Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

HIGH TECH CRIME BRIEF

2005

01

Concepts and terms

New crimes and old crimes committed in new ways

The rapidly expanding capabilities of information and communications technologies (ICT) have created new crimes and new ways to commit old crimes. Criminal threats include: computer intrusions, distributed denial of service attacks, malware (the insertion of malicious software code into a computer), stealing ICT services, online child pornography and the misuse of email. This brief examines some of the terminology and sets out a definitional framework for measuring and analysing high tech crime.

Individual terms

The language is being extended to describe each new form of illegal or suspect activity. Just a few topical examples are given here:

- phreaking – manipulating a telecommunications billing system to obtain telephone services for free;
- hacking – breaking into a computer system to build information, to demonstrate security faults or for other malicious purposes;
- smurfing – using a program known as smurf to use internet protocol (IP) and internet control message protocol (ICMP) to ping or send a request using a packet internet gopher to an internet host to test its response;
- phishing – replicating an existing web site to entice users into entering confidential information in the belief that they are dealing with a legitimate site;
- account harvesting – collecting email accounts from information in the public domain or by using spybots to search for email addresses stored locally on a computer – this is one of the foundations for spamming; and
- spamming – sending bulk unsolicited email; regulated in Australia under the *Spam Act* 2003 (Cwlth).

For more information, a number of cyber dictionaries are available online such as http://foldoc.doc.ic.ac.uk/foldoc/index.html and http://www.netlingo.com/.

Computer crime

A number of terms are sometimes used interchangeably to describe crimes committed using computers.

- computer-related crime – the use of a computer is integral to committing the offence; examples are offences such as computer-related forgery (where false data are put forward as authentic) and computer-related fraud (the fraudulent interference with or manipulation of data to cause property loss);
- computer crime – this is a general label for offences in which a computer is the object of the offence or the tool for its commission;
- internet crime – refers to crimes in which the use of the internet is a key feature and includes content-related offences such as possession of child pornography, or in some countries, the dissemination of hate or racist material; and
- e-crime – a general label for offences committed using an electronic data storage or communications device.

Cybercrime

Statute and treaty law both refer to cybercrime. In Australia, cybercrime has a narrow statutory meaning as used in the *Cybercrime Act* 2001 (Cwlth), which details offences against computer data and systems. However, a broad meaning is given to cybercrime at an international level. In the Council of Europe's *Convention on Cybercrime* (EST no. 185), cybercrime is used as an umbrella term to refer to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences and copyright offences. This wide definition of cybercrime overlaps in part with general offence categories that need not be ICT-dependent, such as white-collar crime and economic crime as described by Grabosky and Sutton (1989).

High tech crime

High tech crime is a common label used by both the Australian High Tech Crime Centre and by the National High Tech Crime Unit in the United Kingdom. These agencies deal with crimes that rely on the use of ICT, or which target ICT equipment, data and services. Their focus is on the complex networking capacity of ICT, which creates a previously unimaginable platform for committing and investigating criminal activity.

'High tech' emphasises the role of ICT in the commission of the offence. Different practical considerations arise according to whether ICT equipment, services or data are the object of the offence, or whether ICT is the tool for the commission of a 'material component of the offence'. The distinction between the use of ICT as either the object or as a tool of offending was drawn by Carter (1995) and has been adopted by Statistics Canada (2003). While it is recognised that criminal activity does not always conform to neat categories, this two-part division of high tech crime is put forward for the analysis of such crime in Australia.

In contrast, while the criminal use of genetically modified organisms may be thought of as relying on advanced technology, it does not involve ICT and would not be considered a high tech crime.

Similarly, while a modern motor vehicle may incorporate sophisticated digital technology, misuse of a motor vehicle of itself, would not be considered a high tech crime.

ICT as the object of offending

In this category are offences that specifically relate to a computer as the object of offending. The following offence types are included:

- illegal access
- illegal interception
- data interference
- system interference
- misuse of devices

Offences of this kind are contained in the *Cybercrime Act 2001* (Cwlth). Within the European *Convention on Cybercrime* (EST no. 185), relevant offences are those 'against the confidentiality, integrity and availability of computer data and systems'.

Some of these activities are similar to traditional offences involving physical objects, such as theft, malicious damage or trespass. These new crimes specifically cover the intangible nature of data and services on a computer. Possible motives of perpetrators are: economic gain, vandalism, extortion, revenge attacks, economic sabotage and mischief.

ICT assets (including both software and hardware) may also be subject to traditional offences of theft or malicious damage. Other targets for dishonesty offences are telephonic or data transfer services, which may be stolen or fraudulently misappropriated. For statistical purposes, it is possible for police to record instances where an ICT asset is the target of a traditional offence as a sub-category of that offence.

ICT as a tool for offending

As indicated, offences are included in this category if ICT is the tool for the commission of a material component of the offence. A subjective judgment has to be made whether there has been sufficient involvement of ICT to warrant recording it as such. Examples include manipulating data to obtain a fraudulent payment, or using digital technology to commit forgery, or to steal intellectual property. Other relevant offences are the collection and dissemination of illicit online content, such as child pornography and the use of ICT to commit cyber-stalking.

For the purposes of analysing high tech crime, this category does not include offences where the use of ICT is incidental to the commission of the offence. It is recognised, however, that many offences may be supported by a low level of reliance on ICT, for example by recording payments for drugs (Smith et al. 2004). While law enforcement officials need to be mindful of the adaptation of ICT to a wide range of criminal purposes, it is not practical to consistently measure the minor use of ICT. The alternative approach, to record whether ICT was used at all in the commission of an offence, would lack sufficient definition to be meaningful.

Implications for data collection and analysis

In collecting high tech crime data it is necessary to take into account problems of under-reporting of offences and possible over-reporting where there are multiple regulatory agencies, and many potential victims for the same offending behaviour. The under-reporting of high tech crimes is thought to be a serious problem. A computer crime survey of Australian organisations in 2004 indicated that just 30 per cent of respondents reported security incidents to law enforcement authorities. The main reason given for not reporting was a belief that the organisation was not specifically targeted (AusCERT et al. 2004).

The issue of over-counting must be considered if reported crime figures are aggregated from more than one agency or jurisdiction, as the one incident of offending may be recorded by each agency or jurisdiction.

In relation to an offence that occurs across jurisdictions, it may be caught under the law of more than one place, for example, where the affected computer is, where the offender who launched the attack is, or where a computer used to launch the attack is. A prosecution brought where the offender is does not require extradition but may face evidential problems of proving what happened in another jurisdiction. A prosecution brought where the victim is, may require extradition of the offender but may be proved in accordance with local laws of evidence. Competing issues such as these will affect the choice of jurisdiction if a matter is to be prosecuted.

The problem of data capture occurs with many other crimes where information on the method of committing the offence is needed in addition to simply knowing how many offences of a given type have been recorded. Given the ubiquity of ICT, there are difficulties in quantifying the full extent of high tech crime in a meaningful way. Considering ICT as either the object or tool of offending provides a consistent framework for analysis. Understanding the nature and impact of high tech crime also requires the application of qualitative analytical approaches to explore how crimes are committed in addition to quantitative measures that count the number of offences recorded.

Contact
Australian Institute of Criminology
GPO Box 2944 Canberra ACT 2601
Phone: 02 6260 9200 Fax: 02 6260 9201
Web: www.aic.gov.au

Project no. 0074 ISSN 1832-3413

The Australian High Tech Crime Centre
funded this research.

Further reading

AusCERT, NSW Police & Deloitte Touche Tohmatsu 2004. *2004 Australian computer crime and security survey* Sydney: AusCERT

Carter D 1995. Computer crime categories: how techno-criminals operate. *FBI law enforcement bulletin* 64 (7): 21

Davis R & Hutchinson S 1997. *Computer crime in Canada.* Toronto: Thomson Canada Limited

Grabosky P & Sutton A 1989. *Stains on a white collar* Sydney: Federation Press

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

Statistics Canada 2002. *Cyber-crime: issues, data sources and feasibility of collecting police-reported statistics.* Ottawa: Canadian Centre for Justice Statistics

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government, the AIC or the AHTCC