14th BILETA Conference:
"CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

'Between the risk and the reality falls the shadow': evidence and urban legends in computer fraud

(with apologies to TS Eliot)

Dr. Michael Levi
Professor of Criminology,
Cardiff University

Introduction

The definition, harmfulness, incidence and prevalence of computer-related crime continue to be controversial. The unifying theme around cyber-crime as an issue seldom amounts to more than a claim to be late or post-modern. Sceptics traditionally argue that much of what is described as computer crime is crime that would not have been significantly harder had computers never been invented but although, as I shall argue, that may be true of *conceptual* categories such as trespass, theft, obscenity and violence (Wall, 1998: 203), it is undoubtedly true that computers – and especially the Internet - democratise criminal opportunities by opening up the possibility of virtual access to sites such as financial and defence systems that would not be available physically to many offenders. (For an excellent introduction to this aspect, see Mann and Sutton, 1998.) Even if we were to agree on a definition of the phenomenon, given non-reporting and - even when reported - the difficulty of fitting the crime to existing legal categories, our understanding of when and where 'it' occurs is very limited. Indeed, Wall (1998: 203) goes so far as to assert that "it is …too early even to attempt an assessment of the extent of cybervictimization, indeed, there are many good reasons as to why this might never be possible." Whilst I agree that this is so in the round, this paper sketches out some brief perspective on the emergence of computer fraud as a social issue and then goes on to examine what surveys to date tell us about its incidence and prevalence. I will *not* examine what the legal implications of this are, because there is no reason why the legal framework of fraud and attempted fraud should not cope adequately, though evidential issues may be far from easy.

It is not my aim here to examine policing of cyber-crime. Suffice it to state that electronic activities seem to have been grafted onto existing steam-age and pre-steam age roles. In the UK, for example, we have several Fraud Squads dealing with Internet pornography: why? Because in forces into which PCs have barely been introduced, Fraud Squads are the only specialist police units which deal with electronic transfers and with documents held on computer which often have to be tested, and with 'mirror-imaging' computer disks to search for deleted files: therefore officers have at least a modicum of computer literacy. Moreover, dealing with Internet porn helps to convince the police hierarchy that fraud squads serve a socially valuable function: a social value that they only intermittently see in dealing with white-collar crime (Levi and Pithouse, forthcoming).

I commence in this way to contextualise how antediluvian the interests of both police and academics are. Automatic Fingerprint Recognition and the Police National Computer excepted, the mainstream policing activities of public order and policing juvenile crime and petty persistent adult crime – from ‘broken windows’ upwards – lie outside the scope of ‘digi-crime’; and most police (and researchers who – in biological rather than pejorative terms – are parasitic upon their activities) can go through their entire careers without needing to know anything about its subject matter. Nevertheless, anyone interested in drugs dealing, fraud, the transmission of pornography, trans-national crime, money-laundering and the policing methodologies such as electronic eavesdropping that often accompany them has to have some comprehension of the impact of electronics and computing. This is not *just* the top slice of crime, for even street dealers are able to frustrate easy ‘analogue’ eavesdropping by using digital phones that require different, easier methods for interception but are harder to decrypt. This is merely one example of how technology can alter opportunities for crime concealment, though not necessarily crime commission itself, except insofar as it alters the risk/reward ratio for potential offenders. The extent to which such activities are *policed* is outside the direct framework of this paper, though it is dealt with elsewhere (Wall, 1998; Mann and Sutton, 1998).

The media and the social construction of computer crime

What follows is intended to be suggestive rather than a systematic analysis of media coverage of ‘computer crime’. However, it is useful to set ‘the problem of cyber-crime’ in a social context, since seriousness is not – or certainly not *always* – a natural categorisation process but rather an interaction between active interpreters of messages and ‘infotainment’ groups conveying them, sometimes at the behest of pressure groups seeking to communicate a particular vision of ‘the problem’ (see Hall, 1994). In constructing forms of crime (and even, arguably, crime in general) as a ‘social problem’, the media both create and reflect conceptions of seriousness. Different groups advocate particular conceptions that serve their material and symbolic interests, though to ‘expose’ these interests tells us nothing about the ‘truth value’ of their statements about the ‘scale of the problem’. The normal methodological tools of victimisation surveys and self-report studies are only beginning to be tapped, and a current dilemma is whether to take on trust official assertions or simply to discredit them without any further substantiation. How, for example, does one evaluate statements by computer security experts that events happened when they refuse to give details either about dates or the corporate identity of victims? In practice, the media give credibility to elite claims about prevalence, incidence and harm, though defence expert witnesses such as Peter Sommer – the author of the original Hacker’s Handbook - may receive a fair hearing, especially in liberal newspapers such as The Guardian and in the specialist press. It is not suggested here that computer criminals are demonised in the same way as are black people, for computer *use* does not permit the sort of simplistic physical ‘out of place’ definitions of colour and demeanour as does the topography of urban travel. Anti-counterfeiting groups, in particular, have difficulties in raising the seriousness perceptions of copying software, since many ordinary people find nothing wrong in making extra copies of ‘overpriced’ commodities: they therefore have to resort to allegations about the links between counterfeiting and ‘organised crime’, hoping that the negative image of the latter will contaminate all the activities they touch.

It is important to appreciate the interaction between ‘findings’ and news values. Reports on fraud by Parliamentary bodies, accountancy firms, commercial security firms, and individual experts can command attention if they assert that the problem is a serious and growing one. For example, if the Ernst & Young surveys of fraud against large companies – discussed later - had found high levels of ‘computer fraud’, this fact would have been heavily publicised in both specialist and general news media, since the revelation of large amounts of previously undetected hi-tech crime would be very newsworthy. The fact that the surveys did not find widespread computer fraud was unattractive to the media, in spite of (or because of) our efforts to suggest that the computer issue contained an element of ‘hype’ and that ‘the human factor’ and corporate cultures were more significant in accounting for fraud. (This was echoed by the Audit Commission, 1994.)

More generally, from the BBC television series The Consultant and the Disney movie War Games to mid-1990s films such as The Net and Goldeneye, 'computer crime' is used as titillating entertainment which generates fear at the power of technology beyond the control of respectable society. In newspapers, also, the ready market for stories involving young 'hackers' remains: in September 1991, prominence was given to the son of an Israeli guided missile expert who allegedly had hacked into Pentagon computers and into the Visa International credit card network. The most substantive error in the front page headline in The Independent was that he had not hacked into the Visa network but into the credit reference agencies' network: a rather significant difference. Even had he got into the Visa network, the implication conveyed to readers that untold riches would have materialised would have been mistaken, since funds transmission has nothing directly to do with either the Visa or the credit reference agencies' network. The Independent also ran stories during 1994 exposing the vulnerability of private information about senior British politicians and military personnel via the British Telecom network, which, despite some implausibilities, seemed to stack up. Likewise, though speculative and exaggerated, there was a kernel of truth in the threats of computer hacker extortion publicised in the Sunday Times (2 June 1996).

One way of enhancing crime seriousness is to associate the activity with 'organised crime' or 'organised criminals' as if, merely by being organised by a syndicate rather than one or a small group of professional criminals or anarchic 'pranksters', that made the impact much worse. This is an arguable point, though under some circumstances, people outside traditional crime groups may be regarded as a less manageable risk and therefore more dangerous even than gangsters. Where technology can be added to gangsterdom, this makes ideal media copy. Illustrations include the Russian technician who hacked into Citibank's phone lines and diverted millions of dollars in 1995 – made into at least one excellent television documentary and endlessly re-cited - and the over-hyped tale of an ATM fraud plot described below. The Independent (18 December 1996) caught even the broadsheet mood :

> John 'Little Legs' Lloyd, an underworld hardman, and his partner Kenneth Noye, wanted for the M25 road rage murder, hand-picked a team of criminals to pull off an £800m fraud....
>
> The gang was thwarted by an unlikely crime-busting team, made up of a softly spoken prison chaplain and a computer wizard who once tried to burn his wife and child to death.
>
> The swindlers' plan had been to use the help of corrupt British Telecom technicians to tap into the telephone lines which link cash dispensers to bank computers. The taps would have given the gang access to confidential information about tends of thousands of accounts which was to be downloaded onto a computer. The data would have been decrypted and transferred to 140,000 plastic bogus cash cards.
>
> Lloyd...and Noye had established a world-wide network of criminals to carry out fraud on a global scale.

By contrast, in The Times of the same day, the well-informed Stewart Tendler told readers that 'Noye was never questioned about the cashcard plot and detectives now say they believe he was only peripheral to the plot'. One can readily query terms like 'hand-picked': how else would one pick a criminal team? And note the 'Little Legs' cue that we are not dealing with a member of the social élite here! Lloyd was sent to prison for five years.

The BBC1 television 'infotainment' programme Here and Now was similarly obsessed with the ease with which plastic card numbers could be re-encoded and used for fraud, despite evidence that it accounted for only a small proportion of plastic fraud (BBC, 21 April 1997): a ‘good prog’ is one that alarms the public and attacks the competence of large institutions. The publicity accorded to many hacking scares - such as the vulnerability of most pager messages in Britain to simple hacking and recording (What Cellphone, November 1996 and several national newspapers) - serves to generate fear of crime and, perhaps, mislead readers into believing mistakenly that ‘the fraud problem’ is technological and external rather than social and internal. This applies especially to cyber-warfare stories, such as ‘Hackers attack military satellite’ (Daily Telegraph, 4 March 1999), which did at least go on to point out that there was no evidence of intent to blackmail or disable. There are occasional debunking stories, such as ‘More Naked Gun than Top Gun’ (The Guardian, 27 November 1997), which deflated US cyber-warriors’ claims about their methods and the threat posed by two British hackers, and ‘The hacker who turned himself in’ (The Guardian, 26 March 1998): but the general tone is hysterical and ‘deviance-amplifying’.

Disputes about harmfulness are part of the ideological terrain over which defendants and prosecutors battle. According to Sterling (1993), the FBI systematically misrepresented the organised nature of the hacking ‘group’ called ‘Legion of Doom’ and their involvement in crime: in reality, he argues, they did not steal or crash anything. Such battles over social definitions of social harm are not restricted to computer crime, but they are particularly salient to whether those hackings that do not involve pecuniary gain for the perpetrator but may involve substantial pecuniary loss for the victims (and those using allied systems, should they hear about the penetration) should be defined as serious crimes or as what – in the delinquency literature – might be termed ‘play vandalism’. This is especially problematic when many companies and governments themselves hire hackers to test the vulnerability of their systems to penetration: arguably, provided that they leave a trace calling card, free-lance hackers are doing for free what the institutions would otherwise have to pay for (except that they are people who might otherwise not be authorised to see the material they see). During 1998, one of a pair of British hackers – the other was acquitted – was given only a modest fine by a judge, in spite of a Pentagon official giving evidence that his activities could have undermined the entire US military defence system. So was this judgement sound, or did it fail to appreciate a ‘clear and present danger’ or a plausible future risk?

A nice illustration is the Israeli teenager Ehud ‘The Analyser’ Tenenbaum - a member of a group dedicated to fighting racist and paedophile Web sites – who hacked into NASA and Pentagon computers, before hacking into the Home Page of an FBI officer to tell the FBI that he was the one the 47 FBI agents were looking for. Prime Minister Netanyahu described him as ‘damn good’, but a director of Internet service provider Net Decks stated that ‘The Analyser is a vandal, not a hero’. Though the Americans certainly took the opposite view, the Chair of the Israeli Parliament Science and Technology committee observed in re-integrative mode – after all, Ehud was looking forward to joining the Israeli army very shortly - (The Guardian, 26 March 1998):

> He didn’t cause damage but rather exposed flaws in terms of the protection of important computer information….his huge amount of knowledge should be used to help the state, but this time in accordance with accepted rules and standards.

His activities required all passwords to be changed at Western Michigan University, and hundreds of (expensive) hours of repair work. Due to other hackers, for most of October 1997, two overseas US State Department posts had almost to be disconnected from the global network, since hacker traces made them insecure. A 1998 study by the General Accounting Office revealed that computer hackers could obtain data such as the travel schedules of US embassy officials - useful for assassinations – while the US Computer Security Institute survey found that 72 per cent of respondents from government and business stated that they had suffered financial losses from electronic criminals. In 1996, the Pentagon reported that there had been some 250,000 attempted hackings, only one in 250 of which had been detected at the time: but it is difficult to estimate the economic cost of these attempts other than the cost of security, which I have omitted here on the grounds that security costs are not strictly costs of crime but are costs of doing particular sorts of things about crime.

Nevertheless, such an omission has its flaws, insofar as security may be necessary in order to enable an entity to function at all: a good illustration of this is the simulation of warfare in hacker changes to the communications of defence satellites (Daily Telegraph, 4 March 1999). The key point is that these attempts are integrated into the necessity to spend billions on fighting cyber-terrorism, one of the major issues mentioned in the 1999 Clinton 'State of the Union' message. They are also related to battles over encryption and the 'need' for the law enforcement/intelligence agencies to retain access to telecommunications without the need for slow and expensive decryption.

More pragmatically, new forms of technology can also be used to point up the 'need' for changes in criminal law, such as the absence of preventative legislation to stop false claims being advertised on the Internet. In 'Internet sting lures 82,000 isle "lairds"', The Observer, (10 March 1996) warned about a firm selling square-yard plots of remote crofting land to Americans with a fictitious scroll guaranteeing that for $100, purchasers will become 'an authentic Scottish laird'. The article began: 'In cyberspace no-one can hear the victim scream'. This is part of the general advisory role of the media, but it also reflects the technophobia that is prevalent whenever risks of new technology are exposed (see also Mann and Sutton, 1998; Grabosky and Smith, 1998; and Levi and Pithouse, forthcoming, ch.2).

Finally, it should be appreciated that there is a serious social point about the interaction between computers, trust and security. As Grabosky and Smith (1998: 47) put it,

> [T]rust and confidence in the systems that support commerce, communications, air traffic control, electric power generation and other modern institutions are at the very core of our society. Thus, even the potential for disruption and harm is cause for concern.

The extent of computer fraud

In activities such as computer crime, alongside 'organised crime', the normal disciplines by which we evaluate the plausibility of threat levels are absent, for – as in other arenas of white-collar crime (Levi and Pithouse, forthcoming)– the victims are

1. Not asked about victimisation;
2. Do not respond when asked;
3. Do not tell us about all their experiences (or so we believe); or
4. Are unaware of their victimisation.

Grabosky and Smith (1998: 8) approach this 'harm measurement' issue with some delicacy:

> Quantification can also be deceptive….Often these [financial losses] amount to billions of dollars….Some estimates need to be treated with caution, however, since they are based on figures extrapolated from relatively small surveys to represent losses suffered by industries which have an enormous customer case and daily deal in turnovers amounting to vast sums of money….However…there are abundant examples of substantial and quantifiable sums being stolen throughout the world.

They add that qualitative dimensions are also important, not least because hackers may inflate their achievements. These statements are true as far as they go, but this does not address the deeper problem that official sources may deliberately or paranoiacally inflate the threat and may conflate *experience* of with theoretical *risk* from computer crime. This is not simply the attempt to gain more resources acknowledged (p.8) by the authors: it is part of the intelligence threat-assessment mental set, encouraged also by the 'concerns' (a.k.a self-serving PR) of security consultants whose income depends on shocking (or as they put it, 'creating awareness among') senior executives and government agencies who complacently fail to spend 'enough' money on security.

Unlawful (and lawful) major transfers of funds almost invariably involve a financial institution as intermediary, if not as a victim, of fraud. The definition, incidence and prevalence of computer-related crime continue to be a matter of much debate, in which diverse phenomena such as hacking for fun or espionage, theft of computer equipment, counterfeiting of software, criminal damage, blackmail and fraud become intertwined in a single gestalt. Sceptics traditionally argue that much of what is described as computer crime is crime that could have occurred even if computers had never been invented, though the process of money transmission would have been slower. Even if we were to agree on a definition of the phenomenon, given non-reporting and - even when reported - non-recording of such alleged crimes by the police, our understanding of when and where 'it' occurs is very limited. The Audit Commission (1983) states: 'computer fraud is any fraudulent behaviour connected with computerisation by which someone intends to gain dishonest advantage'. But there are wide variations in definition, which we will not address here.

It is important to think through whether what we are concerned with is corporate (and national security) loss or corporate/individual/governmental fraud. The latter speaks to traditional criminal law notions of blameworthiness and the precise allocation of blame to individuals; the former speaks to harm reduction and prevention, irrespective of whether anyone is blameworthy in a way that fits into the curious categories of the criminal law. Thus, for example, faulty ambulance dispatch systems or car safety measures can be looked at from a preventative perspective without necessarily seeking simply to fire or prosecute the personnel involved. In the light of this sort of consideration, the Audit Commission has shifted its focus to 'computer abuse', which it describes (1994: 6) as

> an umbrella term embracing various types of deliberate criminal acts, each of which calls for different skills and techniques in detection. The term embraces computer fraud, virus infections, hacking, theft of data and programs, sabotage, unauthorised private work, invasion of privacy, and unauthorised use of illicit software.

All of these may be subject to shifts in awareness, as different methods of tracking people and their activities highlight a greater proportion of the 'dark figure' not only of unreported but of unperceived 'abuse'. (A return to the 1983 definition would artificially reduce 'computer crime'.) Fraud includes:

- unauthorised input or alteration of input
- destruction/suppression/misappropriation of output from a computer process
- alteration of computerised data
- alteration or misuse of programs (but excluding virus infections).

The Audit Commission's sample includes all local authorities and National Health Service bodies in England and Wales; the majority of central government departments and agencies; and a 'range of middle- and large-sized companies throughout the UK' (1998: 5), though the response rate from each sector or in aggregate is not specified. Taking all forms of IT fraud and abuse together, the proportion of respondents who were victims rose from 36 per cent in 1994 to 45 per cent in 1997. But the proportion of respondents who reported experiencing fraud fell from 10 per cent in 1994 to 8 per cent in 1997, though the average value of frauds rose from £28,000 to £35,000, making total losses identical. In 1997, input frauds constituted 70 per cent of all frauds by volume. A quarter of all frauds detected were committed by management.

Thirty-seven 'computer fraud' cases were reported in 1994-95 to the Treasury (1995: 6) in its survey of internal fraud against government departments, though most were low value or no loss, only two being over £10,000 (of which one was over £60,000, with more being attempted). However, in a further case, a staff member approached a departmental debtor and offered to clear his liability by manipulating records, in exchange for £50,000 (less than half the debt). However, the debtor contacted the police who taped a subsequent conversation, and the civil servant was jailed for attempted corruption. Far heavier losses were generated by the theft of computer hardware and memory, as professional criminals in the mid-1990s targeted computer chips, which were in short supply following the destruction of a major factory in Kobe, Japan due to the earthquake there, and due to the growth in demand for memory to run Pentium processors and Windows 95 applications.

Since there is so much disagreement about the definition of computer crime, it is hardly surprising that there is little consensus about its cost. If we take telephone fraud, for example, what is termed 'shoulder-surfing' - i.e. looking over someone's shoulder while she or he is punching in their credit card code, and then selling it on cheaply to others - costs the phone companies more than any hi-tech methods of hackers (Sterling, 1993: 49). The ongoing war of computer fraud prevention resembles that which has occurred with safes, making safe-breaking virtually defunct. The chips on cellular phones can be reprogrammed to generate a false 'caller identification', to avoid billing, tapping by the police, and any other unwanted activities. The cost of the theft of long-distance service is in some sense theoretical (though the opportunity cost is real where a significant proportion of the calls would have been made anyway through the official system), but when stolen codes have to be deleted and new ones issued, this is a real cost, as is the trouble for real owners: there are analogies here with plastic card fraud generally, even when the bank pays up.

Some UK data also exist on the prevalence of computer fraud against large private sector organisations (Levi and Pithouse, forthcoming). The Ernst & Young 1986 and 1989 reports showed that whereas in both the questionnaire and the telephone surveys, executives expressed considerable concern about computer fraud and hacking, responses revealed that if we exclude simple forgery of input or output documents - which can be effected quite adequately without a computer - only one 'worst fraud' was a 'real' computer fraud that relied totally on the new technology. Even in a later section of the questionnaire that dealt with unreported as well as reported fraud, there were no computer frauds by outsiders, and no computer fraud by users and systems people exceeded £1 million in any case in our sample. Although more than two thirds of companies stated that computer viruses and hacking were fairly serious or very serious, only eleven per cent had experienced either of these and five per cent both of them.

In 1991, as in previous years, computer frauds again featured very modestly. Only one was committed by systems people - and that was under £10,000; only three - one under £10,000, one £10-100,000, and one over £100,000 - were committed by computer users; and none were committed by outsiders. The number of computer frauds was significantly lower than in 1989, which may be an artefact of responses or may reflect the success of computer security people in selling their message. Finally, our international surveys in 1996 and 1998 (Levi and Sherwin, 1996, 1998) turned up very few cases of reported or unreported computer frauds. In making these remarks, we are not debunking the cost to firms of protecting their systems against unlawful use by outsiders of insiders: actual and potential damage to data, for example, can be catastrophic for the operation of computer-dependent businesses and can provide the basis for corporate blackmail in exchange for unravelling the damage (Sunday Times, 2 June 1996), but this 'cyber-warfare' is different from fraud risks.

The same difficulties apply to American studies of computer crime. The 1998 Computer Security Institute/FBI study found that based on 520 security practitioners' responses (a 13 per cent response rate), 64 per cent had suffered security breaches in the previous year, at a cost (for the less than half who replied) of $136.8 million. (If one includes those experiencing computer viruses or laptop theft, the proportion victimised rises to 88 per cent.) The cost of financial fraud (against those who could quantify this loss) was stated to be $7.87 million, and telecommunications fraud $17.3 million (with a combined 2 year cost of $35 million): a far cry from the claims of private sector specialists, and less than one fifth of the total imputed cost of computer crime (Computer Security, 1998). The Internet connection was equal to the internal systems as a frequent point of 'attack', with over a half citing it. However, only 15 per cent reported financial fraud, the remainder comprising unauthorised access by employees (44 per cent) and denial of service attacks (25 per cent).

A recent survey by Barnes and Sharp (1998) found that technology was identified very seldom by insurance (6.3%) or retail (13.6%) sector respondents as a cause of the rise in fraud, largely because those sectors were exposed more to thefts and false claims outside the cyber-sphere. By contrast, 42.9% of services and of oil & gas sectors attributed the rise in fraud to technology. Whether correct or incorrect, this at least focuses us to more finely tuned analysis of risk by the nature of the activities.

Telemarketing frauds, stock price manipulation via Internet 'chat group' demand stimulation of interest in lawfully quoted securities, and advertising of offshore investments to tempt the needy and greedy are all methods by which remote persons can commit frauds with even less human contact and risk of arrest than in normal frauds: they also alter the 'capable guardianship' component of fraud prevention. Modern technological changes such as call-forwarding also assist telemarketing and investment fraudsters by enabling them to give as their ostensible phone number one in upmarket areas of London, Miami and other major cities, combined perhaps with an accommodation address there: but in reality, all calls are forwarded instantaneously to some other location, for example offshore in some difficult-to-penetrate offshore finance centre, without the knowledge of the communicators. But notwithstanding the vast estimates offered in some countries like the US (and some huge individual cases involving $200 million of which we are aware), there are no reliable estimates of the aggregate cost to individual or corporate victims. In short, we are not suggesting that concern about computer crime is irrational: on the contrary, we agree with Grabosky and Smith (1998) and with Mann and Sutton (1998) that computer security is going to be a major issue in the 21st Century. However, the term must be unpacked into sub-types of crime and we believe that concern about computer fraud should normally be less than concern about (i) many other types of fraud, and (ii) other types of computer crime.

Preventing cyber-fraud

Contrary to the beliefs of Grabosky and Smith (1998), general education about the consequences of computer crime is unlikely to have much impact on inhibiting either destruction, economic, or mischief motivations. By definition, the programmers and operatives of the future are part of the general public, but as with fire-setting and some of the more exotic forms of drug-taking, remote consequences are very difficult to re-educate people about (see Mann and Sutton, 1998). That is, even if one is optimistic about the *possibility* of weaning people away from the sociopathy of their relations with the large, impersonal institutions of late modernity.

Where there is no doubt at all is that the criminal justice process is ill-suited (and inconsistently so) to dealing with these forms of crime, prevention itself is tough

1. first, because of modest disapprobation among the set of potential abusers – and I would like to see some contextualised research on this looking at sub-group attitudes and social self-regulation;
2. second, because for all the scolding (Grabosky and Smith, 1998: 63) about the importance of controlling public information about telecoms systems, *some* systems information will inevitably leak out and may well be posted on the Net rather than kept to oneself as, arguably, a rational *economic* criminal would do;
3. third, because of the continual increase in processor power, which enables unlawful decryption as well as other explorations to take place under circumstances that would have required a massive capital outlay; and
4. finally, because it is hard to prohibit criminals from the market, as can be done in some areas of white-collar crime or, increasingly via the civil law (Bamfield, 1998), from stores or even private shopping malls (making intrusion burglary). However, the damage caused even by *individual* acts of computer fraud or vandalism may be entirely disproportionate to offenders' assets and income, far more so than in shop theft or fraud.

Another important theme is the relationship between risk, fear and technological change. It is asserted (Grabosky and Smith, 1998: 75) that because of high crime risks, consumers may be reluctant to take up new technology and producers may be reluctant to develop it. This is a concept that would benefit from further development. 'Fear of crime' is fairly well studied (though often under-theorised) in the settings of conventional crime against individuals and business, but not where purchasing products is concerned. For example, until recent improvements, the Internet was a very insecure place over which to give credit card and other personal details, yet many people happily gave away such details, just as they do when ordering goods and services by mail order or on the phone. To what extent does convenience (or relative convenience) overcome fear? Despite publicity given to consumer claims that their accounts have been debited by 'Phantom Withdrawals', most people use ATMs (though they have little choice, given bank opening hours): are they not fearful, and what would it take to make them fearful enough not to use these facilities?

Despite their initial caveat, the 'net effect' of Grabosky and Smith(1998)'s work and that of other authors in this arena is dealing with crimes by individuals against business and against individuals (a 'blue' collar crime study): there is only a modest amount on the ways that computerised bar coding can facilitate fraud *against* consumers, as the price may not correspond to that advertised (one sees the excuse 'programming error by junior staff' flashing before one's eyes), let alone the excellent possibilities for scams on investors by grossly oversold hype about hi-tech products and anti-trust activities by dominant suppliers (though these are not themselves inherently produced by *digitisation.* What we need to know is more about how the organisation of work under digitisation affects the possibilities of fraud.

BIBLIOGRAPHY

Audit Commission (1983) Computer Fraud Survey. London: HMSO.

Audit Commission (1994) Opportunity Makes a Thief: an Analysis of Computer Abuse. London: HMSO.

Audit Commission (1998) The Ghost in the Machine, London: Audit Commission.

Barnes, P. and Sharp, D. (1998) The Fraud Survey – 1998, Leicester: Association of Certified Fraud Examiners.

Computer Security (1998) '1998 CSI/FBI Computer Crime and Security Survey', Computer Security Issues and Trends, 4(1) 1-12.

Grabosky, P. and Smith, R. (1998) Crime in the Digital Age, New York: Transaction.

Hall, S. (1994) 'Reflections on the encoding/decoding model' in J. Cruz and J. Lewis (eds.) Viewing, Reading, Listening: Audiences and Cultural Reception, Boulder: Westview Press.

Levi, M. and Pithouse, A. (forthcoming) White-Collar Crime and its Victims: the Media and Social Construction of Business Fraud, Oxford: Clarendon.

Levi, M. and Sherwin, D. (1996) Fraud - the Unmanaged Risk: an international survey of the effects of fraud on business, London: Ernst & Young.

Levi, M. and Sherwin, D. (1998) Fraud – the Unmanaged Risk: an international survey of the effect of fraud on business, London: Ernst & Young.

Mann, D. and Sutton, M. (1998) 'NetCrime: more change in the organisation of thieving', British Journal of Criminology, 38, 201-229

Sterling, B. (1993) The Hacker Crackdown: Law and Disorder on the Electronic Frontier. London:

Viking.

Treasury (1996) Frauds against Central and Local Government, London: HM Treasury.

Treasury (1997) Frauds against Central and Local Government, London: HM Treasury.

Treasury (1998) 1996 - 97 Fraud Report. An analysis of reported fraud in government departments, London: HM Treasury.

Endnotes