International Association of Prosecutors
13th Annual Conference
New Technologies in Crime and Prosecution: Challenges and Opportunities

Singapore
27-31 August 2008

---

28 August 2008 -

PLENARY 1

EMERGING TRENDS IN CYBER CRIME

Nicholas Cowdery AM QC
Past President, IAP
Director of Public Prosecutions, NSW, Australia

INTRODUCTION

Cybercrime is not a new form of crime – it is a description applied to new ways and means of committing familiar crimes of various kinds, principally involving dishonesty, principally (but not exclusively) involving money and often (but also not exclusively) involving very old forms of crime indeed (such as theft). Many of these crimes are well known, their jurisprudence is well understood and they arise in this context mainly from human greed. Electronic ways of committing them, however, are new and modern crimes against the operation of computer technology itself are as new as the technology. Cybercrime as a means of offending operates in white collar crime, economic crime, intellectual property infringement, telecommunications crime and in the civil jurisdiction. The common feature is the use of information technology (computers) in their commission.

Even though the methods of prosecution and judicial disposition of cases of cybercrime are fundamentally no different from those for already established crime, novel practical challenges do need to be addressed by prosecutors. Conventional legal concepts continue to apply, but often there is need for the creation of specific new offences and new procedural rules (including evidence law) to enable an effective response to new methods of offending by the use of new technology. We need to respond to the emerging trends in cybercrime by developing our own trends in fighting it.

NATURE OF CYBERCRIME

I doubt that anyone here has not received an e-mail version of the so-called "Nigerian scam" or advance fee "419" fraud in one form or another. They are obvious attempts at commencing frauds that involve the use of the Internet, able to be committed once bank account and identity details are made known. That is a crude form of cybercrime

that plays directly upon the greed and gullibility of people both naïve and otherwise worldly.

Cybercrime has been defined as encompassing *"any proscribed conduct perpetrated through the use of, or against, digital technologies"*[1]. That definition says it all. It embraces three areas of activity.

- Crimes in the commission of which computers are used. These include online fraud and financial crime, the electronic manipulation of share and other markets, the dissemination electronically of offensive material, misleading advertising, identity theft and so on.
- Specific crimes committed against digital technology itself. These include "hacking", cyber stalking, theft of communication services and the transmission of malware – viruses, worms, Trojans, botnets, backdoors, phishing and so on.
- Conventional crimes attended by incidental cyber methods. These include encryption or steganography (the embedding of information in data) to conceal information relevant to other crime and the use of databases to store or organise information about criminal activity.

Some offending has elements of more than one of those divisions, such as the electronic transmission and perhaps covert storage of child pornography where real children are initially victimised. Another example is the all-too-prevalent use of computer chat rooms to groom and entice victims into illegal sexual activity with the offenders. Another example is to be found in the new offence called, colloquially, "upskirting" – where offenders use digital cameras to photograph up the skirts of women in public places and then disseminate the images.

The infrastructure of cybercrime is in computers, communications technologies and other networked services. It is sometimes known by other names, such as computer crime, or virtual, online, high-tech, Internet-related, electronic crime, and so on.

NATURE AND EXTENT OF THE PROBLEM

Victimisation surveys among populations consistently show a concern at the level of cyber offending. That concern is likely to increase as applications of digital technology expand. Already cybercrime accounts for more economic crime than any other type.

All that is needed to commence a cybercrime is a computer (with relevant connections, of course). This means of committing crime has been harnessed by everyone from enthusiastic (and sometimes young) amateurs to terrorists and with international drug and money traffickers, smugglers and criminal gangs in between. The bombing in Bali in 2002, for example, was financed by electronic transfers of funds from the Middle East to Bangkok, organised by a man here in Singapore. (A problem for investigators and prosecutors is whether any of those acts constituted an offence or offences? If so, where and under what law? And who should prosecute it?)

[1] "Cyber Criminals on Trial"; Smith, Grabosky and Urbas; Cambridge University Press (2004)

It is easy for cybercriminals to identify targets. For crimes using computers, databases of names and addresses and other particulars are compiled for a wide range of purposes and are sold or given away to persons who may wish to use them for criminal purposes. E-mail addresses may be obtained by other means. Targets are then contacted and inveigled into providing, for example, details of their bank accounts or personal particulars. The callers might even pose as government or bank officials seeking to "update" records and using designs on their messages that mimic genuine sites. Done by e-mail, this process is known as phishing. Means are then found for accessing those accounts and stealing funds.

In a case involving Carson City in California last year, nearly USD 450,000 was removed from the city's general fund by infiltrating into its systems a program that mimicked the computer strokes made by the financial officer and obtaining bank passwords by those means.

For crimes against computers, networking is all that is needed. Hacking and even ordinary, open access do the rest. There is a higher risk of acquiring malware by accessing movies and music than by visiting pornographic sites, for instance.

Even the best equipped law enforcement agencies are likely to be unable to deal with the growing volume of cybercrime even in their own jurisdictions[2].

Any increase in cybercrime must be considered in the context of the enormous and continuously expanding growth in the use of digital technologies. Just the capacity of digital storage media has grown exponentially in recent years. The average size of a hard disk installed in a personal computer has grown from 12 gigabytes in 1997 to well over 1,000 gigabytes now. The use of the Internet for financial transactions of many kinds (sales, transfers of funds for many purposes) continues to grow rapidly.

Continuing measurement of the extent of the problem and reporting of its incidence are essential. Only against that background can it be judged whether or not the investigation and prosecution of cybercrime are being conducted effectively.

INVESTIGATION

The investigation of cybercrime and the gathering of computer-based evidence encounter new problems. The expansion of data storage capacity has been mentioned. Even if investigators have a good idea of what they are looking for and a reasonable suspicion of where it might be, searches in digital memories may be hampered by the mislabelling of data (accidental or deliberate), encryption, storage in hidden directories or embedding in space that a simple file listing will ignore.

Evidence of a crime may be stored among other data that do not relate to the investigation. Prima facie the data may be protected by privilege or privacy laws. Evidence of a crime being investigated may be stored with evidence that discloses other offending. If information about the former is being obtained pursuant to a search warrant, evidence obtained about the latter may not later be admissible in a prosecution. These can become real issues for prosecutors.

[2] Interpol (2001), "Criminal Threats to e-Commerce"

If the data sought are in a networked system, the practical and impact problems that can arise from intervention by investigators can be serious.

Digital evidence may be readily damaged or destroyed. For example, an investigator on site may come across a system that is uncommon and inadvertently destroy data. A computer may have been booby-trapped by the operator (perhaps by a short program that requires a password to be entered at intervals, failure of which triggers deletion), so that a search will trigger the destruction of data. A "hot key" may be programmed, destroying evidence when a particular key is pressed. When a police officer knocks at the door, the button may be easily pressed and evidence lost.

Skilled hackers make use of the logical structure of the Internet itself to compromise systems and leapfrog between systems without leaving a trail, making it difficult (if not impossible) to trace them.

Locard's principle of exchange (that anyone or anything entering a crime scene takes something of the scene away and leaves something of themselves behind) does not apply generally to the cyber world. It might apply in some circumstances, but especially is it the case that most computer security systems currently used do not track, trace and generate legally admissible evidence through the systems designed into computers.

PROSECUTION – SOME ISSUES AND CONCERNS

Prosecutors become involved in the response to crime as the criminal justice process attempts to deter, incapacitate, punish and/or rehabilitate offenders. We are one part of the system and take on the principal role of proving the commission of offences to the satisfaction of the court on the basis of the material provided by investigators. (In some jurisdictions, of course, prosecutors have a role in the investigation process itself.) What particular matters do we need to be especially aware of when dealing with cybercrime?

Various approaches have been adopted to grapple with this ever-growing problem. At first prosecutors and criminal justice systems generally tried to squeeze new ways of offending into existing old offences proved by conventional means. Over time and in its conservative manner the law, in some jurisdictions at least, has come to address the conduct directly by the creation of new offences and the provision of new ways of proving them.

Some issues remain, however, and we continue to address them as the problems continue to be exposed.

RESOURCES

An important policy issue is the extent of the state's resources that should be put into investigating and prosecuting some of these offences, some of which may result in the loss of huge amounts of property, but some of which may amount to not much more than nuisance value. From the prosecutor's point of view, it is important that adequate financial and other resources are provided to enable prosecutions to be carried out effectively, fairly and in a timely manner.

TECHNICAL UNDERSTANDING

Continuing training (or "learning and development") for prosecutors in this area is essential. Prosecutors need to have enough knowledge and understanding of the issues they are addressing in order to do so effectively. (This conference is a good example of what can be done in this area.)

HARMONY OF LAWS

One important international issue is the obvious benefit in having the laws of countries mesh together to provide more effective and efficient ways of investigating and prosecuting cybercrime across national borders by mutual legal assistance of various forms. National governments also need to publicise their opposition to cyber-offending and cooperate with each other, in very public ways, to address the problem. Only then can some real deterrent value be obtained from law enforcement efforts.

In the UK there is newly enacted anti-fraud legislation that it is hoped will address technology fraud; but its effective implementation will require the cooperation of other jurisdictions, especially in extraditing people for trial. Many countries will not extradite their own citizens – that is not a new issue, but it has a particular relevance in global cybercrime. Internet and e-mail related scams cost UK citizens around 100 million pounds every year. Russia, Romania and African countries are commonly the homes of the scammers. Two new offences are directed particularly against technology crime: "obtaining services dishonestly" and "possessing articles for use in frauds".

In 2005 the USA passed the Anti-Phishing Act which added two new crimes to the US Code. One prohibits the creation or procurement of a website that represents itself to be that of a legitimate business and that attempts to induce the victim to divulge personal information with the intent to commit a crime of fraud or identity theft; the other prohibits the creation or procurement of an e-mail message that does those things with those intents.

Nations must modernise and continually update substantive and procedural laws and coordinate their efforts internationally to deal with evolving methods of criminal offending across national borders. Cybercrime provides a spur for action already under way to some extent in most regions.

JURISDICTION

Another question is the jurisdiction in which a prosecution should be brought, once an offender has been detected. Electronic impulses may cross many jurisdictional boundaries before hitting their targets or bringing about the responses they seek. A cybercriminal can sit in one country, route electronic communications through several others, commit a crime in another and park the proceeds in yet another. Offences may be committed in several countries along the way. Decisions may have to be made about where the perpetrator may be amenable to justice and what offence/s should be prosecuted, under what law (and where) in the general public interest. Practical considerations such as the effective obtaining of evidence may impact on those decisions.

General issues of jurisdiction also apply – is it sufficient that an act occurs in the jurisdiction; is a national subject amenable to the jurisdiction of his or her citizenship, wherever the offence occurs; and so on.

OFFENCE/S

Similarly, the choice of offence may be problematic. For example, should an offender be charged by reference to what is done or the effect it achieves – or for both? Are there more appropriate offences, or offences more easily proved, in one place or another covered by the offending? The selection and framing of charges from a course of offending pose other problems.

DEFENDANTS

Who is to be prosecuted? If several people are involved in the offending, should they all be prosecuted? Is there scope for obtaining the evidence of one against another? If so, how is that to be determined? (Again, these are not new issues, but they need to be viewed in new light in the context of cybercrime.)

Juveniles are empowered as never before by access to the means with which to commit cybercrime. Should they be dealt with any differently from adult offenders in this area? In North Carolina in the USA there was a proposal to require parental consent for juveniles to join MySpace.com and other social networking sites in an effort to protect them from sexual predators – but it might serve other subsidiary purposes, too. Would it be effective?

EVIDENCE

The obtaining and admissibility of evidence need to be considered. This is an area where careful consideration needs to be given to the procedural law of the place of trial and the procedural laws of the places from which evidence is obtained. For example, a prosecution in Malaysia might rely on evidence obtained from another country where search warrants may be given only for physical evidence and not for digital impulses. Is the admissibility of the digital evidence affected by the way in which it was obtained?

EXPERTS

It will often be the case that expert evidence will be required to explain structures and systems in the cyber world. Tests for the admissibility of expert opinion evidence may vary from place to place. In the USA the Daubert[3] test is applied. That requires that the following questions to be addressed.

1. Can the theory or technique be tested and has it been?
2. Has the theory or technique been subject to peer review and publication?
3. Does the technique have a high known or potential error rate?
4. Does the theory or technique enjoy general acceptance within the relevant scientific community?

It must be remembered that computer forensics is still really in its infancy (although there are many very competent practitioners).

[3] Daubert v Merrell Dow Pharmaceuticals Inc 509 US at 579

VOLUME OF EVIDENCE – DISCLOSURE
The prosecution's obligation of disclosure to the defence must be observed; but with huge volumes of potentially relevant digital evidence available, judgment must be exercised in every case. Disclosure must also be made in an acceptable electronic form.

We have had to grapple with this sort of issue for a long time, for example when there are thousands of intercepted telephone calls to be assessed; but we will confront it increasingly in the future.

ACTUS REUS AND MENS REA
Sometimes difficulties may arise in proving the required guilty mind for specific offences. In some cases inferences may be able to be drawn easily enough; but in others the proof of a specific intent, for example, may be uncertain.

DEFENCES
What defences have been thrown up by suspects? How can they be met?

VICTIMS
Who are the victims of cybercrime? Sometimes that can be answered easily, sometimes not.

SENTENCING
What are the appropriate punishments for this kind of offending? Because information technology is used in the commission of an offence, does that make it more or less serious than a similar crime committed by traditional means – or does it make no difference? How are the traditional purposes of punishment – deterrence, retribution, reform, incapacitation – measured against cyber-offending? How may corporate offenders be implicated and punished?

The theme of this conference makes reference to opportunities and challenges. The challenges are being placed before us in cybercrime on an ongoing basis and we are able to identify trends in our individual jurisdictions. It is up to us to help to develop the opportunities for combating it effectively – and, of course, efficiently.