pornography images to join.[32] Groups vary in their membership base, with some having memberships in the tens of thousands.[33] Another indicator of the prevalence of child pornography online is the number of reports made to authorities. In the US the CyberTipline coordinates the reporting of online child sexual exploitation, including child pornography. In 2006, 76,584 reports were made to the CyberTipline, of which 62,480 related to the possession, manufacture and distribution of child pornography.[34]

The number of children who have been sexually solicited online has yet to be reliably estimated. One early Australian study reported that more than a quarter (27%) of adolescent survey respondents who used chat rooms believed they had received a sexual solicitation.[35] In the US in 2005, approximately one in seven youth (13%) reported receiving sexual solicitations online, down from one in five (19%) in 1999/2000.[36] The CyberTipline, also in the US, received 6,384 reports of online enticement of children for sexual acts in 2006.[34] Farfinski estimated that 850,000 unwanted sexual approaches were made to children in the United Kingdom in 2006.[28]

Research suggests that girls aged between 13 and 15 are at highest risk of internet-initiated sexual offences, in stark contrast to the image often presented in the media of a paedophile preying on young children online. Based on a stratified random survey of law enforcement agencies in the US, Wolak, Finkelhor and Mitchell reported that 75% of juvenile victims of sexual offences where the offender and victim originally met online were 13 to 15 year old girls.[37] In the majority of cases, the adult offenders were openly sexual from the beginning and the victims claimed to have formed close attachments to the perpetrators. This type of relationship has been described by Wolak et al as better fitting a model of statutory rape than paedophilic child molesting. Internet-initiated statutory rape was estimated to comprise 7% of all statutory rapes in the US in 2000.[38]

The potential for children and youth to be exposed to pornographic material online is high. Based on a survey of 629 high school students aged between 13 to 16 years in the Australian Capital Territory, Fleming, et al reported that the majority of adolescents online were exposed to inappropriate materials and behaviours.[39] More than nine out of ten males and six out of ten females surveyed reported exposure to pornography online. However, some caution is needed in interpreting the results of this survey as it was not specified whether the exposure was inadvertent or planned. Where surveys ask about unwanted exposure, lower rates are reported. For example, successive 'Youth Internet Safety Surveys' conducted in the United States found that one-quarter[16] to one-third[36] of youth report exposure to unwanted sexual material online over a 12 month period.
An exception to this was an Australian study of 16 to 17 year old Australians, where the majority of survey respondents (84% boys and 60% girls) reported accidental exposure to internet sex sites.[15] Increased unwanted exposure has been attributed to increasing internet use, improved technology and the aggressive marketing of pornography websites[40], with the introduction of 3G mobile phones posited to further increase unwanted exposure.[41]

Cyber-Harassment

Just over one-third of 13 to 16 year old Australian students surveyed reported being cyber-bullied online[39]. This is consistent with estimates of cyber-bullying and harassment from two major surveys of adolescent internet users[42,43] but three times higher than reported in the Youth Internet Safety Survey.[44] Despite the seemingly high prevalence of cyber-bullying and harassment reported by youth, the majority of youth (67%) report that bullying and harassment happen more frequently offline than online.[43] Similarly, surveys of college students have found that between one in ten and one-third of students report at least one form of online harassment.[45,46]

Most surveys of stalking do not allow the disaggregation of cyber-stalking from other stalking behaviours. Typically telephone calls, mail and electronic communication are combined into a single category.[47] However, recent research based on a large sample (~1,000) of self-identified stalking victims suggests that more than half of stalking cases do not involve cyber-stalking components at all. Four percent of respondents reported online stalking only, while 5% reported that online stalking was followed by offline stalking. A further 38.6% experienced some online harassment supplementing offline harassment.[48] Similarly, between one-half and one-third of college students who report being stalked, report emailing as part of the stalking behaviour.[49,50]

Cyber-Victimisation

Victims vary in their responses to criminal acts. Factors influencing individual responses include characteristics

of the victim (e.g. age, gender, pre-victimisation adjustment), characteristics of the criminal event (e.g. type and seriousness of crime, relationship between victim and offender, and victim's perception of who was to blame) and characteristics of the post-victimisation experience (e.g. level of involvement in the criminal justice system and degree of social support.[51] Typically, victims experience an initial shock reaction which may be followed by physical, psychological and/or financial effects in the short term and possible longer term effects on employment and relationships.[52] In addition to primary victimisation resulting from the criminal event, an individual may experience secondary victimisation resulting from the way institutions and individuals respond to their situation and needs.

Victims of cyber-crimes are also likely to vary in their responses. Only a small percentage of cyber-crimes are reported to the police, estimated at 120 to 150 reports per 1,000,000 cyber-crimes in the United Kingdom.[53] Reluctance to report cyber-crimes may be due to embarrassment, lack of knowledge on where or how to report the crime, or the small size of the loss.[53] Some, especially identity theft victims, may not realise their victim status until sometime after the criminal act when they are denied a loan or other services because of a poor credit rating.

Victims of Identity Theft

Organisations (defrauded creditors) are often regarded as the primary victims of identity theft as they typically incur the financial cost of the fraudulent use of stolen identities.[54] Estimates of the indirect financial costs borne by the individual in addressing the identity theft and related fraudulent activities vary widely, with the cost to the individual increasing with the time from theft to discovery.[55] In addition to financial loss, identity theft victims may experience impaired credit ratings, damage to their reputation and their integrity of identity, criminal investigation, lost productivity and psychological impacts including stress, emotional trauma and relationship breakdown.[56,57,58,54] Where these problems are difficult to resolve, victims are more likely to experience mental health problems such as clinical somatisation, depression and anxiety.[59]

Victims of identity theft may experience secondary victimisation where they are denied access to victim services because they are not recognised as being the primary victim.[58,60] Impaired credit ratings may contribute to secondary victimisation through denial of credit, increased insurance and credit card interest rates, cancellation of credit cards, denial of services and continued contact by collection agencies.[61,57,55] Further, victims may be investigated by police in relation to crimes committed with the stolen identities.[61,58,62,57]

Child Victims of Online Sexual Exploitation

Child pornography is a form of sexual abuse that may be physically, psychologically and emotionally damaging to the child leading to maladaptive and destructive behaviours in later years.[63,64] The recording of the sexual abuse may further exacerbate the effects of sexual abuse.[65] Surprisingly little is known about the child victims of online pornography. A key point that is often lost in discussion of child pornography online is that the original victimisation typically occurs offline, with further victimisation occurring through the wide dissemination of images. Key areas identified for further research in this area are determining how to identify the children in order to stop the abuse and provide support and examining the effects on the child victim.[66]

The nature of online sexual solicitation of youth online is changing along with the changing behaviours of youth online. The results from the Youth Internet Safety Surveys, conducted in 1999/2000 and 2005, indicate that youth are now less likely to interact with strangers online (34% in 2005 from 40% in 1999/2000) and form close relationships (11% from 16%) than previously. This is reflected in changes in the relationship between perpetrator and victims. In 2005, approximately one in eight solicitations were from offline friends and acquaintances (up from 3% in 1999/2000). A significant minority of solicitations (41%) occurred while the victim was using the Internet with offline peers. While the majority (91%) of youth exposed to unwanted sexual material or solicited online do not report being distressed by the incident[36], youth with problems or a history of sexual or physical abuse may be particularly vulnerable to sexual solicitations online.[38]

Potential harms associated with children and youth accessing pornographic material online include misinformation, exposure to developmentally inappropriate material and the potential development of sexually compulsive behaviour or sexual addiction.[67] Australian research suggests that when adolescents are exposed to upsetting content online the actions they take are appropriate. The majority (80%) leave the site with other common responses including blocking the sender (44%) or logging off (12%).[34]

The exposure of youth to pornographic images and sexual solicitations online needs to be viewed within the context of youth's behavior off and online. Many youth actively seek out sexually explicit material, whether for curiosity, knowledge or sexual stimulation.[15] Approximately three-quarters of 16 to 17 year old Australian boys have watched x-rated movies offline, and approximately two out of five report actively searching for sex sites online.[15] Chat rooms are frequently used by teenagers in developing their sexual identity and the use of sexualised nicknames, utterances and themes are common.[68] Rather than a common site for sexual exploitation of minors, it has been proposed that the Internet may provide a 'safer' environment for exploring sexuality than offline settings.[69]

Victims of Cyber-Harassment

Children harassed and bullied online vary in their reactions to the behavior. More than one-third (38%) of 10 to 17 year olds harassed online report being distressed as a result of the harassment.[44] Many victims of cyber-bullying experience sadness, anger, anxiety, and fear.[70]

Being a victim of online harassment may be an indicator of problems in the child's offline life. Youth victims of online

harassment are more likely than other youth to exhibit major depressive-like symptoms[71], report more school problems such as detentions, suspensions, and unauthorised school absences[42,72], violent behaviours[42], substance use[42], social problems[44] and victimisation in other contexts.[44]

Youth involved in bullying offline (as victim or perpetrator) are two and a half times more likely to experience cyber-bullying online than other youth.[42] Those who report being an aggressor as well as a target of Internet harassment face significant psychosocial challenges.[73] Youth targeted for harassment were more likely to harass others online themselves. Similarly, Li reported that almost one-third of Canadian junior high student victims who had been bullied offline, had also been cyber-bullied.[74]

Research comparing the experiences of victims stalked, on and offline suggests that medical, psychological, social and financial effects are commonly experienced by both victims of online and offline stalking, with the loss of family and friends more frequently reported with online stalking.[48] In addition, the harm caused by cyber-smearing (e.g. placing false information about an individual on the Internet) may be greater than harm caused offline due to the persistence of records online and the increased potential audience.[75]

More competent computer-mediated communication users may be less likely than inexperienced users to become the victims of cyber-stalking[76] and experience harassment as less distressful.[20,21] The Internet presents a 'double-edged sword' for stalking victims.[77] While information and communication technologies provide tools for stalkers to use in stalking their victims, they can also provide the means of information, communication and support for victims and helping professionals.

How do we, as a Society, respond to Cyber-Victimisation?

All governments have an ethical responsibility to address the needs of victims of crime, and this includes the victims of cyber-crimes. While most western countries, including Australia, offer a range of services to crime victims only a minority of victims avail themselves of these services, tending to rely instead on the support of family and friends. Cyber-crimes are relatively new crimes and responses to cyber-victimisation are still developing. These include legal, technical, regulatory, educational and professional responses.

Legal Responses

The justice needs of cyber-victims may be partially met through the criminal investigation of cyber-crimes and prosecution of cyber-offenders. This is dependent on the existence of laws covering cyber-crimes and the willingness of police to investigate cyber-crimes. Some cyber-crime offences are already covered under existing laws or through the introduction or amendment of legislation to cover online instances of existing criminal behaviours. However, the key issue hampering legal responses is that while cyber-crime is global, most laws are restricted to nations or states and the investigation and prosecution of cyber-crimes is reliant on cooperation between jurisdictions. Cooperation is currently hindered by the lack of consistent definitions of cyber-crimes and inconsistencies in the sanctions imposed across jurisdictions.[78] Within Australia, the Australian High Tech Crime Centre is charged with providing a national coordinated approach to cyber-crime investigation and of improving the capacity of jurisdictions to deal with cyber-crime.

Blindell reviewed the legal status and rights of identity theft victims in Australia.[79] In most states of Australia, identity theft victims are not classified as victims of crime and are consequently not eligible for existing victims' rights and services. The report highlighted the need for the development of a specific identity theft offence and the explicit inclusion of identity theft victims within statutory definitions of victims. These statutory rights should include the recovery of costs relating to reporting the theft, preventative action to limit further use and financial reputation restoration; the right to access victim assistance services; the right to victim certificates and to have victim affidavits recognised; and the right to present victim impact statements to sentencing courts. Similarly, to effectively respond to the growing identity crime problems, identity theft needs to be made a federal crime in Australia.[80]

Within Australia, the Australian Federal Police established an Online Child Sexual Exploitation Team (OCSET) in January 2005, to provide a national assessment and coordination capability for international and national referrals of child pornography. In 2005/2006, OCSET made 21 arrests and secured ten convictions/guilty pleas on charges relating to the possession and transmission of child pornography and cyber-grooming.[81]

At the state level, police 'sting' operations have been established in Western Australia and Queensland.[33] These operations involve police officers posing as children or youth online in order to attract and identify paedophiles. The police officers do not initiate sexual discussions but respond to advances. In Queensland, the police officers pose as girls aged 13 to 16 years. The activities engaged in by 'suspects' during these stings included meeting offline to perform a sexual act, discussing sex and sexual acts in general, discussing sexual acts involving the child, sending sexually explicit material, online masturbation using a webcam and making offers of reward for sexual services.[33]

Legislative and investigative approaches are unlikely to be sufficient to enable the investigation and prosecution of all cyber-crimes, highlighting the need for police to establish a network of relationships in order to effectively police cyber-crimes. The majority of cyber-

criminal activities are resolved without police involvement and working relationships need to be established between police and internet user groups, online virtual environment managers, network infrastructure providers, corporate security organisations, and non-governmental and governmental non-police organisations in order to effectively 'police' cyberspace.[82]

Technical Responses

Technical solutions may be utilised to reduce or 'design out' some types of cyber-crimes, typically through the filtering, blocking and monitoring of digital data. Internet filters such as 'Net Nanny' are employed to block content unsuitable for children. Approximately one in five Australian adolescents report that software filters are used at home.[39] However, no blocking or filtering system provides complete accuracy in the material that is blocked. For example, recent Australian tests of the efficacy of server based internet content filters found that the best of the filters blocked only 76% of content that should be blocked.[83] Filtering and blocking systems need to be updated continuously to retain any form of currency.

Industry Codes, Standards and Regulations

Industry codes of practice and standards have been advocated as a means of controlling cyber-crimes.[84] Within Australia, the relevant government regulatory body for information and communication technologies is the Australian Communications and Media Authority (ACMA). The Internet Industry Association is currently developing the *IIA Cybercrime Code of Practice* (see http://www.iia.net.au). The degree to which the onus of detecting and reporting of cyber-crimes should be the responsibility of Internet Service Providers is contentious.

Educational Responses

All internet users need to be aware of how to protect their personal information online and how to interact safely within virtual environments. Materials relating to internet safety are readily available online. For example, NetAlert (http://www.netalert.net.au/), the website of Australia's Internet Safety Advisory Body (a not-for-profit community organisation established by the Australian government to provide independent advice and education on managing access to online content), contains a wide range of information on internet safety directed at parents, teachers, librarians and children. This includes online interactive educational games that are targeted at children of different ages. Parents, teachers and caregivers will need to keep abreast of changing technologies in order to protect children.

An internet harassment component should be added to all anti-bullying programs in schools. Prevention efforts need to be targeted at those youth most at risk, with education about sexual solicitation targeted at preteens and teens. Reporting of all types of online harassment should be promoted, with increased options for reporting, and the reasons for reporting emphasised.[40,37,36,38,44,72]

Professional

Support services to cyber-crime victims may be provided on or offline, through existing agencies supporting all types of crime victims, or through specialised services. Professionals working with cyber-crime victims need to be familiar with the varying impacts of cyber-victimisation and the needs of victims. Mental health professionals need to be aware of online sexual predatory behaviour in order to recognise the signs of children and youth who may be victims and to become sensitised to their needs.[17,14] Cyber-crime victims (children, youth and adults) may present with online victimisation as the primary presenting problem, or with a range of online and offline problems.[85,86,87]

Summary

Information and communication technologies create new opportunities for criminal activities. New forms of cyber-crime will continue to emerge with the introduction of new information and communication technologies and are likely to produce new victims. Victims will vary in their responses to cyber-criminal acts and not all will experience distress or require access to victims' services. Combinations of strategies will be required to effectively prevent cyber-victimisation. For example, the need for a combination of technical solutions, education, parental monitoring and legal responses have been proposed as essential to protect children from sexual exploitation online.[88,89,90] Where prevention activities are not effective, crisis intervention, counselling, advocacy and support services will need to be equipped to deal sensitively with those cyber-victims who do require help. To inform this service provision, further research is required into the impact of cyber-victimisation and appropriate responses.

TASMANIAN INSTITUTE OF LAW ENFORCEMENT STUDIES

References

1. Australian Bureau of Statistics. (2007). *Catalogue 8153.0 - Internet Activity, Australia, Mar 2007*. Retrieved April 14, 2008 from http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8153.0Main+Features1Mar%202007?OpenDocument
2. Wall, D. S. (2005). The Internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 78-94), Thousand Oaks, CA: Sage.
3. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.
4. Savona, E. U., & Mignone, M. (2004). The fox and the hunters: How IC technologies change the crime race. *European Journal on Criminal Policy and Research*, *10*, 3-26.
5. Urbas, G., & Krone, T. (2006). Mobile and wireless technologies: security and risk factors. *Trends & Issues in Crime and Criminal Justice, No. 329*. Canberra: Australian Institute of Criminology.
6. Sweeney, L. (2006). Protecting job seekers from identity theft. *IEEE Internet Computing*, *10*(2), 74-78.
7. Paget, F. (2007). Identity theft. *McAfee Avert Labs technical white paper No 1*. Retrieved May 27, 2007 from http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf.
8. Lynch, J. (2005). Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks. *Berkeley Technology Journal*, *20*, 259-300.
9. Jagatic, T. N., Johnson, N. A., Jacobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*, 94-100.
10. Anti-Phishing Working Group (2008). *Phishing activity trends report for the month of December*, 2007. Retrieved April 10, 2008 from http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf
11. Parliament of the Commonwealth of Australia (2004). *Parliamentary Joint Committee on the Australian Crime Commission: Cybercrime*. Canberra: Commonwealth of Australia.
12. Schell, B. H., Martin, M. V., Hung, P. C. K., & Rueda, L. (2007). Cyber child pornography: A review paper of the social and legal issues and remedies- and a proposed technological solution. *Aggression and Violent Behavior, 12*, 45-63.
13. Paul, B., & Linz, D. G. (2008). The effects of exposure to virtual child pornography on viewer cognitions and attitudes toward deviant sexual behaviour. *Communication Research*, *35*, 3-38.
14. Deirmenjian, J. M. (2002). Pedophilia on the Internet. *Journal of Forensic Science*, *47*(5), 1-3.
15. Flood, M. (2007). Exposure to pornography among youth in Australia. *Journal of Sociology*, *43*, 45-60.
16. Mitchell, K. J., Finkelhor, D., & Wolak, J. (2003). The exposure of youth to unwanted sexual material on the Internet: A national survey of risk, impact and prevention. *Youth & Society*, *34*, 330-358.
17. Chisholm, J. F. (2006). Cyberspace violence against girls and adolescent females. *Annals of New York Academy of Sciences*, *1087*, 74-89.
18. Campbell, M. A. (2005). Cyber bullying: An old problem in a new guise? *Australian Journal of Guidance and Counselling*, *15*(1), 68-76.
19. D'Ovidio, R., & Doyle, J. (2003). A study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin*, *72*(3), 10-17.
20. Bocij, P. (2003b). Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet. First Monday, *8*(10). Retrieved April 15, 2007 from http://firstmonday.org/issues/issue8_10/bocij/index.html
21. Bocij, P., & Sutton, M. (2004). Victims of cyberstalking: Piloting a web-based survey method and examining tentative findings. *Journal of Society and Information, 1*(2). Retrieved April 15, 2007 from http://josi.spaceless.com/.
22. Wolak, J. D., Mitchell, K. J., & Finkelhor, D. (2007). Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *Journal of Adolescent Health, 41*, S51-S58.
23. Bocij, P., Bocij, H. & McFarlane, L. (2003). Cyberstalking: A case study of serial harassment in the UK. *The British Journal of Forensic Practice, 5*(2), 25-32.
24. Bocij, P., & McFarlane, L. (2003a). Cyberstalking: The technology of hate. *The Police Journal, 76*, 204-221.
25. Marshall, A. M., & Tompsett, B. C. (2005). Identity theft in an online world. *Computer Law & Security Report, 21*, 128-137.
26. Finch, E. (2007). The problem of stolen identity and the Internet. In Y Jewkes (Ed.), *Crime on-line* (pp. 29-43). Cullompton: Willan.
27. Haygood, R., & Hensley, R. (2006). Preventing identity theft: New legal obligations for businesses. *Employment Relations Today, 33*(3), 71-83.
28. Farfinski, S. (2007). UK Cybercrime Report. Retrieved April 10, 2008 from https://www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf
29. Hoskin, P. (2006). Emerging fraud risks and countermeasures in government welfare programs. Paper presented at The Australian & New Zealand Society of Criminology 19th Annual Conference, Sydney, Australia.

30. Javelin Strategy and Research. (2007). 2007 *Identity fraud survey report-Consumer version:. How consumers can protect themselves.* Retrieved May 27, 2007 from www.javelinstrategy.com.

31. Wallis Consulting. (2007). Community attitudes to privacy, 2007. Retrieved April 4, 2007 from http://www.privacy.gov.au/publications/rcommunity07.pdf

32. Krone, T. (2005). International police operations against online child pornography. *Trends & Issues in Crime and Criminal Justice, No. 296*. Canberra: Australian Institute of Criminology.

33. Krone, T. (2005). Queensland police stings in online chat rooms. *Trends & Issues in Crime and Criminal Justice, No. 301*. Canberra: Australian Institute of Criminology.

34. CyberTipline (undated). *CyberTipline fact sheet*. Retrieved June 3, 2007 from http://www.cybertipline.com/en_US/documents/CyberTiplineFactSheet.pdf

35. Stanley, J. (2001). Child abuse and the Internet. *National Child Protection Clearinghouse Child Abuse prevention Issues No. 15*.

36. Wolak, J., Mitchell, K., & Finkelhor, D. (2006). *Online victimisation of youth: Five years later*. Durham, NH: National Center for Missing and Exploited Children.

37. Wolak, J., Finkelhor, D., & Mitchell, K. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health, 35*(424), e11– e20.

38. Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online "predators" and their victims: Myths, realities, and implications for prevention and treatment. *American Psychologist*, *63*, 111–128.

39. Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A., & Morrison, S. (2006). Safety in cyberspace: Adolescents' safety and exposure online. *Youth & Society, 38*, 135-154.

40. Mitchell, K., Wolak, J., & Finkelhor, D. (2006). Trends in youth reports of sexual solicitations, harassment and unwanted exposure to pornography on the Internet. Journal of Adolescent Health, 40, 116-126.

41. Reid, A. S. (2005). The rise of third generation phones: The implications for child protection. *Information and Communications Technology Law, 14*(2), 89-113.

42. Hinduja, S., & Patchin, J. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimisation. *Deviant Behavior, 29*, 129-156.

43. Lenhart, A. (2007). *Cyberbullying and online teens*. Washington, DC: Pew Internet & American Life Project. Retrieved April 14, 2007 from http://www.pewinternet.org/PPF/r/216/report_display.asp

44. Ybarra M. L., Mitchell, K. J., Wolak, J. & Finkelhor, D. (2006). Examining characteristics and associated distress related to Internet harassment: Findings from the second Youth Internet Safety Survey. *Pediatrics, 118*(4), e1169-e1177.

45. Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*(4), 468-483.

46. Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society, 4*(1), 71-92.

47. Australian Bureau of Statistics. (2006). *Personal Safety Survey Australia: 2005 (Reissue)*. Canberra: Commonwealth of Australia.

48. Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law, 13*, 627-640.

49. Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of cyberstalking among college students. *Brief Treatment and Crisis Intervention, 5*(3), 279-289.

50. Fisher, B. S., Cullen, F. T., & Turner, M. G. (2000). *The sexual victimisation of college women*. National Institute of Justice and Bureau of Justice Statistics Research Report: NCJ 182369. Retrieved April 15, 2007 from http://www.ncjrs.gov/pdffiles1/nij/182369.pdf

51. Lurigio, A. J., & Resnick, P. (1990). Healing the psychological wounds of criminal victimisation: Predicting postcrime distress and recovery. In A. J. Lurigio, W. G. Skogan & R. C. Davis (Eds.), *Victims of crime: Problems, policies and programs* (pp. 50-67). Newbury Park, CA: Sage.

52. United Nations. (1999). *Handbook on justice for victims: On the use and application of the Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power*. New York: Centre for International Crime Prevention

53. Wall, D. S. (2004). Digital realism and the governance of spam as cybercrime. *European Journal on Criminal Policy and Research, 10*, 309-335.

54. LoPucki, L. M. (2001). Human identification theory and the identity theft problem. *Texas Law Review, 80*, 89-135.

55. Synovate (2003). *Federal Trade Commission-Identity theft survey report*. Retrieved May 20, 2007 from http://www.ftc.gov/os/2003/09/synovatereport.pdf

56. Identity Theft Resource Centre. (2003). Identity theft: The aftermath 2003. Retrieved March 2, 2007 from http://www.idtheftcenter.org/idaftermath.pdf.

57. Identity Theft Resource Centre. (2005). Identity theft: The aftermath 2004. Retrieved March 2, 2007 from http://www.idtheftcenter.org/idaftermath2004.pdf.

58. Jefferson, J. (2004). Police and identity theft victims-Preventing further victimisation. *Australasian Centre for Policing Research, No 7*. Retrieved May 27, 2007 from http://www.acpr.gov.au/publications2.asp?Report_ID=154.

59. Sharp, T., Shreve-Neiger, A., Fremouw, W. Kane, J., & Hutton, S. (2004). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Sciences, 49*(1), 131-136.

60. van der Meulen, N. (2006). *The challenge of countering identity theft: Recent developments in the United States, the United Kingdom, and the European Union*. Report Commissioned by the National Infrastructure Cyber Crime program (NICC). Retrieved May 20, 2007 from http://www.tilburguniversity.nl/intervict/publications/NicolevanderMeulen.pdf.

61. Baum, K. (2006, April). Identity theft, 2004: First estimates from the National Crime Victimisation Survey. *Bureau of Justice Statistics Bulletin*. Retrieved May 27, 2007 from www.ojp.gov/bjs/pub/pdf/it04.pdf.

62. Kreuter, E. A. (2003). The impact of identity theft through cyberspace. *Forensic Examiner, 12*(5-6), 30-35.

63. Klain, E. J., Davies, H. J., & Hicks, M. A. (2001). Child pornography: The criminal justice system response. Paper prepared by the American Bar Association Center on Children and the Law for the National Center for Missing & Exploited Children. Retrieved 12 April 2008 from http://www.missingkids.com/en_US/publications/NC81.pdf

64. Pierce, R. L. (1984). Child pornography: A hidden dimension of child abuse. *Child Abuse & Neglect, 8*, 483-493.

65. Itzin, C. (1997). Pornography and the organisation of intrafamilial and extrafamilial child sexual abuse: Developing a conceptual model. *Child Abuse Review, 6*, 94-106.

66. Krone, T. (2004). A typology of online child pornography offending. *Trends & Issues in Crime and Criminal Justice, No. 279*. Canberra: Australian Institute of Criminology.

67. Freeman-Longo, R. E. (2000). Children, teens, and sex on the internet. *Sexual Addiction & Compulsivity, 7*, 75 – 90.

68. Subrahmanyam, K., & Smahel, D. (2006). Connecting developmental constructions to the Internet: Identity presentation and sexual exploration in online teen chat rooms. *Developmental Psychology, 42*(3), 395-406.

69. Subrahmanyam, K., Greenfield, P. M., & Tynes, B. (2004). Constructing sexuality and identity in an online teen chat room. *Journal of Applied Developmental Psychology, 25*(6), 651-666.

70. Beran, T., & Li, Q. (2005). Cyber-harrassment: A study of a new method for an old behavior. *Journal of Educational Computing Research, 32*(3), 265-277.

71. Ybarra, M. (2004). Linkages between depressive symptomatology and Internet harassment among young regular Internet users. *Cyberpsychology & Behavior, 7*(2), 247-257.

72. Ybarra M. L., Diener-West, M., & Leaf, P. J. (2007). Examining the overlap in Internet harassment and school bullying: Implications for school intervention. *Journal of Adolescent Health, 41*, S42–S50.

73. Ybarra, M., & Mitchell, K. (2004a). Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry 45*(7), 1308–1316.

74. Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior, 23*, 1777-1791.

75. Bocij, P., & McFarlane, L. (2003b). Seven fallacies about cyberstalking. *Prison Service Journal, 149*, 37-42.

76. Spitzberg, B. H. (2006). Preliminary development of a model and measure of computer-mediated communication (CMC) competence. *Journal of Computer-Mediated Communication, 11*, 629-666.

77. Spence-Diehl, E. (2003). Stalking and technology: The double-edged sword. *Journal of Technology in Human Services, 22*(1), 5-18.

78. Pocar, P. (2004). New challenges for international rules against cyber-crime. *European Journal on Criminal Policy and Research, 10*, 27-37.

79. Blindell, J. (2006). Review of the legal status and rights of victims of identity theft in Australia. *Australasian Centre for Policing Research Report Series No 145.2*. Canberra: Commonwealth of Australia.

80. Cradduck, L., & McCullagh, A. (in press). Identifying the identity thief: Is it time for a (smart) Australia Card? *International Journal of Law and Information Technology*.

81. Senate Standing Committee on legal and Constitutional Affairs, Question No. 113. from http://www.aph.gov.au/senate/committee/legcom_cttee/estimates/sup_0607/agd/qon_113.pdf

82. Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research, 8*(2), 183-205.

83. RMIT Test Lab. (2006). *A study on server based Internet filters: Accuracy, broadband performance degradation and some effects on the user experience*. Report commissioned by NetAlert Limited. Retrieved June 7, 2007 from http://www.netalert.net.au/03100-A-Study-on-Server-Based-Internet-Filters---26-May-2006.pdf

84. Mitrakas, A. (2006). Information security and law in Europe: Risks checked? *Information and Communications Technology Law, 15*(1), 33-53.

85. Mitchell, K. J., Finkelhor, D., & Becker-Blease, K. A. (2007). Classification of adults with problematic Internet experiences: Linking Internet and conventional problems from a clinical perspective. *Cyberpsychology & Behavior, 10*, 381-392.

86. Wells, M., & Mitchell, K. J. (2007). Youth sexual exploitation on the Internet: DSM-IV diagnoses and gender differences in co-occurring mental health issues. *Child and Adolescent Social Work Journal, 24*, 235-260.

87. Mitchell, K. J., & Wells, M. (2007). Problematic Internet experiences: Primary or secondary presenting problems in persons seeking mental health care. *Social Science & Medicine, 65*, 1136-1141.

88. Dombrowski, S. C., LeMasney, J. W., Ahis, C. E., & Dickson, S. A. (2004). Protecting children from online sexual predators: Technological, psychoeducational, and legal considerations. *Professional Psychology: Research and Practice, 35*, 65–73.

89. Dombrowski, S. C., Gischlar, K. L., & Durst, T. (2007). Safeguarding young people from cyber pornography and cyber sexual predation: A major dilemma of the Internet. *Child Abuse Review, 16*, 153-170.

90. Thornburgh, D., & Lin, H. (2004). Youth, pornography and the Internet. *Issues in Science and Technology, 20*, 43-48.

TILES

TASMANIAN INSTITUTE OF LAW ENFORCEMENT STUDIES

TASMANIAN INSTITUTE OF LAW ENFORCEMENT STUDIES

Contact:

Associate Professor

Roberta Julian

Institute Director

University of Tasmania

Private Bag 22

Hobart Tasmania

Australia 7001

Telephone

+61 3 6226 2217

Facsimile

+61 3 6226 2864

Email

Roberta.Julian@utas.edu.au

tiles@utas.edu.au

Website

www.utas.edu.au/tiles

ISSN: 1832-701X