Crime in Australia: International Connections
Australian Institute of Criminology International Conference

Australian Government
Australian Institute of Criminology

Hilton on the Park, Melbourne, Australia 29-30 November 2004

CONFERENCE PAPER:

CYBER CRIME SENTENCING

The Effectiveness of Criminal Justice Responses

Dr Russell G. Smith
Principal Criminologist, Australian Institute of Criminology

CYBER CRIME SENTENCING: THE EFFECTIVENESS OF CRIMINAL JUSTICE RESPONSES

Dr Russell G. Smith
Principal Criminologist
Australian Institute of Criminology

Introduction

This paper considers the question of the effectiveness of criminal justice responses in reducing cyber crime, or of what is known as 'tertiary crime prevention'. Often crimes with devastating transnational consequences can be committed by individuals, sometimes young amateurs, operating personal computers from home. For example, computer viruses can be created and disseminated throughout the world's users of Microsoft products; millions of dollars can be removed from bank accounts electronically, or share markets manipulated by spreading false information; and children can be exploited for reasons of commercial gain or sexual gratification.

The use of judicial punishments to respond to crimes perpetrated through the use of computers raises many intractable questions. How should the courts deal with offenders in such cases? What are the most appropriate punishments that will reflect the seriousness of malicious on-line conduct, and yet provide effective and long-lasting deterrence, without unduly interfering with the rights of others?

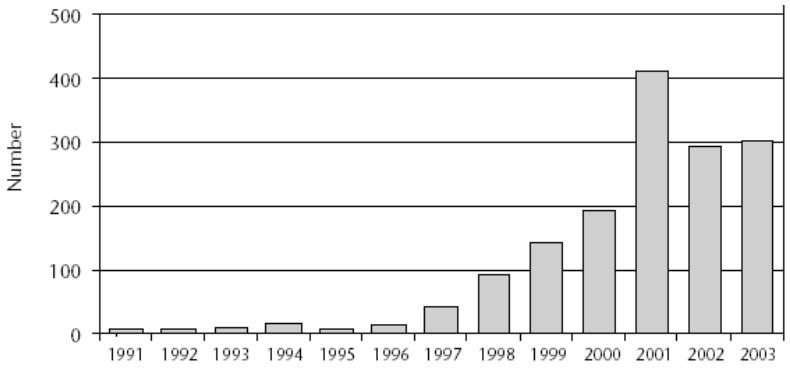
This paper applies the principles used by the courts when determining criminal sentences to cases involving cyber crime and explores the problems that have arisen when the courts have sought to impose both conventional and novel sanctions upon cyber criminals.

The Scale of the Problem

At the outset, it is important to understand the scale of the problem we are dealing with. The first cases of cyber crime to reach the courts were those involving the 'phone phreakers' in the mid-1970s. These were cases involving theft of telecommunications services, such as the famous 'Cap'n Crunch' case in which the offender was sentenced in California to two months' imprisonment for repeatedly using a toy whistle to evade charges for long distance phone calls (Clough and Mungo 1992).

Over the last decade, there has been an increasing number of cases involving cyber crime being reported to police and coming before the courts. The Australian Federal Police's caseload involving electronic crime referrals has increased considerably as is apparent from Figure 1.

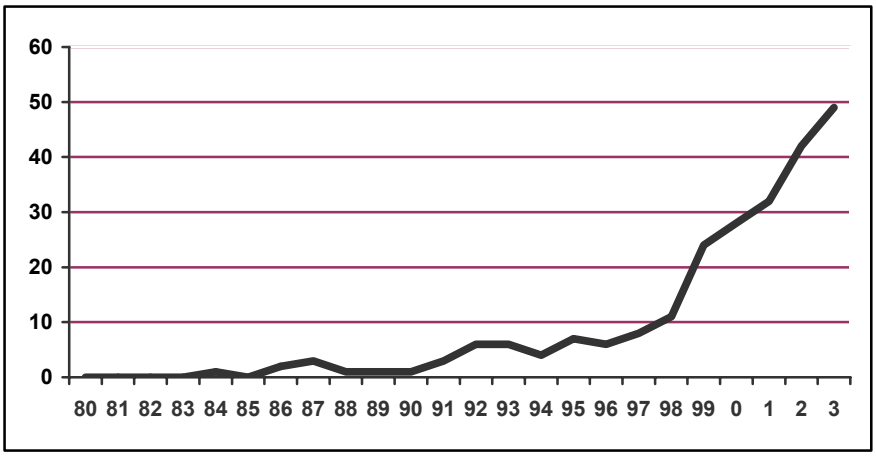
Figure 1 – Electronic Crime Referrals Received by the Australian Federal Police 1991-2003



Source: Australian Federal Police *Annual Reports* (1991-2003)

In Smith, Grabosky and Urbas (2004) the most important cyber crime cases that had gone to the courts in Australia, the United Kingdom, Canada, Hong Kong and the United States since the early 1980s were identified. Some 240 publicly-reported cases had gone to court, with 164 of these involving a conviction. Over the last five years or so the number of cases has increased dramatically as is shown in Figure 2.

Figure 2: Number of Cyber Crime Cases Examined by Smith, Grabosky and Urbas (2004)



Source: Smith, Grabosky and Urbas (2004)

Clearly there are many more cyber crimes that actually take place and many more are reported to the police, than those which go to court. One study in the United States, for example, found that 75% of cases referred for prosecution to federal authorities were declined, primarily due to lack of evidence (Smith, Grabosky and Urbas 2004, p. 38).

Cyber Crime and Punishment

Punishment entails something which is assumed to be unwelcome to the recipient such as loss of liberty through incarceration, disqualification from some activity, or loss of something of value, such as money or time. In determining an appropriate sentence, Judges not only have to comply with sentencing legislation, which sets the maximum penalties that can be imposed, but they also have to comply with principles set out in case law which include the need to accommodate the following aims: proportionality, denunciation, incapacitation, deterrence, rehabilitation, and restitution. Applying these various aspects to the circumstances of cyber crime cases raises some difficult legal and practical problems.

Proportionality

Proportionality in punishment is the modern form of retribution sometimes known simply as 'Just Deserts'. This means that the severity of punishment should be commensurate with the seriousness of the wrong. In the case of cyber crime this raises serious difficulties as the consequences of some types of offending can be devastating, such as the creation and release of a computer virus, and yet the conduct itself may involve no physical violence or even contact with other people.

In one Queensland case in 2001, for example, a 49 year old hacker, Votek Boden was sentenced to two years' imprisonment after being found guilty of hacking into the Maroochy Shire's computerised waste management system. Boden was accused of causing millions of litres of raw sewage to spill out into local rivers and parks killing marine life and causing offensive smells. He was apparently motivated by revenge after having been refused a job at the plant (R v *Boden* [2002] QCA 164).

Denunciation

Denunciation involves the imposition of sanctions in order to express the public's abhorrence of the crime committed. It acts as a symbolic statement that society considers a particular crime as being sufficiently serious to warrant punishment, and that society will not tolerate the law-breaking conduct of the offender. Sentencing remarks of judges in cyber crime cases often denounce the conduct in question. In one of the earliest hacking cases in Melbourne in 1993, the Judge said:

> I formed the view that a custodial sentence is appropriate in respect of each of these offences because of the seriousness of them, and having regard to the need to demonstrate that the community will not tolerate this type of offence. Our society is being increasingly served by and dependent upon the use of computer technology. Conduct of the kind in which you engaged poses a threat to the usefulness of that technology, and I think it is incumbent upon the courts in appropriate cases to see to it that the sentences they impose reflect the gravity of this kind of criminality. . . (County Court of Victoria, 3 June 1993, *per* Judge Smith).

In order to be effective in this sense, the imposition of a sanction must be widely publicised. Unlike in some other types of crime, cyber crimes invariably do attract wide media attention. The risk arises, however, that notoriety in cyberspace, such as that obtained by famous hackers such as Kevin Mitnick, could actively be pursued by young people keen to make their mark in the world (see: http://www.kevinmitnick.com/).

Incapacitation

Incapacitation simply means that because the offender is isolated from society, generally through imprisonment, he or she will be prevented from committing further crimes of the same or similar nature while in isolation. In the case of cyber criminals, however, prison has sometimes allowed them to continue their activities, and there have been cases in which fraudulent scams and paedophile activities have been carried on from prisons through the use of prison computers and mobile telephones smuggled into prison.

In one case, inmates of a correctional facility at Lino Lakes in Minnesota, compiled an extensive database on children from the surrounding area. The prisoners, who had access to information technology through a prison-based computer programming and telemarketing business, scanned children's photographs and collated other information from local newspapers. The annotated files on local children contained information regarding which girls took piano lessons, who had entered children's beauty contests, and also included descriptions of children's physique. The towns in which the children lived were alphabetised and coded with map co-ordinates (Bernstein 1996). It was unclear whether these data were collected purely for purposes of voyeurism or fantasy, for planning subsequent criminal activity following release, or for sale to child molesters.

The other problem with incapacitation is that although offenders may not repeat their offence while in prison, they often re-offend immediately upon release. In the case of Kevin Mitnick, a number of hacking offences were committed while he was on parole. Mitnick had been previously arrested four times for hacking during the 1980s and served a one-year prison term (see http://www.usdoj.gov/USo/cac/pr/cac70627.1.html).

Deterrence

Deterrence can take two forms which were concisely summarised by Cesare Beccaria in 1764: 'punishment aims to dissuade the criminal from doing fresh harm to his compatriots (special deterrence), and to keep other people from doing the same (general deterrence)'. In determining whether punishment is an effective deterrent for cyber crime, evidence is needed of the extent to which individuals are aware of the possible punishments which may result from their criminal conduct; whether they understand the probability of detection, prosecution and conviction, and whether or not individuals are minded to act upon any such knowledge by modifying their propensity to commit crime. Unfortunately, serious doubts have been raised about these matters.

Surveys of offenders have found that they rarely know what penalties govern their conduct, although the hacking community is often quite knowledgeable about the exploits of other hackers and how they have fared in the courts. As we have seen, the probability of conviction tends to be relatively low in these cases for a range of legal and evidentiary

reasons. Finally, research has shown that offenders rarely make a rational decision to carry out their offence or to desist, based upon the possibility of being punished.

A further problem with achieving deterrence lies in the fact that many individuals believe that what they have done should not be illegal. Many cyber criminals have claimed that they had no malicious intention but were simply motivated by curiosity. Some who have stolen software illegally have believed that it is their right to make use of anything that is provided online. The result is that cyber criminals might simply not accept that what they were doing is wrong. One 17 year old offender from West Wales, who styled himself 'Curador', claimed that he was authorised to gain access to e-commerce sites because there was no warning that unauthorised access was prohibited. He called himself the 'saint of e-commerce' on his Internet sites 'e-crackers.com' and 'freecreditcards.com' and wrote:

> I'm for e-commerce when concluded in a secure and sensible manner but this is a rare thing. Most companies put some kind of page together and wait for the money to roll in. These people are the criminals (see: http://www.guardian.co.uk/internetnews/story/0,7369,517864,00.html).

In July 2001, he was sentenced to 3 years' probation. Nonetheless, the courts in many cases involving cyber crime continue to identify deterrence as one of the aims of punishment when sentencing. The role of deterrence has also motivated some legislatures to increase maximum penalties in the hope of reducing cyber crime. Once again, research has shown that increasing maximum penalties does not lead to reduced offending.

Rehabilitation

Rehabilitation has gone through periods of support and criticism throughout history as an objective of punishment but still remains one of the main purposes relied upon by the courts in sentencing offenders. Prisons see their role as being, amongst other things, places which provide opportunities for rehabilitation, by encouraging offenders to be productive, law abiding citizens. They seek to achieve this aim by challenging the offence-related behaviour; encouraging responsibility for one's actions; promoting self-esteem and developing educational, social and living skills.

On some occasions, it seems that punishment has, indeed, had a rehabilitative effect on cyber criminals. Simon Vallor, 22, from North Wales, who created some of the world's most prolific computer viruses, served eight months of a 2 year sentence of imprisonment. When he was released he said:

> I've learnt from my mistakes. I would never try to create a virus again. I want to help companies improve their security systems. I never meant the bug to spread across the globe and I was shocked when the FBI became involved. Going to prison was terrible. It was the worst time of my life (see: http://news.bbc.co.uk/2/hi/uk_news/wales/2678773.stm).

Restitution

Restitution aims to compensate the victim for the injury caused by the criminal act. The main problem with restitution is that offenders rarely have the means available to them to pay compensation – particularly young offenders who have caused extensive harm. A further problem is that criminal courts are not well-equipped to quantify financial loss which is usually left to the civil courts to assess. Some offenders may, however, undertake community work or even unpaid-work for the victim, although this can also present practical problems. On occasions, however, substantial orders for restitution are made against cyber criminals.

In the case of Geoffrey Osowski and Wilson Tang, for example, who were former accountants of Cisco Systems Inc., and who had illegally issued more than US$8million worth of stock to themselves through the use of the company's computers, sentences of 34 months' imprisonment were made in addition to restitution orders amounting to US$7.9 million (see: http://www.usdoj.gov/criminal/cybercrime/cccases.html).

Forfeiture and Restriction of Use Orders

In addition to conventional punishments of imprisonment and fines, courts have recently used some novel orders either as conditions of probation or for parole in which computers have been forfeited, or in which the offender's usage of computers has sought to be restricted or monitored. In Australia, there have been a number of cases in which these orders have been used. In the first case, the offender's computer was subject to a forfeiture order in order to facilitate compliance with other conditions that he seek psychiatric treatment for an addiction to cyber sex (District Court of Queensland, Ipswich, 20 June 2002; see West 2003).

In 2003, a 17 year old, was alleged to have attempted to murder a man whom he met in an Internet chat room, and with whom he had allegedly engaged in a sexual encounter following the online meeting. As part of the bail conditions imposed on the accused teenager, were orders that he not use the Internet except for school work, that he obey a nightly curfew of 9.00pm, and that he report to police three times a week until his next court appearance. His computer, allegedly used to make contact with the man was seized by police (Melbourne Magistrates' Court, 28 October 2003; see Milovanovic 2003).

A further case involved a 69 year old man in New South Wales who was charged with possession and publication of child pornography. He was originally sentenced to two years' imprisonment for the publication offence and five years' probation for possession with conditions that he not use any computer at any time connected to the Internet, and that he not be in the company of any person under the age of 18 without the specific written permission of a probation and parole officer. On appeal the sentence was reduced to two years' imprisonment with a non-parole period of 12 months (Nowra District Court, 18 November 2003).

Recent research into cyber crime sentencing has found 33 cases in which conditional orders had been used (Smith 2004). In approximately one third of cases, these conditional

orders were not challenged on appeal; in another third of cases the conditions were challenged and set aside on appeal; and in the final third of cases the orders were affirmed (see Table 1).

Table 1 – Restriction of Possession and Use Cases 1992-2003

Order	Un-challenged	Held Valid	Held Invalid	Total
Forfeiture	3			3
Ban / restriction on possessing computers	2	5	5	12
Ban / restriction on using computers	4	5	1 – in prison 4 – on parole	14
Monitoring of computer usage	4	3		7
Ban / restriction on using Internet	1 – on bail 4 – on parole	8	9	22
Total	18 (31%)	21 (36%)	19 (33%)	58 (100%)

Note: 33 cases (29 USA, 3 Australian, 1 Canadian) identified during the current research. Some cases involved more than one type of order in addition to other sentences.
Source: Smith (2004).

The Effectiveness of the Orders?

How, effective, then are forfeiture and restriction of use orders in reducing cyber crime? A number of problems seem to be present. First, the use of forfeiture of an offender's personal computer and modem is unlikely to stop the offender from using any one of a number of computers that are readily available to members of the public in libraries and other public places such as Internet cafes. Forfeiture is, therefore, unlikely to have an incapacitating effect. Secondly, forfeiture of a personal computer may affect individuals other than the offender, such as where other family members make use of the computer for school work or recreational activities. Forfeiture could, therefore, infringe the principle of proportionality in punishment.

Thirdly, restriction of use orders will only be effective to the extent that the order is capable of being enforced. This may require that probation officers be trained in computer forensics to conduct thorough inspections of the offender's computer, which is unlikely to be feasible for most probation services. Technologically adept offenders would be quite capable of concealing their activities from most probation officers who have not been fully trained in computer forensics. Fourthly, if monitoring or filtering software is installed on the offender's computer this could be disabled by the offender, or be either inadequate to detect the full range of prohibited content, or, alternatively, could be over-inclusive and prevent the offender from gaining access to legitimate content. This could impede a person's potential rehabilitation or employment during parole.

Fifthly, forfeiture and restriction of use orders could create problems in terms of rehabilitation of offenders, particularly for individuals who work in the information and communications technologies industries where a ban on computer or Internet usage may make them unemployable. In addition, the use of filtering software may be over-inclusive and prevent the offender from gaining access to legitimate content.

Finally, and related to the problem of achieving rehabilitation, forfeiture and restriction of use orders may mean that the offender is unable to earn sufficient money to pay compensation orders or other financial penalties. Similarly, offenders subject to forfeiture or restriction of use orders could not engage in some types of constructive community service that might require the use of computers. In this sense, their skills are being wasted during the period of the order.

Future Directions

From these few illustrations of sentences imposed on cyber criminals in recent years, we can see that courts are beginning to adapt sanctions to suit the novel circumstances of the cases. The difficulty which courts face in sentencing is to impose an appropriate punishment that will have some deterrent effect while at the same time devising orders that will be enforceable and not overly restrictive on the offender and other third parties. Rather than seeking to impose *restrictions* on the use of computers as a means of punishment, courts could, arguably, adopt the alternative approach of requiring offenders to *use* their computer skills or knowledge for *constructive* purposes. This could occur in a variety of ways (see Smith 2004).

First, by assisting police in investigating high tech crime cases. In the case of *United States* v *David Smith*, the author of the Melissa virus, for example, the offender's assistance as a police informer led to the conviction of Jan DeWit, the author of the so-called Anna Kournikova virus, in the Netherlands on 27 September 2001 and Simon Vallor, the author of the Gokar virus, in London on 21 January 2003.

Secondly, by delivering lectures to the public or in schools about the dangers associated with computer crime and publicly discouraging others from engaging in similar conduct, such as occurred in the case of *United States* v *Richard W. Gerhardt* District Court of the Western District of Missouri, 13 March 2003, a case involving theft of passwords. Some offenders could be required to make use of their skills by performing periods of supervised community service in the high tech field.

Finally, offenders could be required to express their remorse for what happened and to publicise the outcome of their case. This has already occurred in the case involving the juvenile hacker known as 'c0mrade', who, in addition to serving six months' in a detention facility, was ordered to write letters of apology to the Department of Defense and NASA whose computers he had hacked, and also to permit public disclosure of information about his case which might not normally occur in a case involving a 16 year old (see: http://www.usdoj.gov/criminal/cybercrime/comrade.htm).

Although conventional punishments of imprisonment and fines will continue to be used in appropriate cases, it is likely that some judges will experiment with a range of conditional orders. Some of these may result in legal challenges or be counter-productive in reducing crime, but carefully framed conditional orders could enhance the effectiveness of judicial punishment in certain cases by making constructive use of the motivational factors that drive many cyber criminals.

References

Australian Federal Police 1991-2003. *Annual Reports 1991-2003*. Canberra: Australian Federal Police.

Bernstein N 1996. 'On prison computer, files to make parents shiver', *New York Times*, 18 November: A1.

Clough B & Mungo P 1992. *Approaching zero: Data crime and the computer underworld*, London: Faber and Faber.

Milovanovic S 2003. 'Student banned from Internet after stab charge', *The Age (Melbourne)*, 29 October: 3.

Smith R G 2004. 'Criminal forfeiture and restriction-of-use orders in sentencing high tech offenders', in *Trends and Issues in Crime and Criminal Justice*, No 286. Canberra: Australian Institute of Criminology.

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