



## COVER SHEET

---

Broadhurst, R.G. (2005) International Cooperation in Cyber-crime Research. In *Proceedings 11th UN Congress on Crime Prevention and Criminal Justice, Workshop 6: 'Measures to Combat Computer Related Crime'*, pages pp. 1-12, Bangkok.

**Copyright 2005 (please consult author)**

Accessed from:

[https://eprints.qut.edu.au/secure/00004448/01/UNw\\_shop07revised.doc](https://eprints.qut.edu.au/secure/00004448/01/UNw_shop07revised.doc)

## **International Cooperation in Cyber-crime Research**

*R.G. Broadhurst, The University of Hong Kong*

11<sup>th</sup> UN Congress on Crime Prevention and Criminal Justice, Workshop 6: 'Measures to Combat Computer Related Crime', Bangkok, April 23-24, 2005

DRAFT 27.3.2005 21 PAGES AND 6,008 WORDS ALL INCLUSIVE.

### **Abstract**

*A wide range of research methods and comparative approaches need to be employed to provide basic data on the prevalence and severity of the various types of cyber –crime now confronted. In addition research on the effectiveness of new laws, policing strategies and prosecution via case review and attrition studies are crucial. Research must not be limited to police or court data and these sources often need to be more specific and uniform. Amongst the most pressing research questions is to learn more about victim and offender behaviour, as well as keeping track of legislative and enforcement developments across the globe. Mechanisms for the commissioning and sharing of research need to be developed that involve partnerships or networks between industry, government, academia and grass-root groups.*

### **Introduction**

In general three basic research objectives or phases can be identified in the legal response to cyber-crime over the 30 years since the birth of the Internet: exposé, criminalization and evaluation research. First, exposé research had an emphasis on revealing new modes of crime and new types of criminals (i.e. the 'hacker') via detailed case examples while the second phase focused on the best measures to combat cyber-crime by considering the forms of regulation (i.e. criminalization) or technologies best suited to control it. The most recent phase has been research on the effects of governmental and private sector interventions aimed at reducing the impact of cyber-crime by understanding both the scope of cyber-crime and the relative costs and benefits of different security responses.

Research on cyber-crime will increasingly focus on the problems of crime prevention in 'cyberspace'. Evaluative research will attach greater importance to evidence-based methods of research and will assay various groups, including cross-national populations of end-users, criminals, law enforcement and information security specialists and the numerous digital or other means employed by these actors.

The research and investigations that dramatized cyber-crime and contributed to the perception of an excessively lawless and dangerous medium of the Internet was a necessary phase in the response to national and international regulation of the criminal use of information communication technology (ICT). While there continues to be a role for investigative or 'exposé research'<sup>1</sup> the complexities and demands of e-commerce, public safety and privacy create the need for a systematic long-term research process that can inform the regulatory policy of governments at the national, regional and global level. An international approach to research on computer-related crime is necessary for an effective international law enforcement and crime prevention response.

The diversity of research on the 'information age' engages many disciplines and crucially, novel cross-disciplinary approaches. Such multi-disciplinary collaborations have been fostered within the academy and are successful when partnerships with police,

---

<sup>1</sup> An early example was the account of an espionage case involving a Californian research centre triggered by an accounting error observed by the computer system's manager (Stoll, 1991).

and the ICT industry occurs. Given the cross-border character of many crimes experienced on the Internet, mobile telephones and other networked environments, a strong comparative element will also be obligatory. As we learn more about the dynamic phenomena of cyber-crime, and especially the response of governments, industry and private actors, the dissemination of what is known will be a vital element in crime prevention.

### Global Context

The emergence of trans-national networks of Computer Emergency Response Teams (CERTs), G8 24/7 law enforcement contact points<sup>2</sup>, Internet Crime Reporting Centres, On-line Child Safety Networks<sup>3</sup> and other public/user interest groups (e.g. cyber-patrol, cyber angels) with a crime prevention mandate demonstrate that research and action iterate when communities perceive that they indeed 'share the same fate' regardless of how distant or different they may be. The pressing need for international cooperation also stimulates self-help<sup>4</sup>.

The risks of cyber-crime are not uniform and will reflect the diversity of criminal opportunity, the capacity of policing agencies (public and private) and the scope of the digital divide (in terms of e-commerce activity and extent technology uptake) both within and across nations. Risk of cyber-crime and the capacity to respond varies dramatically across nations but nearly half of Interpol's member countries lack the infrastructure for online communication (Noble 2003)<sup>5</sup>. Thus the cliché that the response to cyber-crime (as with trans-national crimes in general) can be no stronger than the 'weakest link' applies and compels the more able to assist the less able. A key research priority is therefore the continual *monitoring of legislative and enforcement capability* across nations given differential risks arising from the relative development of ICT. A number of multi-lateral organizations (e.g. Council of Europe [CoE], Asia Pacific Economic Forum, Organization of American States, European Union, Organisation for Economic and Cooperative Development) have already undertaken initiatives to monitor legislative developments but without co-ordination there is a risk of duplication. Macro-risk or global assessment protocols have not been developed although strategies for harmonising legal definitions and procedures have been suggested (Kaspersen 2004).

Because of the digital divide, only a small number of jurisdictions will have the capacity to provide for comprehensive research capabilities. In the advanced ICT countries that underwent a fundamental shift after the 'millennium bug' and the associated hubris, governments and relevant corporations have taken the initiative to support research; however, the focus has largely been on criminalization and intellectual property issues with child pornography catching most attention as a public safety problem.

---

<sup>2</sup> Co-ordinated by US Department of Justice Computer Crime and Intellectual Property Section, involving some 40 countries in mutual legal assistance: <http://www.cert.org>

<sup>3</sup> A number of US sites illustrate: CyberSpacers.org, Cyber-Hood-Watch.org, and StaySafeonline.info: an example is the animated program created by Microsoft and Boys and Girls of America to help children make safe use of the Internet, chat rooms and e-mail.

<sup>4</sup> For example, the Scientific Working Group on Digital Evidence (SWGDE) standardizes the exchange of computer forensics information among law enforcement agencies and guides the judicial system about the admissibility of digital evidence and the qualifications of experts.

<sup>5</sup> Interpol has stressed financial and high-technology along with drugs, terrorism, people smuggling and organised crime as it's top five priorities. Note mobile telephone technologies may reduce these disparities rapidly.

While Internet and ICT connectivity continues to grow exponentially, how ready are the key players in the academy, private sector and government to undertake a global program of research and dissemination? What should such a research program look like and how can it be done? This paper explores the likely research agenda through the prism of criminology (with its cross-disciplinary approach) rather than the systems engineering or information security perspective. Such a perspective sees cyber-crime as a social rather than as a technical problem and, although it recognizes that the criminal behaviour is said to be taking place in 'cyberspace' or 'virtual world', the actors involved and their intentions are not, as sometimes supposed, literally in another dimension. Thus any research agenda must begin by finding a common language to identify the research priorities. For example translating frequent references to "social engineering" (referring to the human element by technology experts) into meaningful questions about offender and victim interactions would be a good place to start.

### **Research networks and the cost of collective security**

The Interpol-payment card industry model could also be applied as a means for co-ordinating the many emerging networks interested in cyber-crime research. Generic problems of forgery and counterfeiting were the focus of Interpol's secure website for a Universal Classification System for Counterfeit Payment Cards, that provided up-to-date information on trends and techniques of forgery of payment cards and fraud. Apart from illustrating how Interpol's unique clearing house function can be adapted to meet new problems, the site serves as an example of how international agencies can assist with essential tasks, such as secure shared intelligence, and the potential role of private non-state actors in the prevention of crime.

An on-line research network, with several *nodes* of reference in government agencies, private industry, university research centres and self-help groups would enable an *international forum on cyber-crime research* to be developed. This may require a *virtual hub* located in an international agency (e.g. United Nations Office on Drugs and Crime, or regional agencies such as UNAFEI) or one of the university centres focusing on the social and technical problems of ICT<sup>6</sup>. An *on-line research forum* mediated and supported by the relevant international agencies could act as a clearing house about developments in cyber-crime, legislative innovations, the scope of relevant laws, capacities of law enforcement agencies, as well as disseminate research findings and act as an 'honest broker' of what constitutes best practice.

A research network would entail closer cooperation between the private IT security sector, academia and law enforcement than is usual and a degree of mutual suspicion and uncertainty about who pays and what form this cooperation should take is evident (Grabosky, Smith & Dempsey 2001). Increasingly costs rather than technology determine the kinds of security used but paradoxically the more successful the security investment, the less visible and less measurable the prevention results (Schneier 2003). Businesses often fail to account for the collateral costs of non-investment in security or consider

---

<sup>6</sup> The non-profit Computer Crime Research Center (CCRC) located in Zaporizhzhya, Ukraine is an example of cross-border initiative supported by public and private sponsors that seeks to improve co-operation on computer-related crime research, child pornography and cyber terrorism between CIS countries, Europe and the USA (see <http://www.crime-research.org/>, visited March 3, 2005).

crime prevention as an external cost<sup>7</sup>. Consequently incentives for doing the right thing (i.e. installing a patch) may be needed to minimize vulnerabilities. Although sharing information about cyber-threats (e.g. the FBI's InfraGard Information Sharing Analysis Centers) is essential collective security systems rely on exchanges about failures and sensitive problem areas and therefore must operate in a climate of trust. Important information is routinely hidden from those who need it most, and providers of IT security seldom pay the costs when they fail (see Loeb & Lucyshyn 2003). Thus a crucial issue will involve means to assess the real effectiveness of investments in cyber-crime prevention.

### **The legal response to cyber-crime**

A key research focus is on how to regulate behaviour in ICT environments such as the Internet and mobile phone networks. A decade ago the need to create new laws to address high-tech crimes was pressing. Many jurisdictions sought to use their existing criminal statutes to cope with unauthorized access, ID theft, malicious computer software and other offences, others introduced purpose built criminal laws or sought technologically neutral definitions to reduce ambiguities about devices and media that were rapidly evolving<sup>8</sup>. Consequently a degree of uncertainty surrounds the behaviour of interest and the best means to define these diverse crimes (Schjolberg 2004).

The CoE's *Cybercrime Convention*, which came into force in mid-2004 offered the prospect of a potential global treaty for the prosecution of cyber-crime. The convention provides a sound model of the definitions of cyber-crime and is a force for comity and harmonisation of law. It has been drawn on by many non-CoE nations in the framing of their own laws (e.g. Thailand). The many jurisdictions involved in the CoE convention quickly realized their mutual legal assistance arrangements [MLA] were inadequate to deal with the speed and diversity of crimes generated by greater connectivity and efforts in improving MLA are as vital as harmonised definitions of the offences. While the monitoring or mapping of legal changes (Kaspersen 2004) and jurisdiction (e.g. Brenner & Frederiksen 2002) across the globe are crucial research priorities because there are many challenges in achieving uniformity of terminology and practice such that cyber-crimes might be prosecuted by any competent tribunal anywhere as now happens with piracy.

#### *Diversity of cyber-crime*

A typology of computer-related crime comprises a) crimes in which computers are instrumental to the offence, such as child pornography and intellectual property theft; b) attacks on computer networks; and c) conventional criminal cases in which evidence exists in digital form. All of these different forms of cyber-crime raise different questions and specific kinds of research methods. Morris (2004) surveyed relevant experts and reported that online paedophiles, fraud and various forms of espionage (including corporate spying) were ranked the most serious cyber-crime threats. The ability of 'net-criminals' to use cryptography, steganography and anonymous re-mailers and the abuse of websites and email also ranked highly as significant threats. As with

---

<sup>7</sup> For example worms are relevant since they do no direct harm to the infected computer but use it to launch 'phishing' or similar programmes that in turn have real affects on other computers.

<sup>8</sup> Useful sites include 'FindLaw' see <http://cyber.lp.findlaw.com/criminal/>; and McConnell International see <http://www.mcconnellinternational.com/services/Updatedlaws.htm>.

conventional criminality it would be prudent to assess if online offenders are generalists rather than specialists.

Many public police agencies in ICT advanced nations have recognised the increased interdependence of global markets and have responded to the general risks of cyber crime especially to commerce and financial services. The response of the Hong Kong Police is typical and its mission broadly reflects the scope of public policing now required:

- maintaining a professional investigation capability and broadening the investigation; i.e. specialising and mainstreaming expertise;
- developing accredited computer forensics;
- proposing changes in laws and policies;
- prevention and education;
- intelligence management, and liaison with industry and professionals; and
- liaison with overseas law enforcement agencies and international MLA cooperation.

Each of these goals needs to be informed by adequately resourced research capable of informing the operational demands of the comprehensive role envisaged by public policing agencies. A highly useful function is formal risk assessment<sup>9</sup>. However, how best to promote public education about on-line crime prevention is equally important. Other issues that require both primary and policy research (often with a comparative context) are for example:

- the modus operandi of 'new' crimes exploiting new forms of ICT;
- the most efficient means to train law enforcement agents;
- the optimum periods to compel ISPs to store traffic or content data;
- the impact of 'virtual deterrence' in the on-line environment
- the characteristics of user responses to security emergencies, patch compliance and other attributes of effective crime prevention; how individuals and private industry can contribute to their own security; and
- the investigative protocols to apply in the proactive identification of unlawful conduct on the Internet.

### **Emerging prevention priorities**

Although there is consensus about the risks of computer-related crime, apart from criminalising the conduct at a global level, there is much less consensus about what might be done to prevent it. There is concern that the technological solution is a mirage despite improved software resistance to intrusion. Faith in a deterrence-based approach where the criminal law is deployed as the principal instrument of prevention may also be misguided since deterrence is likely to succeed only in some circumstances, and experience with conventional crime suggests that over-reliance on law as a deterrent or moral educator alone is unlikely to be enough despite community support. Research about the effectiveness of different sanctions and the attrition of cases from reporting to prosecution will be one means of gauging the role of conventional interventions. Most incidents of cyber-crime do not proceed to conviction and we know little about the eventual sentences imposed or

---

<sup>9</sup> The UK, National Hi-Tech Crime Unit for example produces an annual hi-tech criminal and technological threat assessment as a component of the National Criminal Intelligence Service's national assessment

the levels of disparity within and across nations<sup>10</sup>. Systematic studies of sentencing can help clarify the role of deterrence-based responses to cyber-crime<sup>11</sup> (Smith, Grabosky & Urbas 2004).

Recent developments in the general context of more data, places, customers and complexity suggest *likely priorities* for research as follows:

- Accounting for changes in the form (i.e. greater sophistication) and profit focus of criminal activity, especially fraud and deception-like offences (see Morris 2004).
- The scope, prevalence, severity, and duration of cyber-crimes among different populations and how best to identify high-risk populations (see below).
- Understanding the role of organised crime and, the overlap between traditional organized crime and new modes of crime facilitated by computers and Internet connectivity (see Council of Europe 2004, Brenner 2002).
- Increases in the virulence and sophistication of malicious code now required identifying the best mechanism for the co-ordination of rapid and secure information sharing about such threats among CERTs.
- The nature and efficiency of private sector investments in security as an aspect of ‘true’ external costs (Schneier 2003).
- The effectiveness and efficiency of civil law deterrents and the role of government requires the attention of policy research (Grabosky et al. 2001).
- Despite increased cross-national cooperation, systematic evaluation of the progress made in developing comprehensive forms of MLA has yet to occur. Action is necessary to map the ‘density’ of these relationships (including intelligence-sharing networks) and assay the effectiveness of MLA in closing the gaps in the international legal system. The monitoring of compliance is now a priority (Kaspersen 2004).
- Observing trends in public confidence in e-commerce over time in one country is important and could be conducted on a cross-national comparative basis. Comparing findings relating to public confidence with actual levels of e-commerce can also be useful (Grabosky & Broadhurst 2005).
- The parlous state of some law enforcement agencies and the consequent risk of cyber-crime safe havens required the attention of development economics and cross-cultural specialists.

Much of what we think will help in preventing cyber-crime is based on too little knowledge about offender and victim behaviour as it applies in the online environment. To guide research a number of theoretical approaches will need to be tested.

**‘There is nothing more practical than a good theory’<sup>12</sup>**

That criminal behaviour need not depend on social deviance is a fact that makes distinguishing good or bad behaviour from good or bad people one of the natural conundrums of policing. In the online ‘situation’ the theft of information and the

---

<sup>10</sup> We know very little from any country about what constitutes aggravating or mitigating circumstances in cyber-crime cases.

<sup>11</sup> The longest sentence yet by a US court was 108 months to Brian Salcedo in December 2004, for his role in a conspiracy to hack the nationwide computer system of a retail corporation. Previously Kevin Mitnick received the longest sentence of 68-months (see [www.cybercrime.gov/cccases.html](http://www.cybercrime.gov/cccases.html) visited March 6, 2005).

<sup>12</sup> The quote is attributed to Emmanuel Kant

manipulation of identity and trust are the key. Leading crime prevention scholars Newman and Clarke (2003) argue that crime follows *opportunity* when the presence of motivated offenders, and attractive and tempting targets in the absence of effective guardians combine in time and place. When this situation arises crime will occur providing the offenders also have appropriate resources (i.e. social and technical capital) to undertake the crime. A crucial factor is how trust is acquired and maintained when on-line merchants must be more intrusive about their (unseen) customers' identity and credit risk and the apparent ease in which trust is manipulated by fraudsters and others. Clarke and Newman also note the risks posed in the post-transaction phase (i.e. the delivery of goods or services ordered), a matter often overlooked. Efforts to reduce cyber-crime need to recognise these ingredients and the numerous pathways for crime. Therefore in the online environment crime prevention must be more integrated than the conventional environment..

Most measures designed to counter cyber-crime rely on either identifying potential offenders or shoring up 'guardianship'. Identifying the relationship between the offender's motivation (e.g. fraud, espionage, extortion or thrill seeker) and the kinds of target or victim (specifically targeted, the product of opportunity or merely an unfortunate victim of random offending behaviour) can provide the basis of offence profiles.

It is through a network of relationships that the resources necessary to complete a criminal transaction are mustered; coupled with the availability of targets and, the absence of capable guardians, this is what gives criminals their sustenance. In the context of cyber-crime we are only now beginning to understand the complexity of these networks (often operating in 'chat rooms' or closed or encrypted access sites) and new research methods based on sophisticated 'search engines', 'traffic analysis' and data mining techniques are required. These methods help visualise web communities and the key players in on-line illicit markets.

#### *Motivation of offenders: the 'hacker' myth?*

While the situational crime prevention model outlined above rests on the basic rationality of actors and the intrinsic role of deterrence other theories that include the role of deviant learning (i.e. differential association), social control or conditioning and the impact of labelling also require attention. Too much credence has been given to the 'hacker' as the relevant offender and 'techniques of neutralisation' are frequently paraded as 'hacker' motivations for criminality.<sup>13</sup> Yet motives will vary depending on the nature of the crime in question, and include greed, lust, revenge, challenge and adventure. Offenders have always been quick to adopt the benefits technology and tend to be generalists rather than specialists in choice of crime and computers are a means to illicit profits or pleasures.

Demetriou and Silke (2003) provide an example of how criminological research may help evaluate enforcement by reporting on a research project that monitored the illegal and

---

<sup>13</sup> An example offered by the editor of *2600: The Hacker Quarterly* defines the hacker as "...asking a lot of questions and refusing to stop asking. This is why computers are perfect for inquisitive people" and hackers are "...drawn to the sites and systems that are said to be impossible to access", but "...the ability to go anywhere, talk to anyone, and not reveal your personal information unless you choose to...attracts people to the hacker culture, which is slowly becoming the Internet culture": cited in CNN.com, April 19, 2004 visited November 10, 2004.

deviant activities (motivated hacker or not) that ensued when a website trap ('honey-pot') was developed. The research showed that 56% of 803 on-line users accessed illegal or pornographic sections of the website and as with 'real' sting operations<sup>14</sup> raise questions about user perceptions of detection risk, the severity of the offending and the ethics of the method used. It is perhaps easier to create problematic entrapment websites than to identify the actual victims of child pornography and hence gather evidence against the producers of such images.

### **Prevalence of cyber-crime**

Developing uniform and reliable measures of the nature, incidence, prevalence, duration and severity of crime is a major challenge in computer-related and Internet crime. Not only are the methods and medium novel but also a significant proportion of computer-crime *events* take place across *two or more jurisdictions*. Many policing agencies have only recently developed specific measures for recording cyber-crimes, but often these may not be differentiated from other commercial crime, fraud reports or criminal damage statistics. Thus the extent of computer-related crimes, even when reported, remains unclear. Official measures of crime incidence on the Internet will be more useful if they develop user-friendly reporting systems that fully utilize the new mediums. Digital technology affords new opportunities for individual citizens to communicate efficiently with police<sup>15</sup>.

Police statistics about reported crime often tell us more about the activities and priorities of police than they do about the extent of crime. This is because in many traditional crimes, victims do not report them and this is undoubtedly also the case for computer crime. Replicated random surveys of crime victims in many jurisdictions over the past 30 years have shown there are various reasons why victims do not report to police. These include, for example: the belief that police cannot (or will not) do anything; the offence was trivial or the victim felt the matter was better dealt with privately; reporting the case was too troublesome; or fear of reprisal or further trouble if they did report the incident (Alvazzi del Frate 1998).

#### *Cyber Crime Victim Surveys (CVS)*

Criminological interest in cyber-crime victimization has recently been recognized by the inclusion for the first time of questions about Internet crimes in the 2003 US National Institute of Justice household Crime Victim Survey (CVS). The scope is restricted to the *personal use* of computers (at home, school or work), or for operating a home business and also asks if any monetary loss occurred and if the matter was reported to police or other agencies. Over time CVS will yield valuable data about the cyber-crime experience of ordinary users and provide tracking data helpful in evaluating policy responses<sup>16</sup>.

---

<sup>14</sup> For example, 'Operation PIN' involved a website that purports to contain images of child abuse but anyone who entered the site and attempted to download images was confronted by an on-line law enforcement presence and informed that he has committed an offence, his details captured and passed to the relevant national authorities. The aim is to undermine "...the confidence of those who think that the Internet is an anonymous place where paedophiles and other criminals can operate without fear of being caught" (see <http://www.virtualglobaltaskforce.com>, visited March, 3 2005)

<sup>15</sup> An example is the US Internet Fraud Complaint Center, which receives on-line information from the public relating to questionable on-line activity. Personnel at the centre evaluate these communications and refer them to the appropriate agency or jurisdiction.

<sup>16</sup> A Chinese translation of these questions is to be implemented in the UN International CVS to be conducted in Hong Kong [HK] China in 2005.

Specifically the CVS asks “ Have you experienced any of include the following computer-related incidents in the last 6 months:

- Fraud in purchasing something over the Internet?
- Computer virus attack?
- Threats of harm or physical attack made while online or through E-mail?
- Un-requested lewd or obscene messages, communications, or images while online or through E-mail?
- Software copyright violation in connection with a home business?
- Something else that you consider a computer- related crime?

Another useful alternative model or strategy is the annual Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad (FBI) *Computer Crime and Security Survey*<sup>17</sup>, which focuses on ICT professionals<sup>18</sup>. Such an approach relies on an informed and knowledgeable group to assay how often crimes occurs, the costs and risks on the Internet<sup>19</sup>. As a tracking survey this method provides information about trends in cyber-crime as perceived by security specialists and goes some way in evaluating the impact of counter-measures. The latest survey (9<sup>th</sup>) shows a decline in cyber-crime and in particular intrusions.

#### *Surveys of vulnerable groups*

Also useful alternative or complimentary measures will be purpose-built surveys of victims. Such surveys must develop suitable means of involving respondents and overcome the complex ‘denominator problem’ or unknown dimensions of the Internet. Many of the methodologies that will need to be deployed, especially those that are implemented on-line will be untried. Generally the ‘metrics’ of the prevalence or extent of cyber-crimes among, for example, the estimated (in 2000) 18 million active but volatile domains and 1.4 billion publicly accessible pages are unreliable and few studies can be confidently generalised.<sup>20</sup>

A relatively well-researched area has been the risks to children of unsolicited sexual contacts, but the data is limited and as yet no trends that may help us evaluate the impact of interventions<sup>21</sup>. Although often of varying quality and using a variety of methods to obtain respondents, these surveys provide useful material for local responses to the risks for children. Typically such surveys focus on ‘exposé’. For example a 2001 US study found one in five 10–17-year-olds had received sexual contacts in the preceding year, and 4% received ‘aggressive’ solicitations (off-line contact sought)<sup>22</sup> while a 2004 Hong Kong survey of 1,175 high-school students (aged 12-15) on-line activities showed that 55% of them had made friends with strangers contacted on the Internet. Of these 39.5%

<sup>17</sup> Gordon, L.A., Martin P. Loeb, M.P., William, Lucyshyn, W. & R. Richardson (2005) Ninth Annual 2004 CSI/FBI Computer Crime and Security Survey, see GoCSI.Com.

<sup>18</sup> The 2004 survey is based on responses from 494 computer security practitioners in corporations, government agencies, financial institutions, medical institutions and universities.

<sup>19</sup> In 2003, the Computer Crime and Security Survey reported average losses per respondent of about \$800,000.

<sup>20</sup> E. O’Neil, B. Lavoie & R. Bennet, 2003, ‘Trends in the evolution of the public web’, cited in <www.caslon.com.au/metricsguide1.htm>.

<sup>21</sup> Commercial enterprises provide content filtering and these may offer further data on the nature of problems.

<sup>22</sup> The sample comprised 1501 teenagers who used the net regularly; see D. Finkelhor, K. Mitchell & J. Wolak, 2001, Risk factors for and impact of online sexual solicitation. *Journal of the American Medical Association*: cited at <www.caslon.com.au/securityguide11.htm>.

went on to meet their on-line contact, 12.3% subsequently dated and 6.9% had sexual contact. A significant proportion (11.6%) suffered financial loss after meeting their on-line acquaintance and 9% were sexually assaulted or harassed (Moy 2004). Recent research on cyber-stalking also broadens our perspective by including organizations (businesses, agencies etc.) as well as individuals and our understanding of the differences between 'off-line' and 'on-line' behaviour (Bocij 2004). Considerable more research needs to be undertaken to account for differences amongst victims and for the assumed role of anonymity on the Internet in such behaviours

Industry may also support research and the Internet Watch Federation (IWF) 2004 survey of ICT personnel's awareness about their duties as defined by the UK *Sexual Offences Act* (SOA) 2003 provides an example. The SOA was devised to provide ICT professionals with a legal defense for viewing and holding illegal child abuse images found on company networks for the purpose of evidence forwarded to the police. According to this on-line survey only 13% of ICT personnel knew about the law and 30% were not sure what constituted illegal content.<sup>23</sup> In addition the regular loss estimates reported by intellectual property businesses and periodic client or industry surveys by large accounting firms to determine the incidence and prevalence of computer-related crime are also available. If these survey methods are clearly specified they could, along with official and CVS statistics, contribute as one of several components of an evidence-based surveillance system.

### **Developing evidence based research**

Research on cyber-crime is in its infancy and providing an international evidence base for future policy development is a challenging task. Knowledgeable individuals and institutions may for commercial, political or national security reasons be disinclined to share their wisdom with researchers. Information that enters the public record often may actually be misinformation or disinformation. The creation of a *cyber-crime research network* supported by international and regional agencies in partnership with industry and academia will play a vital role in improving the quality of information and reducing overload.

Given the cross-national nature of cyber-crime, country case studies, focusing on individual incidents and more general developments, can help raise public awareness of policy imperatives. It would also be instructive to analyse known cases of cross-border offending. Were 24/7 arrangements in place, and did they function as intended? Were the laws of the country from which the offending originated adequate to deal with the matter? Was there agreement or disagreement on the part of the authorities about whether domestic prosecution was preferable to extradition? Other issues call out for comparative study: for example the ways in which different national law enforcement agencies cope with evidence of possible criminal activity that may be encrypted. When evidence exists in a form that is not accessible to investigators, what do they do? Do they seek to mobilise decryption technology to 'break' the code (less effective given the widespread availability of strong encryption technology)? Do they issue, subject to judicial oversight, 'decryption orders' requiring assistance in rendering the evidence intelligible, with

---

<sup>23</sup> IWF (see <http://www.iwf.org.uk>) an Internet 'Hotline' also noted that although 90% of respondents thought their organization had an acceptable Internet use policy, 27% did not monitor staff use or report such matters to police (70% claimed they would dismiss staff involved) and 35% had no policies for dealing with such images.

penalties for non-compliance? Do they use high-technology means of identifying encryption keys, such as keystroke logging devices or the technologies of remote search?

Similarly, case studies of individual investigations, successful or otherwise, can also be instructive. Success stories can help build confidence among new investigators, or among public officials. ‘Recipes’ for success may also be useful for training purposes. Studies of unsuccessful investigations are no less important. Despite the fact that individuals or agencies do not like to dwell on failure, it is important to understand what went wrong, in order to reduce the likelihood of subsequent similar mishap. Just as hospital staff meet in regular mortality and morbidity conferences, and aviation safety specialists analyse the circumstances of aircraft accidents, so too should cyber-crime specialists reflect systematically on cases that ‘go wrong’ (Broadhurst & Grabosky 2005).

Countries differ in terms of their policy priorities. It would be useful to develop an overview of priorities in the different regions and to observe how priorities change, both within individual countries and in multilateral forums. What are individual countries concerned about and what sorts of trade-offs between security levels that decrease e-commerce and levels of crime are they prepared to accept? What kinds of cyber-crime take precedence: hacking, fraud, or theft of intellectual property? Are governments more concerned about infrastructure protection or child pornography? What explains the elevation or decline of an issue on the public agenda: lobbying by the affected industries or a real increase in the underlying behaviour, or international pressure?

Government has driven much of the response to cyber-crime but the private sector plays a crucial role in the prevention of crime in the digital age and can also contribute to research. Apart from the need for coordinated research three issues remain essential: the creation of a viable international law enforcement mechanism; the role of trans-national criminal networks; and making private and public partnerships genuinely collaborative.

## References

- Alvazzi del Frate, A. 1998, ‘Preventing crime: Citizen’s experience across the world, Issues and Reports, No. 9., UNICRI: Rome.
- Bocij, P., 2004, *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, Westport: Praeger.
- Brenner, S.W. 2002, ‘Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships’, 4 *N.C. J.L. & Tech.* 1
- Brenner, S.W. & B.A. Frederiksen, 2002, ‘Computer Searches and Seizures: Some Unresolved Issues’, 8 *Michigan Telecommunications & Technology Law Review* 39.
- Council of Europe 2004, ‘Summary of the Organised Crime Situation Report: Focus on Cybercrime’, Octopus Interface conference: Challenge of Cybercrime, September 15-17, Strasbourg
- Demetriou, C. & A. Silke, 2003, ‘A Criminological Internet ‘Sting’: Experimental Evidence of Illegal and Deviant Visits to a Website Trap’, *British Journal of Criminology*, 43:213-222.
- Kaspersen, H. 2004, ‘Convention on Cybercrime – current state of implementation’, Council of Europe Octopus Interface Conference: Challenge of Cybercrime, September 15-17, Strasbourg.
- Grabosky P., & R.G. Broadhurst 2005, ‘The Future of Cyber-crime in Asia’, in Broadhurst, R.G & P. Grabosky [Eds.], *Cybercrime: The Challenge in Asia*, The University of Hong Kong Press, pp. 347-360.

- Grabosky, P., Smith, R.G. & G. Dempsey 2001, *Electronic Theft: Unlawful Theft in Cyberspace*, Cambridge University Press: Melbourne.
- Loeb, G. & W. Lucyshyn's, 2003, 'Sharing Information on Computer Systems Security: An Economic Analysis', *Journal of Accounting and Public Policy*, 22 (6).
- Morris, S., 2004, 'The future of netcrime now: Part 1 – threats and challenges', Home Office [UK] Online Report 62/04.
- Moy, P., 2004, Teens admit outings, sex with net strangers. *SCMP*, October 4, 2004: C3.
- Newman, G. & R. Clarke, 2003, *Superhighway Robbery: Preventing E-commerce Crime*. Willan Publishing, Devon.
- Noble, R. 2003, 'Interpol's New Approach: A Return to Basics', in R. Broadhurst (Ed.) *Bridging the GAP: A Global alliance on Transnational Organised Crime*, Hong Kong Police: Printing Department HKSAR.
- Schneier, B., 2003, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, NY: Copernicus Books.
- Schjolberg, S. 2004, 'Computer-related offences', Council of Europe Octopus Interface conference: Challenge of Cybercrime, September 15-17, Strasbourg.
- Smith, R.G., Grabosky, P. & G. Urbas 2004, *Cyber Criminals on Trial*, Cambridge University Press: Melbourne
- Stoll, C. 1991, *The Cuckoo's Egg*, Pan Books: London