Internet anonymity practices in computer crime

H.L. Armstrong
School of Information Systems, Curtin University of Technology, Perth, Australia
P.J. Forde
Curtin Business School, Curtin University of Technology, Perth, Australia

Keywords
Computer crime, Criminals, Internet, Law enforcement

Abstract
Money laundering, drug dealing, terrorism, hacking, fraud, child pornography and the distribution of objectionable material are crimes that are perpetrated using the Internet. Criminals utilise software tools and valuable knowledge from the Internet as well as embracing the Internet's global communications system to participate in virtual communities of disguised people. The Internet provides the facilities for people with criminal intent to associate and exchange intelligence with reduced risk to their personal identification. Using the example of paedophile and hacker Internet practice, this paper proposes an association between criminal Internet activity and Internet anonymity. It discusses the propensity to use anonymity techniques when perpetrating cyber crime. Consequently, a new balance between privacy, freedom of speech and law enforcement must be determined.

Emerald

Information Management & Computer Security
11/5 [2003] 209-215

[ISSN 0968-5227]
[DOI 10.1108/09685220310500117]

Introduction

The Swedish National Criminal Investigation Department stated that "as the number of Internet users increases, so does the criminal usage of the Internet", indeed there were "clear indications that the Internet and other IT structures are to an increasing extent being used in criminal contexts" (SNCID, 1998). The FBI recently declared that cyber crime (crimes perpetrated with the assistance of Internet services):

> ... represented the most fundamental challenge for law enforcement in the 21st Century. By its very nature, the cyber environment is borderless, affords easy anonymity and methods of concealment and provides new tools to engage in criminal activity (Vatis, 2000).

The Chief Constable of Fife Constabulary (in Scotland) commented on the difficulties investigators face as they tackle criminal exploitation of the Internet. He pointed out that (Hamilton, 2000):

- continents may separate crimes with offenders and victims at different locations;
- offences could be measured in seconds yet they occur in different time zones;
- political (national) boundaries were usually ignored;
- new crimes were emerging (i.e. on-line harassment, cyber stalking and hacking); and
- encryption techniques enabled offenders to securely communicate worldwide.

In May 2001, the United Nations Commission on Crime Prevention and Criminal Justice discussed international cooperation to combat transnational crime. The use of technologies that supported criminal activities were described:

> Dedicated security products such as firewalls and encryption software shield criminal communications from interception or intrusion just as effectively as they protect legitimate communications (CCP, 2001).

The commission recognised that Internet technologies were enabling new forms of criminal organisation and cited paedophile offenders (with their ability to locate another and exchange materials anonymously) as an example of a new form of cooperation not covered by existing definitions of organised crime:

> Sophisticated criminals can readily use the easy anonymity that the Internet provides to hide their crimes (Holder, 2001).

For example, in an effort to hinder a police investigation of drug organisations in Holland, criminals from an information warfare division established to support organised crime collected information via eavesdropping and decrypting communications of attorneys, police officers and government officials. By analysing the data collected, the criminals were able to determine which law enforcement and justice units were collaborating on the investigation (Denning, 1999). The information warfare division was reported to work in loosely-coupled cell structures that were illusive and difficult to capture – a common trait of organised criminal groups.

This paper aims to raise the awareness of criminal uses of the Internet. By focussing upon the Internet facilities and practices used by both the paedophile and hacker communities, it is obvious to see how organised crime groups can use global communications facilities to aid anonymity in their activities. The paper concludes with a realisation that individual rights to privacy may have to be subdued in an effort to reduce

Information Management & Computer Security
11/5 [2003] 209-215

cyber crime and use of the Internet for criminal activities.

Individual right to privacy

An individual's right to privacy provides an ongoing obstruction to law enforcement. The FBI stipulated that "respect for privacy was a fundamental guidepost in all of our activities" and that FBI conduct was:

> . . .strictly limited by the Fourth Amendment, statues such as Title III and ECPA, and the Attorney General Guidelines (Vatis, 2000).

In November 2001, the preamble to the European Convention on Cybercrime alerted members states to the impact that efforts to control cyber crime can have on individual rights and called for an awareness to:

> . . . ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human rights and Fundamentals, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the rights of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy (COE, 2001).

Even though criminal utilisation of the Internet is widely recognised the implications of anonymous Internet practices have not received similar attention.

Paedophile internet community

Activists argue for a paedophile's right to free speech (Jay_h, 1997). They argue for a lifestyle that contradicts fundamental cultural practices and violates specific laws. Paedophiles maintain that free speech is not available to them and anonymity is necessary to avoid persecution (Spike, 1997). Most Western societies have considered paedophilia and have concluded that it is not an acceptable lifestyle, many viewing the practice with alarm. The Council of Europe Convention on Cybercrime, which promotes human rights and democracy in Article 9 criminalizes images that appear to represent children engaged in sexual conduct, and this includes virtual child pornography on the Internet (Marcella and Greenfield, 2002).

Reducing opportunities for paedophiles to communicate and organise their own community has been the major incentive behind a number of national investigations. For example, the 1995 Australian report on Organised Criminal Paedophile Activity reported that there was little evidence of organised paedophile groups and included the following findings (PJC and NCA, 1995):

- while very small paedophile-support groups operated openly in Australia in the 1980s there is no evidence they currently do so;
- there is no evidence to suggest that organised paedophile groups have ever resembled what are traditionally thought of as organised crime groups in size, aims, structures, methods, longevity and so forth (to the extent that two or more paedophiles groups together to commit offences, the numbers involved have almost invariably been very small and the groupings very much *ad hoc* and on a peer-to-peer basis); and
- more commonly, where there are contacts between paedophile offenders, they consist of loose informal networks of peer-to-peer contacts.

However, a study that observed the Internet activities of paedophiles suggested that these findings were no longer accurate (Forde and Patterson, 1998). In contrast to the 1995 findings paedophiles were shown to be developing their own community and that the Internet was providing the forum for organised informal networks and peer-to-peer contacts on a global scale. The study concluded that paedophiles used the Internet to create communications structures, distribute objectionable materials and to archive their collections. A paedophile Internet community was observed that mentored its members with instruction on anonymity. In particular, it was noted that (Forde and Patterson, 1998):

- *Paedophiles were very concerned to conceal their identity*. This was not unexpected given society's attitude to paedophilia. Many Internet links described anonymity and privacy techniques. Authors of e-mail sent their messages to newsgroups anonymously. WWW pages displayed disguised e-mail addresses while newsgroup discussions exchanged information about "safe" locations and masking techniques. IRC chat sessions were conducted on private channels using direct one-to-one secure communication.
- *Paedophiles needed to demonstrate their prowess to their peers*. WWW pages were used to make coming-out presentations (although most presenters hid behind masked identities). These pages appeared to provide peer group status. They also acted as a vehicle for soliciting communications from other paedophiles.

Information Management & Computer Security
11/5 [2003] 209-215

> Background profiles and descriptions of individual interests were often detailed on the presentation pages together with samples of images from private collections. The need to demonstrate the extensiveness of individual picture collections was vividly manifested within certain newsgroups. Sending pictures to newsgroups obviously enabled picture distribution however they were distributions to no one in particular. Newsgroup postings appeared to be most concerned with advertising the extent of personal collections.

Casey (2000) also discusses the use of Internet facilities by the paedophile community to support their activities, giving detailed examples of cases. He states that paedophiles utilise Internet facilities (Newsgroups and IRC in particular), to enhance their current *modus operandi* in order to achieve their desired ends.

It is of interest that many of the characteristics presented in the Forde and Pattison study have also been noticed within the hacking fraternity.

Hacker Internet community

The tools and techniques utilised by the hacking community have been widely discussed in both printed and electronic forums. Software tools for hacking all types of computer and communications systems are readily available on the Internet and most can be downloaded at no, or little, cost. Our concern in this discussion is not with the tools *per se*, but with the elements of the hacking community that are similar to those used in other organised crime groups (i.e. paedophiles).

The hacker community is using the Internet to communicate and attack systems on a global scale (Boni and Kovacich, 2000). The Computer Security Institute report 90 per cent of respondents detected computer security breaches in the past 12 months and independent hackers are reported to form the likely source of attack in 80 per cent of cases (CSI/FBI, 2002). Lack of security on the Internet and its protocols aids the hacker's quest by providing vulnerabilities and unrestricted access. By its nature (i.e. sheer size and open connectivity) the Internet provides a facility to encompass the hacker community and its sub-culture. The Internet is an open, interconnected communications infrastructure that is unregulated and largely unpoliced, and also unpoliceable (Ford and Baum, 2001).

> Hackers comprise an:
> ... interesting subculture, technically astute and talented even if socially and morally depraved (Nichols *et al.*, 2000).

The hacker's philosophy is well documented – information should be free and access to computers and information should be unlimited. They work in groups, some groups being limited to only the elite of their trade, others willing to take on inexperienced members and train them. Many hackers will mentor other hackers, particularly those who show promise, enthusiasm, or who have similar values. Hackers share and barter their tools and information including methods of avoiding detection. Many tutoring sites have been established on the Web and hackers, other criminals and security specialists use these sites.

Hackers are motivated by a variety of factors, including the thrill and excitement of doing something illegal, challenge, pleasure, knowledge, recognition, power and friendship (Chantler, 1995; Denning, 1999). Other reasons noted by Chantler (1995) in his study of the hacker culture included self-gratification, addiction, espionage, theft, profit, vengeance, sabotage and freedom. Many hackers admit they are addicted to the thrill of doing something prohibited; they enjoy the associated "high" and rush of adrenaline.

Hackers use Internet facilities extensively, including Web sites, e-mail, chat rooms, FTP sites, Usenet newsgroups and discussion boards. Hacker software tools are stored on private and public Web sites and protected systems. Hacker Web sites are highly secured and access is given only to those who are trusted. Like other organised criminal groups hackers secure their communications using sophisticated encryption tools.

Hackers retain their anonymity by using handles (pseudo names), remailers, anonymous servers, e-mail and IP spoofing (changing their IP address so that transmissions appear to come from another source). Hackers like to advertise their exploits but at the same time remain anonymous. Stephenson (2000) claims that vanity is a hacker trait. Hackers cannot keep quiet about their exploits and bragging rights are one of their chief motivations for cracking systems. The majority of hackers are loners who share their information in public and semi-public forums, however their desire to be recognised for their wares and expertise results in many leaving a mark of their trade on hacked sites and embedded in some tools. Many hackers can be identified by techniques and patterns unique to their work.

Information Management & Computer Security
11/5 [2003] 209-215

Whilst many hackers claim their intentions are noble, their actions remain criminal. The hacker community provides a training ground for those who wish to master computer networks and the Internet whilst remaining undetected and anonymous. Where else would organised crime go to train their operatives?

Internet anonymity practice

The intent to hack automatically classifies hacking as a crime, this decision being based upon the concept of *mens rea*:

> *Mens rea* is a Latin term that refers to the guilty mind. It is used to describe that mental conditional in which criminal intent exists. ... If the suspect unwittingly penetrated a computer system ... there is no *mens rea* and therefore no crime. However, if the suspect was well aware that a security breach was underway and he knowingly employed sophisticated methods of implementing that breach – *mens rea* exists and a crime has been committed (Sams.net, 1997, pp. 30-1).

Hackers are viewed as criminals in most countries, however they claim their values and morals differ from other criminal groups (i.e. paedophiles). In fact, some hackers claim they trace the identity of paedophiles, attack their computers, and remove the images paedophiles post on the Internet (Denning, 1999). The hacking community is decades old and a high standard of technical expertise is normally a pre-requisite to membership (particularly of elite groups). They utilise covert channels and steganography to hide data in transmission (Skoudis, 2002) and their skills in sharing information and tools anonymously are honed and proficient. It is not unreasonable to project that hackers will sell information and expertise to organised crime and/or terrorist groups. The hacker community may be sheltering and training perpetrators to occupy the shadows of cyberspace in organised crime groups.

Paedophiles sought acceptance amongst their peers but they trusted the protection of Internet anonymity. While they do not have the technical expertise of the hacker community, paedophiles are obviously skilled in the use of encryption and remailers as well as the practice of Internet anonymity. Individual notoriety and personal anonymity are characteristics that have been observed in both communities and it is reasonable to expect that other criminal communities would also desire these outcomes. There appears to be an association between particular Internet activities and user identification. Internet practices that provide the strongest anonymity were used to camouflage extreme criminal behaviour (Forde and Patterson, 1998). Therefore, a model of Internet anonymity practice can be proposed that illustrates the relationship between Internet activity and user identification. To assist the derivation of this model it is useful to think of individuals initiating activities as "instigators" and individuals that participate as "readers".

The model presented in Table I supports the proposition that an association exists between the intent of criminal Internet activity and Internet anonymity. When the intended activity is considered benign then low strength anonymity will be acceptable. However, when criminal activities are to be perpetrated then the use of strong anonymity techniques are to be expected.

Web pages offer weak anonymity for their owners. While it may be possible to disguise identity when obtaining ISP facilities, maintaining pages provides ISPs with an opportunity to trace owners. Paedophiles take care not to display "offensive" pictures on Web pages. Pornographic materials are most abundant in "sex-stories" libraries and newsgroups. Materials are distributed and delivered via anonymous e-mail and extensive use of Remailer services as these offered the delivery of potentially untraceable e-mail messages. Where little risk of identity was perceived paedophiles were happy to publish explicit pornographic material on the Internet.

While encryption techniques are readily available, an awareness of the penalties associated with transactional security has to be taken into account by perpetrators. For example, securing a SSL (secure socket layer) requires a hand-shaking process that identifies the parties at each end of the connection. This facility makes it difficult for external parties to read the communication, however it requires communicators to declare their virtual identities. Therefore, even though perpetrators can create "secure" networks they must address the issue of member identification and the attendant risk of membership exposure. Consequently, virtual private networks (VPNs) are a dual edged sword. Their technological construction provides excellent protection against external attack; nevertheless members could be compromised by an individual member's inappropriate action. As a result, if very high levels of trust exist between group members then they can be expected to use VPNs. Otherwise they can be expected to use Internet services offering (or allowing) anonymity.

The increased use of encryption by criminal elements to protect

communications and other materials on the Internet hinders the activities of law enforcement to combat crime. As encrypted electronic files become more difficult to decrypt due to the increasing sophistication of the tools, the rate of non-recoverable encryption escalates and less criminal activity will be detected. In addition, as the use and strength of encryption increases and encryption tools become a standard component of software suites, the threat to public safety will increase proportionately (Marcella and Greenfield, 2002).

A recent inspection of paedophile Internet communications confirmed the continuing adoption of anonymous practices and the distribution of knowledge about those practices. Apart from a well-known portal that provides a vast array of "benign" information to paedophiles, one current technique of distributing "offensive" information uses a combination of discussion boards (e-Boards) and virtual groups (e-Groups). These boards and groups are the Internet's replacement of the old bulletin board systems (BBS). Usually e-Boards do not have passwords and are open to anyone using the Internet. As the Internet service provider (ISP) hosting e-Boards or the owner of an e-Board could log transactions, visitors usually mask their IP numbers using proxies. Anonymous remailers are often used to post messages to these boards. Apart from benign (possibly coded) discussion, messages distribute links to e-Groups that archive offensive material. Even though e-Board users try not to attract outside attention, these boards have a short life expectancy as ISPs attempt to eradicate abuse of their services. Therefore, many messages point to replacement e-Boards. e-Groups provide more services than e-Boards (i.e. picture galleries, bookmarks, chat and message boards) and they have membership structures that require identification information. Requiring membership of

Table I
Internet anonymity practices

	Instigator			Reader		
Internet service	**Intention**	**Technique**	**Identification**	**Intention**	**Technique**	**Identification**
World Wide Web	Low-level information distribution Advertise contact details	Use proxies to mask ownership Use international ISPs Plan to re-locate regularly	Weak anonymity Relies on ISPs not to analyse logs or make them available to authorities	Locate information and contacts	Use anonymous proxies to hide identity	Weak anonymity Relies on ISPs not to analyse logs or make them available to authorities
E-mail	Confidential communications Material distribution	Encrypted e-mail Free e-mail a/c obtained using false ID Post using anonymous remailers	Very strong anonymity Difficult to trace	Confidential communications Material distribution	Encrypted e-mail Free email a/c obtained using false ID Reply using anonymous remailers	Very strong anonymity Difficult to trace
File Transfer Program	Public and private distribution of electronic files	Run and set-up own FTP server	Medium anonymity Relies on regular change to avoid ISP attention	Risky download of files	Anonymous access	Weak anonymity Relies on FTP owner's tolerance
News groups	Broadcasting illegal or objectionable messages	Anonymous e-mail posting	Very strong anonymity Difficult to trace	Downloading illegal or objectionable messages	Proxy masked www to news Use open news servers Regularly change to avoid attention of news server administrators	Medium anonymity Depends on tolerance of new server administrator
Internet Relay Chat	Private real-time chat Exchanging electronic files	False identity Private channels Personal contacts	Strong anonymity Relies on regular identity changes Skipping across channels to avoid the attention of moderators	Private real-time chat Exchanging electronic files	False identity Private channels Personal contacts	Strong anonymity Relies on regular identity changes Skipping across channels to avoid the attention of moderators

Information Management & Computer Security
11/5 [2003] 209-215

hacker and paedophile e-Groups means that outsiders are less likely to visit these groups. However, in order to attract Internet users to their Web sites, ISPs make it easy for new members to join. Easy membership enables paedophiles and hackers to utilise virtual identities and anonymous e-mail addresses when creating e-Groups. Despite the membership risk, paedophiles in particular are currently participating in e-Boards and e-Groups because they seem to think that their anonymity practice protects them against the danger of identification.

Conclusion

The Internet provides an unmanageable infrastructure, protocols and facilities that support anonymity. Both paedophiles and hackers have established organised communities via the Internet to support communications and dissemination of information, tools and techniques via Web sites, e-mail, chat rooms, FTP sites, Usenet newsgroups, encryption tools, remailers and anonymous server facilities. These two organised criminal groups use anonymity to protect individuals whose actions reflect *mens rea*. While the Internet remains unregulated and unpoliced, organised crime groups such as paedophiles and other sexual abusers, hackers, money launders, drug dealers, terrorists and fraudsters will continue to use its infrastructure and facilities to communicate and distribute materials.

An individual's right to privacy granted by numerous international covenants and treaties shelters not only innocent parties but also organised crime. What constitutes an acceptable balance between law enforcement, individual privacy and human rights? The new European Convention on Cybercrime discloses that member states have agreed to adopt legislation and other measures that will empower competent authorities to collect or record (and compel a service provider to collect, record or cooperate) real-time traffic data and the interception of content data. Societies are apparently prepared to tolerate an erosion of personal freedoms in an effort to support the community's core values.

References

Boni, W. and Kovacich, G.L. (2000), *Netspionage: The Global Threat to Information*, Butterworth Heinemann, Boston, MA.

Casey, E. (2000), *Digital Evidence and Computer Crime*, Academic Press, New York, NY.

COE (2001), *Convention on Cybercrime*, Council of Europe, European Treaty Series, No. 185, 23 November, available at: http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm (accessed 14 December 2001).

CCP (2001), *Conclusions of the Study on Effective Measures to Prevent and Vontrol High-technology and Computer-related Crime*, Report of the Secretary-General, Commission on Crime Prevention and Criminal Justice, United Nations Economic and Social Council, 30 March, available at: www.odccp.org/adhoc/crime/10_ commission/4e.pdt (accessed 14 December 2001).

Chantler, A.N. (1995), "Risk: the profile of a computer hacker", PhD thesis, Curtin University, Perth.

CSI/FBI (2002), "2002 CSI/FBI computer crime and security survey", *Computer Security Issues & Trends*, Vol. VIII No. 1, Spring.

Denning, D.E. (1999), I*nformation Warfare and Security*, Addison-Wesley, Reading, MA.

Ford, W. and Baum, M.S. (2001), *Secure Electronic Commerce*, Prentice-Hall PTR, Upper Saddle River, NJ.

Forde, P.J and Patterson, A. (1998), *Paedophile Internet Activity*, Trends and Issues in Crime and Criminal Justice Series, No. 97, Australian Institute of Criminology, Canberra, November, available at: www.aic.gov.au/publications/tandi/tandi97.html (accessed 14 December 2001).

Hamilton, J.P. (2000), Speech by Chief Constable of Fife Constabulary, 23 March 2000 at the Microsoft Combating Cross Border Crime 2000 Conference, Cape Town, available at: www.microsoft.com/europe/public_sector/Gov_Agencies/125.htm (accessed 14 December 2001).

Holder, E. (2001), *Testimony before Deputy Attorney General*, Department of Justice, Washington, DC, available at: www.senate.gov/~judiciary/229200eh.htm (accessed 14 December 2001).

Jay_h (1997), *The Boylove Manifesto*, available at: www.stream.ru/homes/bla/e-manifest. html (accessed November 1998).

Marcella, A.J. and Greenfield, R.S. (2002), *Cyber Forensics*, Auerbach Publications, London.

Nichols, R.K., Ryan, D.J. and Ryan, J.C.H. (2000), *Defending Your Digital Assets against Hackers, Crackers, Spies and Thieves*, McGraw-Hill, New York, NY.

PJC and NCA (1995), *Organised Criminal Paedophile Activity*, report by the Parliamentary Joint Committee on the National Crime Authority, November, available at: www.aph.gov.au/senate/committee/nca_ctte/ncapedo/ncapedo1.htm (accessed 14 December 2001).

Sams.net (1997), *Maximum Security – A Hacker's Guide to Protecting Your Internet Site and*

Information Management & Computer Security
11/5 [2003] 209-215

Network, Sams.net publishers, Indianapolis, IN.

Skoudis, E. (2002), *Counter Hack*, Prentice-Hall PTR, Upper Saddle River, NJ.

SNCID (1998), *Organised Crime in Sweden 1998*, Swedish National Criminal Investigation Department, available at: www.police.se/gemensam/rps/rkp/orgcrime.htm (accessed 14 December 2001).

Spike (1997), "Anonymity made easy: a necessity for most newcomers to the BL community", available at: www.demon.nl/freespirit/fpc/pages/spike/anon.htm (accessed November 1998).

Stephenson, P. (2000), *Investigating Computer-Related Crime*, CRC Press, Washington, DC.

Vatis, M.A. (2000), "Statement of the Director, National Infrastructure Protection Center, Federal Bureau of Investigation on 'cybercrime' before the Senate Judiciary Committee, Criminal Justice Oversight Subcommittee and House Judiciary Committee, Crime Subcommittee, Washington, DC, 29 February 2000", available at: www.usdoj.gov/criminal/cybercrime/vatis.htm (accessed 14 December 2001).