The Australian and New Zealand Society of Criminology
15th Annual Conference
CRIMINOLOGY IN THE 21ST CENTURY:
PUBLIC GOOD OR PRIVATE INTEREST?

21 February 2001
University of Melbourne
Panel Session B - Crime, Computers and the Internet
2.30-4.00pm

"Computer Crime: Crisis or Beat-Up?"

Russell G. Smith

Introduction

The increased use of computers and communications technologies over the preceding decade has created considerable apprehension in the international community that they are being put to illegal use of various kinds. Fears of wide-scale electronic vandalism, copyright infringement, fraud, and other forms of electronic crime have been discussed in the public media and the academic and professional communities alike. It has also been argued that traditional legal responses to computer crime have been both ineffective and inappropriate to deal with such an international phenomenon. But are these views based on a distorted representation of the true position?

This paper evaluates the currently-available evidence in support of the proposition that computer crime has reached crisis point; and the opposing evidence that demonstrates that the problems associated with computer crime have been greatly exaggerated and over-emphasised in public discourse. The evidence will be discussed from four perspectives: empirical and statistical studies; how law enforcement and prosecutors have coped; whether the law has kept up with technological developments; and whether a crisis exists from the victim's point of view.

Some reasons will then be advanced for the posited distortions in the true representation of computer crime and some ideas offered as to how the problem may be discussed more objectively and moderately in the future. To begin, however, we need to define some key concepts and terms.

Terminology

The Meaning of Computer Crime

For present purposes, computer crime will be taken to mean any criminal activity that involves digital technologies as the target or means of offending. Computers are now all-pervasive in modern society, and obvious technologies include telecommunications devices such as fixed-line telephones, facsimile machines, and cellular telephones, and personal computers, servers, modems, and peripheral equipment used to connect users to the Internet. Less obvious technologies that may be put to illegal use extend from computers used in financial transactions such as Automated Teller Machines and Electronic Funds Transfer systems to computerised odometers in motor vehicles that can be manipulated to improve the re-sale value of a used vehicle.

Legislatively, computer crimes have been described using a wide variety of legal concepts including offences proscribing unauthorised access, modification, and impairment of data, theft of data and intellectual property, the transmission of illegal content electronically, and the unauthorised impairment of electronic communications (see, generally, Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000).

The Meaning of Crisis

A crisis is a time of acute danger or suspense. In critical care in hospitals, for example, patients are catered for who face imminent danger of death or whose illnesses have reached a decisive moment in which more intensive forms of therapy are required than previously. To have reached crisis point, there has generally been a progression from bad to worse with innovative and intensive responses being required.

In the digital environment, a crisis could be said to have occurred when one's computer stops working. This could take place through an interruption of the power supply, or because a malicious code such as a virus or worm has interfered with the proper functioning of the computer. A crisis in computer crime could also be seen to have arisen when a user receives a bill for thousands of dollars that relates to unordered goods or services obtained fraudulently by someone else on-line. If we are to believe the media, then there is abundant evidence of a crisis in computer crime.

The Meaning of Beat-Up

In British country life, if one speaks of a beat-up this will usually describe the activities of farm workers going about the countryside seeking to rouse game by creating a noise. In the media, a beat-up is a news story whose prominence and importance greatly exceeds the available supporting evidence. For the purposes of our discussion, the characterisation of computer crime as a beat-up simply means that the problematic nature of computer crime has been exaggerated far beyond any material available to justify such concerns.

The question for discussion, however, is who might be responsible for beating-up the notion of computer crime, and what benefit is to be derived from overstating the seriousness of the problem?

The Evidence

Empirical Evidence - Crisis

The statistical information that we have on computer crime, and particularly economic crime, comes mainly from victimisation surveys carried out in the business community, and extrapolated estimates of loss by business analysts. Police statistics in this field are generally not specific enough to permit an analysis of the means by which crime occurs, such as through the use of a computer.

Over the last few years, business victimisation studies have found increased levels of concern amongst those surveyed about the risk of computer-related fraud as well as actual levels of victimisation.

The latest international fraud victimisation survey conducted by Ernst and Young in October 1999, surveyed 10,000 senior executives in major organisations in fifteen countries, of whom 739 replied (Ernst and Young 2000). Although the response rate of seven per cent was exceedingly low, thus making the findings of limited generalisability, some indications of the seriousness of computer fraud were apparent. Computer fraud was viewed as a threat to organisations more than any other type of fraud with 60 per cent of respondents fearing that such fraud was likely or very likely to occur within their organisation. The kinds of computer frauds that presented the greatest concern were those that involved manipulation of data records or computer programs to disguise the true nature of transactions, hacking into an organisation's computer system to steal or to manipulate business information, and unauthorised transfers of funds electronically.

In the United States, the Computer Security Institute's fifth annual *Computer Crime and Security Survey* released in March 2000, found that more companies surveyed are reporting intrusions than in the past, that dollar losses are increasing, that insiders remain a serious threat, and that more companies are doing more business on the Internet than ever before. Ninety percent of respondents detected security breaches over the preceding 12 months. At least 74 percent of respondents reported security breaches including theft of proprietary information, financial fraud, system penetration by outsiders, data or network sabotage, or denial of service attacks. Information theft and financial fraud caused the most severe financial losses, put at US$68 million and US$56 million respectively. The losses from 273 respondents alone totalled US$265.5 million—more than double the average annual loss for the previous three years—which was US$120.2 million. Losses traced to denial of service attacks amounted to US$77,000 in 1998, and by 1999 had risen to US$116,250. Finally, many companies experienced multiple attacks with 19 per cent of respondents reporting 10 or more incidents (Freeh 2000).

Also in the United States, the newly established Internet Fraud Complaint Centre—organised by the United States Department of Justice and the Federal Bureau of Investigation (2001)—received 19,490 complaints relating to Internet fraud from the time of its establishment on 8 May 2000 and 30 November 2000. The average monetary loss per complaint was US$665.00 with 49 per cent of complaints relating to auction fraud. Complaints were received from 106 countries, most coming from the United States, Canada, Australia, and the United Kingdom. This could, of course, merely be indicative of countries with the highest Internet usage.

Various government agencies also monitor Internet-related fraud. In 1999, Internet Fraud Watch reported an estimated 2 million instances of credit card fraud taking place with respect to on-line purchases in Europe, with a 600% increase in Internet fraud complaints occurring in the United States since 1997 (Philippsohn 2000).

In the United States, over 18,600 complaints were registered on the Federal Trade Commission's fraud database 'Consumer Sentinel' in 1999, more than double the number in 1998—when 8,000 were registered (United States, Department of Justice 2000).

In a telephone survey of 1,006 on-line consumers conducted for the National Consumers League in the United States between April and May 1999, twenty-four per cent said they had purchased goods and services on-line. Seven per cent, which represents six million people, however, said that they had experienced fraud or unauthorised use of credit card or personal information on-line (Louis Harris and Associates Inc 1999).

In a worldwide clean-up operation of the Internet, involving the Office of Fair Trading in Britain and its counterparts in twenty-two other countries, 1,159 potential 'get rich quick' schemes were found being advertised on Internet sites (Office of Fair Trading 1998).

In KPMG's latest Fraud Survey (1999) over 1,800 of Australia's largest businesses were surveyed in February 1999. 367 replies were received (20%) with information being provided on fraud awareness, the experience and cost of fraud, who perpetrated the fraud, how it was discovered, and why it occurred. Specific data were also obtained concerning computer-related fraud. In all, some 7,280 incidents of fraud generally were reported in the two years preceding the survey and fifty-seven per cent of respondents reported at least one incident during that period. Total losses amounted to A$239 million with the average cost per incident of A$1.1 million. Although small in number, between the surveys conducted in 1997 and 1999, there was a 71 per cent increase in the percentage of respondents to KPMGs surveys who reported computer-related fraud (7% to 12%). Total reported losses due to computer crime were over A$16 million, although these figures are likely to be under-estimates as many organisations were unaware of the extent to which their organisation was being defrauded through the use of computers and some did not define other forms of fraud as computer-related. In 1999, 36 per cent of KPMGs respondents who reported computer crime were either unaware of how much they had lost or were unwilling to disclose it.

In Australia, in November 1998, another survey was carried out of 350 large organisations by the Victoria Police and Deloitte Touche Tohmatsu (1999). Thirty-three per cent of respondents reported unauthorised use of their computers within the preceding twelve month period and one quarter of these attacks were motivated by financial gain. More than one third of those who responded believed that computer theft would have an impact on their organisation over the next five years.

A recent International Chamber of Commerce (ICC) survey revealed a three-fold increase in reports from organisations that had had their networks hacked between 1997 and 1998 (Philippsohn 2000).

Computer crime is also of concern to government agencies as they increasingly become reliant on computers for the provision of services and the payment of benefits. In the survey of computer crime and security conducted by the Office of Strategic Crime Assessments and the Victoria Police Computer Crime Investigation Squad (1997), four out of the eleven government agencies surveyed reported misuse of their computer systems with almost half reporting external forms of attack, that is remote access to computer systems. The most frequently reported types of computer abuse reported by the government agencies surveyed related to damage or unauthorised access to, or copying of data and programs.

Empirical Evidence - Beat-Up

Although some of these figures are indeed disturbing, they need to be placed in context. It has been estimated, for example, that some US$2.85 trillion is obtained each year from organised criminal activities such as trafficking in drugs, guns, and people, illegal gambling, fraud, embezzlement, extortion, and other criminal enterprises (Walker 1999). Thus, losses of a few hundred million through computer crime are of less significance that when considered in isolation.

The increase in computer crime also needs to be considered in light of the substantial increase in computer usage.

Internet usage surveys carried out by the Australian Bureau of Statistics (1998, 1999, 2000), for example, have found an increase of fifty-two per cent in the number of adults in Australia who had gained access to the Internet between November 1998 and May 2000—4.2 million adults (31 per cent of the adult population) to 6.4 million adults (46 per cent of the adult population).

The surveys also found a 180 per cent increase in the number of adults who had used the Internet to purchase or order goods or services for their own private use between November 1998 and May 2000—(286,000 or 2.6 per cent of adults in the twelve months to November 1998 to 802,000 adults (6 per cent of Australian adults) in the 12 months to May 2000 (a 2.4 per cent increase in the percentage of the adult population). The percentage of Internet shoppers who paid for goods and services by disclosing their credit card details on-line, stayed much the same, increased by only 0.5 per cent—from 80.5 per cent in November 1998 to 81 per cent in May 2000.

In addition, many of the problems associated with computer crime relate only to a relatively small proportion of the world's population. Even in Australia, only six per cent of the population used the Internet to purchase goods or services on-line last year. If a conservative estimate of 10 per cent of these were defrauded, that means that only 80,000 people would have been victimised.

In terms of electronic funds transfers, the statistics complied by the Australian Securities and Investments Commission (2000) on the operation of the Electronic Funds Transfer Code of Conduct show that there has been an increase from 42 to 64 complaints made under the Code per million transactions between 1998-99 and 1999-2000. In 1999-2000, there were 106,719 complaints out of 1,655,362,481 electronic transactions. In percentage terms, this represents a very small number indeed.

Finally, a number of the surveys that have been conducted cannot be said to have examined the incidence of computer crime objectively. Some have used clearly leading questions when asking respondents about their experiences. Others have been overly general in seeking information—often not even defining or explaining what computer crime actually means.

For example, there are many reports of so-called 'Internet or on-line fraud'. The National Consumers League in the United States found that American consumers lost US$3.2 million to on-line scams in 1999 alone. However, 97 per cent of cases involved consumers paying for goods using cheques and money orders, making the on-line component of the fraud simply the fact that the goods were advertised electronically (National Office for the Information Economy and the Australian Computer Society 2000). In essence, these were no more than traditional cases of cheque or money order fraud.

Investigation and Prosecution - Crisis

If we look at computer crime from the perspective of police and prosecution agencies, there is, indeed, some evidence of a crisis, rather than a beat-up.

Many law enforcement agencies have reported increased instances of computer offences being reported to them for investigation. In the year 1999-2000, the Australian Federal Police received

190 electronic crime referrals with 23 per cent relating to unauthorised access, 15 per cent relating to pornography / paedophilia, and 13 per cent relating to the use of the Internet to threaten or to harass (Australian Federal Police 2000, p. 19). Over the last ten years the computer crime case load has increased substantially as we can see from Figure 1. These, however, represent only the tip of the iceberg as the rate of reporting of computer crime remains extremely low (see Geurts 2000).

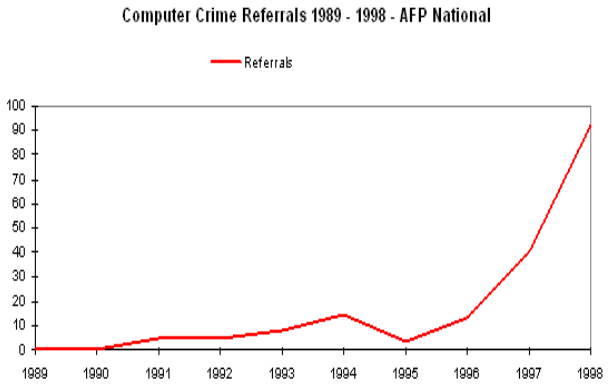

Figure 1
Computer Crime Referrals 1989-1998 - AFP National
Source: Geurts 2000.

In the United States, the Federal Bureau of Investigation's computer crime case load has also increased substantially. In 1998, the FBI opened 547 computer intrusion cases while in 1999, it opened 1154, more than double (Freeh 2000).

Law enforcement agencies have generally found the investigation of computer crime to be costly, slow, and difficult. There have been relatively few successful prosecutions and sentences have tended to be in the lower range of severity for white collar offences. Police computer crime squads tend to be composed of interested amateurs who acquire considerable experience and expertise during the course of investigations. Often their skills are recognised by the private sector to which they invariably gravitate in the pursuit of more remunerative positions.

The evidence of a crisis also arises because of the scale of investigations that computer crime agencies are required to undertake. The Australian Federal Police, for example, has seen an exponential increase in the size of data storage systems that are required to be analysed in investigations. Where a law enforcement examination of a computer hard drive in 1990 involved 50,000 pages of text, a contemporary examination would involve between 5 and 50 million pages of text. AFP statistics also reveal that the average capacity of data storage media seized for analysis has risen from 35 megabytes in 1991 to 3,445 megabytes (3.4 Gb) in 1999. This increase in investigative capacity has created considerable resource implications for police (Geurts 2000).

The crisis, in the policing of computer crime, however, lies not so much in the difficulty of investigation, but in the acquisition and retention of sufficient personnel to undertake the work. Unlike some other police services, the Australian Federal Police has had some success in retaining computer forensic specialist officers through the use of flexible remuneration policies,

opportunities for ongoing professional development, and access to new and updated equipment (Australian Federal Police 2000, p. 19).

Finally, considerable problems arise in the investigation of computer crime which involves cross-border activities. Even if evidence is able to be adduced, problems of locating and extraditing an accused person from other jurisdictions remain. This adds considerably to the cost of law enforcement and delays the completion of matters.

Investigation and Prosecution - Beat-Up

The problem of computer crime for law enforcement also, however, needs to be placed in context. Although computer crimes often involve voluminous information and data trails, so do other crimes. The prosecution of Martin Bryant following the Port Arthur shooting, for example, involved 1,200 witnesses, more than 2,000 relevant reports, more than 2,700 photographs, and a further 2,000 exhibits (Fife-Yeomans 1998).

In fact, the investigation of many computer-related crimes is facilitated precisely because information is recorded digitally. Police are able to search extensive databases and compile computer-generated models to assist with investigations. Often digital data trails are easier to follow and more apparent than paper trails of evidence.

Digital systems can also be used to track the movements of suspects through the use of global positioning systems, or even by tracking cellular telephone communications. The location of Pablo Escobar, for example, one of the world's most notorious cocaine traffickers, was able to be ascertained by law enforcement agencies tracing his cellular telephone activity. In July 1992, a small fleet of aircraft equipped with scanning devices and onboard computers with voice recognition programs, flew over Medellin while monitoring thousands of calls, some of which matched samples of Escobar's voice, thus enabling his location to be identified (Thompson 1996, p. 89).

There are also now numerous international arrangements to deal with mutual assistance to help law enforcement deal with cross-border investigations. Although these are often slow and costly, the difficulties are not essentially any different in the case of computer crime than in the case of other cross-border prosecutions involving international crime. Police and prosecutors have had to deal with international criminals for hundreds of years in cases involving piracy, illegal immigration, drug trafficking, and smuggling, not to mention serious fraud.

The Law - Crisis

Over the last decade a number of legal problems have emerged which have created difficulties for the successful prosecution of computer crimes. Their nature has sometimes been remarkably simple, such as the omission of laws that proscribe deception of computers as opposed to human actors, thus making ATM-related fraud sometimes difficult to prosecute (*Kennison* v *Daire* (High Court of Australia, 20 February 1986), (1986) 160 CLR 129.

As these problems grew, a variety of solutions was adopted. This has created problems itself as laws are now variable and conflicting across different jurisdictions.

The solution has been to seek harmonisation of laws and procedures and this has been successful in a number of spheres. The Commonwealth of Australia, for example, has introduced the

Electronic Transactions Act 1999 to facilitate electronic delivery of services by government. It has also proceeded with the introduction of a Model Criminal Code to harmonise criminal laws throughout Australia and has issued a Discussion Paper on the reform of computer-damage offences and questions of jurisdiction (Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000).

Although there have been recent attempts to harmonise the definition of computer-related crime both nationally and internationally, notably the Council of Europe's *Draft Convention on Cybercrime* (2000) and the G-8 Countries' High-Tech Crime Group established in 1996 (Sussmann 1999), much remains to be done.

McConnell International (2000), for example, recently carried out a survey of laws in 52 countries and found that thirty-three of the countries surveyed had not yet updated their laws to address any type of computer crime. Of the remaining countries, nine had enacted legislation to address five or fewer types of computer crime, and ten had updated their laws to prosecute six or more of the ten types of computer crime identified.

The Law - Beat-Up

Although the process of law reform relating to computer crime has been slow, it is, arguably, quicker than in other areas of law—notably corporations and taxation law. Many of the legal issues concerning computer crime relate not only computer crime but also other types of cross-border crime—particularly those that involve economic offending. The seriousness of the computer crime law reform problem is, therefore, not substantially different from other areas of international law.

Victims - Crisis

Although well-publicised media reports of computer crimes could be said to have beaten-up the problem unduly, many individuals who have suffered the consequences of computer crime have suffered severely—and from their perspective, at least, computer crime is of critical concern.

Individuals have lost substantial sums through funds transfer frauds, businesses have been crippled though external denial of service attacks, commercial secrets have been stolen, and personal information disseminated publicly at significant personal cost.

In the United Kingdom, for example, one case of PABX fraud cost a government department the equivalent of US$80,000 a day while another department lost US$640,000 over a six week period (Wraith 1999). In yet another case, illegal access was gained to Scotland Yard's PABX system in London by computer hackers based in the United States. Unauthorised international calls to the value of A$1.29 million were made for which Scotland Yard was liable (Tendler and Nuttall 1996).

The Internet has also been involved in crimes of a more personal nature—in one case arguably contributing to the death of a user. In north-western Victoria on 11 July 1999, a seventeen year old boy was killed instantly and two of his friends injured when a home-made bomb, constructed from a recipe discovered on the Internet, exploded (Butcher 2001).

In another case, a rejected suitor posted invitations on the Internet under the name of a 28-year-old woman, the would-be object of his affections, that said that she had fantasies of rape and

gang rape. He then communicated via E-mail with men who replied to the solicitations and gave out personal information about the woman, including her address, phone number, details of her physical appearance and how to bypass her home security system. Strange men turned up at her home on six different occasions and she received many obscene phone calls. While the woman was not physically assaulted, she would not answer the phone, was afraid to leave her home, and lost her job (Miller and Maharaj 1999).

There are numerous other examples of individuals and organisations that have suffered considerably at the hands of computer criminals, and for them, the problem is of critical concern (Grabosky and Smith 1998, Grabosky, Smith and Dempsey 2001).

Victims - Beat-Up

Proportionally, however, the instances of computer crime that have affected individual victims have been relatively few, particularly in view of the extensive use made of technologies such as the Internet and electronic funds transfers between financial institutions and customers.

In addition, many of the problems of computer crime are not essentially new. Take the case of the manipulation of sharemarkets through the use of new technologies. In 1867, for example, a Wall Street stock broker collaborated with Western Union telegraph operators to counterfeit messages which reported bankruptcies and other financial disasters supposedly befalling companies whose stock was traded on the New York Stock Exchange. When the share prices were driven down, the wiretappers then purchased their victims' stock (O'Toole 1978, p. 97).

Last year, much the same strategy was employed by a 24 year old man who lived in a Melbourne suburb who manipulated the share price of an American company by posting information on the Internet and sending E-mail messages around the globe that contained false and misleading information about the company.

On 8 and 9 May 1999, he posted messages on Internet Bulletin Boards in the United States and sent more than four million unsolicited E-mail messages, colloquially referred to as spam, to recipients in the United States, Australia and in other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US$0.33 to US$3.00 once pending patents were released by the company, and that the price would increase up to 900 per cent within the next few months. The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than ten times the previous month's average trading volume. The offender had purchased 65,500 shares in the company through a stock broking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A$17,000.

The Australian Securities and Investments Commission prosecuted the offender for distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was sentenced to two years' imprisonment on each of three counts, to be served concurrently. The Court ordered that 21 months of the sentence be suspended upon his entering into a two-year good behaviour bond with a surety of $500 (*Australian Securities and Investments Commission* v *Steven George Hourmouzis*, County Court of Victoria, 30 October 2000, Stott J).

Arguably, then, new technologies merely replicate traditional forms of crime and although the methodology may be novel, the ultimate objective is well known.

Interested Parties

Who, then, is responsible for describing computer crime as being at crisis point and who can be blamed for beating up the issue unnecessarily? There are groups within society who stand to benefit considerably from propagating each of these perspectives and it is as well to be aware of their interests in order to evaluate the objectivity of the positions they espouse.

Those Who Describe Computer Crime as Being at Crisis Point

The Media

The first group with an interest in describing computer crime as being at crisis point and responses to it out of control, are those in the news and entertainment media. Successful news copy invariably emphasises the seriousness of crime, both economically and in terms of its frequency of occurrence. Stories about new technologies also attract attention, and so the combined impact of reports describing the ever-expanding problem of computer crime invariably makes profit for those in the media world.

Although some sections of the media have focussed on the 'good news' stories of computer security achievements, the war stories of individuals losing fortunes on the Internet continue to attract attention.

Criminal Justice Personnel

Critics of the police have often raised the possibility of police manipulating statistics and reports of their work in order to paint a devastating picture of the seriousness of the crime problem—merely in order to justify their existence and to increase public funding for their work. A computer crime crisis, of course, has the direct consequence that funding for specialist computer crime squads is likely to be increased—although this seems not to have occurred to any great extent to date. This could, of course, reflect the absence of a crisis—at least in the eyes of politicians and those responsible for allocating funds. Alternatively, it could indicate entrenched neglect of funding for police services, particularly in the area of sophisticated crime.

Politicians

Politicians, too, have an interest in emphasising the problems associated with computer crime, as they can then offer solutions and receive the kudos for solving an enduring problem (if, indeed, it has been solved). In addition, it is possible for politicians to deflect attention away from other contentious matters by focusing on the extent of the high-technology crime problem which is often incapable of short-term solutions. Discussion of other more pressing issues such as drug and alcohol abuse can thus be avoided if a devastating computer virus has just been released.

Computer Security Industry

Those in the computer security industry who manufacture devices such as encryption software and biometric user authentication systems (for example, fingerprint scanners attached to keyboards or iris scanners on computer monitors), have much to gain from representations of

computer crime being more serious than it actually is. One of the growth industries for the twenty-first century will be computer security and the more people that are concerned about security, the more products will be sold. An example of the marketing potential of computer security concerns was the Year 2000 problem in which the global cost of avoiding the problem was estimated to be US$920 billion according to the Gartner group. In Australia alone, A$12 billion was spent on the Year 2000 problem and its solutions—where the only reported incidents seemed to be the failure of ticket machines on some buses in Tasmania and South Australia (Gettler 2000). The precautions adopted may, however, have been effective in preventing other more profound consequences.

Luddites

The final group could be described as Luddites—namely, those who eschew modern technological developments and who favour more traditional means of communicating and living. Clearly, if computer crime is seen as being problematic, this improves the position of those who have refrained from using new technologies. In particular, where individuals have refrained from taking up new banking or communications technologies through fear of being defrauded, the assertion that such crime has, in fact, taken place, vindicates their position exactly.

Those Who Are Beating Up the Issue of Computer Crime

On the other hand, there are those with a legitimate desire to represent the on-line world as being free from crime and a safe haven for users globally.

On-line Zealots

On-line zealots, and those who choose to make a living from computer-related business have much to gain from ensuring that the public feel safe and secure when using digital technologies.

Offenders

Similarly, potential computer criminals may seek to derive a benefit from the risks of computer crime being under-estimated. If members of the public continue to use computers regardless of the risks and are complacent concerning computer security, then computer crime may be all that easier to commit.

Governments

Governments which seek to enhance on-line procurement and electronic commerce such as the payment of benefits on-line, also have a keen interest in ensuring that the problem of computer crime is not overstated. In Australia, the National Office for the Information Economy in conjunction with the Australian Computer Society (2000) last year published a Report entitled *The Phantom Menace: Setting the Record Straight About On-Line Credit Card Fraud for Consumers* in which facts favourable to the proposition that Internet shopping was safe for consumers were outlined.

Computer Manufacturers

Finally, those who manufacture computer hardware and software have an interest in ensuring that computer crime is not overstated as fear of victimisation may lead to loss of sales.

Conclusions

On the basis of the evidence considered and the arguments canvassed, it may be concluded that some aspects of computer crime represent a serious problem—although arguably not yet in the category of 'crisis'—while other matters have been unnecessarily characterised as problematic.

Statistics

In terms of the empirical data available, computer crime is of no greater concern than other types of white collar crime and fraud—although it needs to be stressed that our knowledge base is at present, seriously deficient.

Investigation and Prosecution

From a law enforcement perspective, computer crime has created definite problems, mainly to do with the trans-jurisdictional nature of many on-line offences and the difficulties associated with investigation and prosecution in multiple jurisdictions. Levels of expertise and funding within law enforcement agencies are also inadequate to deal with many instances of computer crime and in some areas could be described as being in a state of crisis.

The Law

So far as the law is concerned, we have seen that a number of the problems that have arisen in proscribing objectionable on-line conduct have been overcome in some countries—although novel uses of the new technologies are creating new problems all the time. Some effective and adaptable models have been proposed and tried for dealing with computer crime throughout the 1990s and arguably the legal problems that exist at present are not insurmountable.

Victims

From a victim's point of view, computer crime is certainly a serious problem. Substantial losses may be suffered with little or no chance of recovery as offenders may be located in overseas jurisdictions, or may simply be unable to be located at all. The number of victims suffering at the hands of on-line criminals, however, is relatively small, making the impact of the problem in the community as a whole of medium importance only.

As we have seen, there are those who stand to benefit both from the depiction of computer crime as being in a state of crisis as well as being of less seriousness and a beat-up.

It is important to implement change carefully and deliberately, not overreacting to unusual single instances that come to light, but ensuring that reforms are introduced in such as way as to deal with the specific problem at hand and guarding against the unintended consequences of legislative and preventive measures. In this way, the critical aspects of computer crime may be controlled and the exaggerated and unfounded problems ignored.

Towards More Informed Debate

How, then, can the discussion of computer crime become more informed and moderate?

The starting point comes with improved standards of information. Better and more extensive research needs to be carried out not only locally, but also internationally. One idea, for example would be to include computer-related offences in the next round of the International Crime Victims Survey (see van Kesteren, Mayhew, Nieuwbeerta, and Bruinsma 2000).

Government statistical and census agencies could also play a role in conducting surveys of the population as they are well-placed to undertake research objectively. The Australian Bureau of Statistics, for example, could ask some questions about computer crime and security in its regular surveys on household use of information technologies.

Evidence also needs to come from those within the industry rather than outside commentators. Persuading financial institutions and telecommunications carriers to be frank in disclosing computer crime experiences is by no means simple, but some appropriate sharing of information needs to take place.

With improved levels of information and more accurate surveys of computer crime, we may then be in a position to direct resources appropriately to combat the problem. This may ensure that those who seek to obtain scarce crime prevention resources are not provided with funding merely on the basis of their self-interested reports of the extent of the problem.

References

Australian Bureau of Statistics 1998, *Household Use of Information Technology, Australia 1998*, (Cat. No. 8146.0), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 1999, *Household Use of Information Technology, Australia 1999*, (Cat. No. 8146.0), Australian Bureau of Statistics, Canberra.

Australian Bureau of Statistics 2000, *Use of the Internet by Householders, Australia*, February and May 2000 editions (Cat. No. 8147.0), Australian Bureau of Statistics, Canberra.

Australian Federal Police 2000, *Annual Report 1999-2000*, Australian Federal Police, Canberra.

Australian Securities and Investments Commission 2000, *Complaints Made Under the EFT Code of Conduct 1999-2000*, ASIC, Sydney.

Australian Securities and Investments Commission v Steven George Hourmouzis, County Court of Victoria, 30 October 2000, Stott J).

Butcher, S. 2001, 'Ban Urged on Internet Bomb "Recipes"', *The Age (Melbourne)*, 17 January, p. 7c.

Council of Europe 2000, *Draft Convention on Cybercrime*, (Draft N° 25 REV.5), European Committee on Crime Problems, Committee of Experts on Crime in Cyber-Space, 22 December 2000, Council of Europe, Strasbourg (http://conventions.coe.int/treaty/EN/projets/projets.htm)

Ernst & Young 2000, *Fraud: The Unmanaged Risk*, Ernst and Young, London.

Fife-Yeomans, J. 1998, 'Info Warriors: The Frontline Against Cybercrime', *Platypus Magazine: The Journal of the Australian Federal Police*, No 59, June, pp. 24-5.

Freeh, L. J. 2000, 'Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information Washington, D.C. 28 March. http://www.afp.gov.au/ecrime/louisfreeh.htm (visited 30 January 2001).

Gettler, L. 2000, 'From Apocalypse to Y2K Yawn', *The Age (Melbourne)*, 30 December, p. 12.

Geurts, J. 2000, 'The Role of the Australian Federal Police in the Investigation of High-Tech Crimes', *Platypus Magazine: The Journal of the Australian Federal Police*, March, http://www.afp.gov.au/publica/platypus/mar00/intfrd.htm (visited 5 February 2000).

Grabosky, P. N. and Smith, R. G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Federation Press, Sydney / Transaction Publishers, New Brunswick.

Grabosky, P. N., Smith, R. G., and Dempsey, G. 2001, *Electronic Theft: Crimes of Acquisition in Cyberspace*, Cambridge University Press, Cambridge.

Kennison v Daire (High Court of Australia, 20 February 1986), (1986) 160 CLR 129.

KPMG 1999, *1999 Fraud Survey*, KPMG, Sydney.

Louis Harris and Associates Inc 1999, *Consumers and the 21st Century: A Survey Conducted for the National Consumers League*, Louis Harris and Associates Inc, New York.

McConnell International 2000, 'Cybercrime and Punishment? Archaic Laws Threaten Global Information'. http://mcconnellinternational.com/services/CyberCrime.htm (visited 30 January 2001).

Miller, G. and Maharaj, D. 1999 'N. Hollywood Man Charged in First Cyber-stalking Case', *Los Angeles Times*, 22 January 1999. http://www.cs.csubak.edu/~donna/news/crime.html#stalking (visited 12./6/99)

Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000, *Damage and Computer Offences: Discussion Paper, Chapter 4*, Commonwealth Attorney-General's Department, Canberra.

National Office for the Information Economy and the Australian Computer Society 2000, *The Phantom Menace: Setting the Record Straight About On-Line Credit Card Fraud for Consumers*, National Office for the Information Economy and the Australian Computer Society, Canberra.

O'Brien, Chris 2000, 'The Next Revolution?', *The Age(Melbourne)*, I.T.(2), 27 June, p. 1.

Office of Fair Trading 1998, 'Internet Scams Deleted, Sweep Identifies 'Get Rich Quick' Schemes', *Fair Trading Magazine*, Spring, Office of Fair Trading, London.

Office of Strategic Crime Assessments and Victoria Police 1997, *Computer Crime and Security Survey*, Attorney-General's Department, Canberra.

O'Toole, G. J. A. 1978, *The Private Sector: Private Spies, Rent-A-Cops, and the Police-Industrial Complex*, W. W. Norton and Company Inc., New York.

Philippsohn, S. 2000, 'An Overview of Electronic Crime in the 21st Century', *Intersec: The Journal of International Security*, April, http://www.afp.gov.au/ecrime/21c.htm (visited 16 January 2001).

Sussmann, M. A. 1999, 'The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium', *Duke Journal of Comparative and International Law*, vol. 9, no. 2, pp. 451-89.

Tendler, S. and Nuttall, N. 1996, 'Hackers Leave Red-Faced Yard with $1.29m Bill', *Australian*, 6 August, p. 37a.

Thompson, D. P. 1996, 'Pablo Escobar, Drug Baron: His Surrender, Imprisonment, and Escape', *Studies in Conflict and Terrorism*, vol. 19, pp. 55-91.

United States, Department of Justice 2000, *Internet Fraud: Appendix B*, Report of the Criminal Division's Computer Crime and Intellectual Property Section http://www.cybercrime.gov/append.htm (visited 5 July 2000).

United States Department of Justice and Federal Bureau of Investigation 2001, 'Internet Fraud Complaint Centre', http://www.ifccfbi.gov/ (visited 16 January 2001).

van Kesteren, J., Mayhew, P., Nieuwbeerta, P., and Bruinsma, G. 2000, *Criminal Victimisation in Seventeen Industrialised Countries: Key Findings from the 2000 International Crime Victims Survey*, ICVS Working Group, Vienna.

Victoria Police and Deloitte Touche Tohmatsu 1999, *Computer Crime and Security Survey*, Victoria Police Computer Crime Squad and Deloitte Touche Tohmatsu, Melbourne.

Walker, J. 1999, 'How Big is Global Money Laundering?', *Journal of Money Laundering Control*, vol. 3, no. 1, pp. 25-37.