Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

HIGH TECH CRIME BRIEF

Child exploitation

2005

02

Children and ICT

The uptake of information and communication technologies (ICT) has led to new criminal activities and new ways of committing traditional crimes. This is the first in a series of high tech crime briefs looking at the impact of ICT on criminal activities. High tech or ICT-related crime is divided into offences where ICT is the object or target of an offence and where ICT is a tool for committing an offence.

ICTs have also created a new space in which children can learn, play and communicate. It is a place of both opportunity and risk where children can develop but where they may also become the victims of crime or engage in illegal behaviour themselves.

The types of crime in which ICT is the object of the offence (such as data theft, interference or damage) do not have a special focus in relation to children. This brief looks at four main ways in which ICT may be used as a tool to exploit children criminally.

1. Direct exploitation of children online

ICT enables offenders to target children individually or collectively. Possible motives include personal gratification of the offender, often by way of sexual exploitation; making money; or enticing children to gain access to email or web sites from which viruses may be launched or the security of the child's computer may be compromised. Children are particularly vulnerable to exploitation via ICT because the medium is attractive, they often use the internet unsupervised and increasingly have access to portable devices with the capacity for data storage, digital photography and communications such as third generation mobile phones. Electronic communications allow offenders to exploit the curiosity and interests of children for a number of purposes.

Sexual exploitation

Sexual exploitation may commence using seemingly innocent facilities such as internet chat rooms. Initial contact may be part of 'grooming' the child, whereby the child begins to trust the perpetrator and is desensitised to sexually explicit material including child pornography. Possible motives for grooming a child are: to engage in cyber sex or simulated sex online, to distribute pornographic material to the child or to induce the child to submit pornographic images of themselves online. In some cases, grooming leads to a physical meeting in which the perpetrator sexually assaults the child. A number of persons have been charged with the offence of online grooming under section 218A of the *Criminal Code 1899* (Qld).

Sale or distribution of illicit material

Children may intentionally or unintentionally be exposed to material in the following categories:

- pornography that is banned for any person to sell or possess, such as child pornography (depicting persons under 16 years);
- forms of adult pornography that are prohibited from sale, but which are not illegal to possess under state classification laws, such as violent and fetish-based erotica; and
- pornography in the category of non-violent erotica, which in Australia may only be distributed legally to adults.

The *Broadcasting Services Amendment (Online Services) Act 1999* (Cwlth) can be used to shut down web sites hosted in Australia that contain banned pornographic content.

A variety of ways may be used to divert children who are online to pornographic sites. One is to send unsolicited email that contains images or links to images. Within Australia, spam is prohibited under the *Spam Act 2003* (Cwlth). 'Page jacking' occurs when a normal search is diverted to a pornographic web site. One offender in the US deliberately set up web domains using common misspellings of sites popular among children to divert them to pornographic sites. Another method used is to manipulate the metadata associated with a site to allow it to be falsely indexed. Once a suspect site has been entered by a child they may be subject to 'mousetrapping' where they cannot back out from that site and instead are referred back to the same site or other (usually pornographic) sites. Pop-up advertisements may also appear on screen to encourage traffic to pornographic sites. Peer-to-peer exchanges may also occur, especially in online chat rooms.

Fraud

Children may be involved in online fraud as victims, offenders or in some instances, both. An online 'payment' may comprise fraud committed by the child. For example, a child might use the credit card account details of other family members without their authority. 'Internet dumping' is another payment method that a child may knowingly or unwittingly use, where an internet connection is re-directed to a premium telephone service.

2. Indirect exploitation enabled by the use of ICT

The use of ICT may be intrinsic to some criminal activities that indirectly involve children. Typical offences are completed through the use of ICT where people gain access to, store, trade in or possess child pornography in the form of images or text. The networks that are developed may operate on a social or a commercial basis.

Various types of images may be available, including images of children, actors made to appear as children, digitally created images of children and pictures of children manipulated ('morphed') to appear in a pornographic context. There is evidence of considerable growth in the number of people who are involved in the exchange of images compared with those involved in the original abuse.

3. Direct exploitation enabled by the use of ICT

ICT may be used to support many types of offending. It is used to facilitate various forms of physical child exploitation, including sexual abuse. The sexual abuse of children in Australia is prohibited under state and territory law and by Australians overseas, under Commonwealth law. See, for example *Crimes Act 1900* (NSW): 66A (sexual intercourse with a child under 10 years); 66C (sexual intercourse with a child between 10 and 16 years); 61M (aggravated indecent assault child under 16 years); and 61O (aggravated act of indecency child under 10 years, or between 10 and 16 years).

ICT supports informal social networks of paedophiles who seek to abuse children sexually. Organisers of illegal commercial activities may also organise child prostitution in relative secrecy using chat rooms and bulletin boards.

4. Targeting ICT equipment

Children have increasing access to portable items of ICT equipment, which can become the object of theft or misuse. Children may also be involved as victims or perpetrators of computer attacks. Children (like adult computer users) may be enticed to navigate the web, download material and operate email accounts in ways that compromise computer security. They may become witting or unwitting vectors for the propagation of spam, or the spread of harmful code.

Law enforcement implications

The use of ICT in relation to child exploitation presents significant challenges for law enforcement. Particular issues relate to the definitions used, the detection of offences and the identification of victims.

Definitions

There are differences between nations in the categories of behaviour that are prohibited and the ways in which they are regulated. There is not, for example, a common international definition of child pornography. The legal status of 'morphed' images of children under 16 is even less clear. Definitions also have a subjective element, such as a requirement in relation to child pornography, that an image be offensive to a reasonable adult person.

Detection

The misuse of electronic communications is difficult to detect and to investigate, in real time. The capacity to detect exploitative activity may depend on the profile of any network involved. In particular a commercial activity leaves a more obvious trail, such as credit card transaction records. In contrast, social or 'club-like' networks, or individual online contacts may involve an internet chat facility with high levels of security. Children may be co-opted by offenders into keeping their online activity secret. Perpetrators have been known to instruct children to erase computer file directory records of their communication, or to use other facilities such as pre-paid mobile phone services to maintain contact. Although instances appear to be relatively uncommon, the first indication that a child has been targeted in this way may be their disappearance.

Identifying the victims of abuse

There are many thousands of images of child pornography that have been detected by law enforcement officials on the internet. The identification of the children shown in those pictures will assist to stop the abuse of victims, enable support to be offered to them, and identify offenders. The task of identifying victims is being addressed through international cooperation such as with Interpol and the Combating Paedophile Information Networks in Europe (COPINE) project.

Pursuing common threads of investigation

Perhaps the fundamental issue in the international exploitation of children is the enormity of the problem posed by global connectivity. The capacity of often technically expert offenders to use ICT is increasingly being met by the capacity of police in their investigations.

Investigations follow both networked structures and isolated links among offenders and between offenders and individual children. Because of the global nature of computer connectivity, investigation of an ICT offence in one country will probably lead to the discovery of offences and evidence in another. Police agencies have to resolve issues of jurisdictional responsibility at an early stage. The Australian High Tech Crime Centre fosters national cooperation among law enforcement agencies and stakeholders in Australia. International cooperation is provided through the Australian Federal Police Liaison Officer Network and Interpol. Such cooperation will assist responding agencies to properly investigate cases, to ensure that all available evidence is gathered lawfully and that evidence is made available in subsequent prosecutions.

Information on how to report child exploitation that involves ICT can be found at www.ahtcc.gov.au

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

Forde P & Patterson A 1998. Paedophile internet activity. *Trends & issues in crime and criminal justice* no 97. Canberra: Australian Institute of Criminology

Flood M & Hamilton C 2003. *Youth and pornography in Australia: evidence on the extent of exposure and the likely effects* discussion paper no 52. Canberra: The Australia Institute

Johns R 2003. *Child sexual offences: an update on initiatives in the criminal justice system* briefing paper 20. Sydney: NSW Parliamentary Library

Palmer T & Stacey L 2004. *Just one click: sexual abuse of children and young people through the internet and mobile telephone technology.* London: Barnados

Taylor M & Quayle E 2003. *Child pornography: an internet crime.* Hove: Brunner-Routledge