TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 285 October 2004

Impediments to the Successful Investigation of Transnational High Tech Crime

Russell G. Smith

Technology has both facilitated and impeded the investigation of crime, particularly high tech crime involving computing and communications technologies. On the one hand, computers have enabled vast amounts of data to be searched and analysed quickly, and have permitted documents and files to be scanned and transmitted across the globe in seconds. On the other hand, the sheer quantity of information creates considerable problems for investigators who sometimes have to examine gigabytes of data and break encryption codes before the material they are interested in can be discovered. This paper identifies a number of barriers to the effective investigation of high tech crime across borders, and offers some solutions that could be used to streamline future investigations in cyberspace.

Toni Makkai
Director

AUSTRALIAN HIGH TECH CRIME CENTRE

ISSN 0817-8542

ISBN 0 642 53848 4

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends & issues in crime and criminal justice series, visit the AIC web site at:http://www.aic.gov.au

Throughout the world more and more instances of high tech crime are being investigated by law enforcement agencies, often by specialist high tech crime units such as exist in the United Kingdom, the United States and Australia. Along with this increase in workload has come the realisation that crimes involving computers—either as the target of offending, or as one of a range of tools, or the principal tool used in the commission of offences—are technically difficult to investigate and raise many unresolved legal and practical problems (Smith, Grabosky & Urbas 2004; Sussmann 1999). Concerns often arise because of the transnational nature of the conduct involved. This necessitates a degree of cooperation rarely required of investigators in the past.

This paper reviews seven barriers to the successful investigation of cross-border high tech crimes, and identifies policy responses that may be appropriate to deal effectively with these emerging global crime problems.

Identifying suspects

One of the first impediments that investigators face is identifying suspects. Occasionally, this can lead to considerable problems when the wrong person is arrested (see Box 1). In cyberspace, identification problems are amplified. Digital technologies enable people to disguise their identity in a wide range of ways making it difficult to know for certain who was using the terminal from which an illegal communication came. This problem is more prevalent in business environments where multiple users may have access to a work station and where passwords are known or shared, than in private homes where circumstantial evidence can often be used to determine who was using the computer at a given time.

Online technologies make it relatively simple to disguise one's true identity, to misrepresent one's identity, or to make use of someone else's identity. For example 'remailing' services can be used to disguise one's identity when sending email. This is done by stripping messages of

Box 1: Identifying suspects

In March 2003, the FBI was investigating a 72-year-old man in the United States in connection with an alleged telemarketing fraud involving millions of dollars. Since 1989, this man had allegedly been making use of the identity of a 72-year-old retired businessman from Bristol in the United Kingdom. The British man had never met the alleged fraudster, and had no connection with any of his alleged crimes. The FBI issued a warrant for the arrest of the suspect, naming the retired English businessman who was subsequently arrested by South African Police in Durban on 6 February 2003, while on holiday with his wife. The police relied on the fact that the warrant was in his name, he was the correct age, looked similar, and had the same passport number. He was held in custody at police headquarters in Durban, but was released on 26 February 2003 following the arrest of the real suspect in Las Vegas (BBC news 2003).

identifying information and allocating an anonymous identifier, or encrypting messages for added security. By using several remailing services, users can make their communications almost impossible to follow.

Anonymity can also be achieved in cyberspace using less technologically complex means. For example:

- using a false name when purchasing pre-paid internet access from an internet service provider and when renting a telephone line from a carrier;
- registering for a free email service using a false name and address; and
- using internet kiosks to send messages without disclosing one's true identity.

Even e-commerce technologies that make use of public key infrastructures and digital signatures can be easily manipulated by individuals presenting fabricated documents to support a false identity when obtaining a key pair from a registration authority for use in secure transactions. Although the subsequent transaction may be secure from hackers, the identity of the person holding the key may nonetheless be fictitious.

In a recent study of online anonymity, Forde and Armstrong (2002) argue that those internet services that provide the highest levels of anonymity are most likely to be used for criminal purposes. Encrypted email that provides a high level of anonymity was found to be preferred by those engaging in online paedophile activity and hacking, while the use of the world wide web and file transfer protocols which provide weaker levels of anonymity tended to be avoided by serious criminals.

Problems of identifying suspects are usually resolved by traditional investigative techniques. This might include the use of video surveillance, or gathering indirect circumstantial evidence to prove the accused was at a terminal at a particular time and day. However the use of intrusive surveillance is not always successful, and raises issues of human rights and legal privileges—problems which exist in both digital and non-digital environments.

Some investigators are beginning to use biometric means of identification. At present, few computers have biometric user authentication systems (for example, a fingerprint scanner for logging on). DNA samples may also be gathered from keyboards which have been used to identify an individual with a particular computer. When such techniques become more widespread, problems of identification may be reduced although, of course, once a person has logged on, this does not prevent someone else from using that terminal without the person's knowledge if they are absent. A further problem concerns the need to link the time at which a suspect was using a computer (as disclosed in computer forensic evidence) with biometric evidence of the whereabouts of the suspect at a given point in time, because DNA or fingerprints, for example, cannot be time-stamped.

Box 2: Extradition

In May 2000, a student in the Philippines was alleged to have sent out the so-called 'Love Bug' virus. This virus infected Microsoft Windows operating systems by sending email attachments which, when opened, damaged files in the computer and then replicated itself by sending similar messages to all the addresses in the infected computer's address book. The estimated damage caused was between US$6.7 billion and US$15.3 billion globally. The virus was traced to an Internet service provider in the Philippines who cooperated with police to locate the residence in question. The student was arrested, but the creation and release of a computer virus was not proscribed by Philippines law at the time. Because the conduct was not illegal in the Philippines, the principle of dual criminality precluded extradition to the United States where such activity was a crime (Bell 2002).

Criminal law and securing extradition

Where an accused person is resident in a country other than the one in which criminal proceedings are to be taken, it is possible for that person to be extradited to stand trial. However, the procedures involved in extradition are complex and difficult, making applications costly and slow. As the Commonwealth Director of Public Prosecutions (2003: 46) notes:

> there have been cases where an extradition request has been withdrawn because the delay has been so long that criminal charges can no longer proceed, and cases where a person has died of natural causes while contesting extradition.

Extradition requires not only that an appropriate treaty exist between the two countries concerned, but also that the conduct in question be criminalised in both the referring and receiving country. In the case of computer crime, this is often not the case.

For example, a survey of cybercrime laws in 52 countries in 2000 found that 33 of these countries had not yet updated their laws to address any type of computer crime (McConnell International 2000). Of the remaining countries, nine had enacted

legislation to address five or fewer types of computer crime, and 10 had updated their laws to prosecute six or more of the 10 types of computer crime identified. An example of the kind of difficulties that can arise is shown in Box 2.

Choosing an appropriate jurisdiction

One of the foremost problems facing high tech crime investigators is determining the jurisdiction in which proceedings should be taken. Where offences are committed in various countries, or where the offender and victim are located in different places, questions arise as to which court should deal with the matter. If charges can be laid in the country in which the offender is located, then problems of extradition will be avoided. But if the charges originate from the country in which the victim is located, or where the effect of the conduct occurred, then the offender may need to be extradited to that country. Importantly, it will often be the case that only some of the essential elements of the offence occur within one jurisdiction, making prosecution practically impossible.

The problem of 'negative international jurisdiction' also arises. This refers to cases that are not investigated because they could be prosecuted in one of many countries, but none wants to take action. There is also the reverse problem of too many countries wanting to prosecute a particularly noteworthy case. What may be needed to deal with this situation is the creation of an international instrument along the lines of the United Nations protocol on negotiating jurisdiction, setting out how jurisdiction is best determined in these cases. Generally, the rule is that if a country refuses to extradite an offender and it has power to take action, then it should be obliged to do so.

Search and seizure

Two methods of obtaining data from a computer system can be distinguished on technical and legal criteria:

- the first method involves obtaining data during a physical search of premises or the place where the computer system is located; and
- the second method involves the interception or monitoring of data being transmitted from, to or within the system.

This is an important distinction because remote access to computers via the internet can sometimes result in the search amounting to an interception of telecommunications that may require a warrant in order to be legal (see Box 3).

Difficult problems arise in obtaining digital evidence in high tech crime cases, although in some ways computers have made the process easier through the ability to conduct searches of hard drives remotely via the internet. Some of the main difficulties include:

- obtaining permission to conduct searches remotely—this is still illegal in Australia;
- securing the relevant access device, such as a password;
- imaging a hard drive without interfering with the evidence; and
- conducting searches quickly so that data cannot be removed.

Often transnational high tech crime operations need to be closely coordinated. Warrants may need to be simultaneously executed in different countries in order to ensure that suspects do not collaborate in the alteration or destruction of evidence. In recent years, police have been successful in mounting such operations. One case of online child pornography involved the execution of 30 warrants for 12 suspects in 10 different countries (US Customs Service 2002).

A final problem concerns the retention of material by investigators. If child pornography has been seized by police, they may be unable to return it to accused

Box 3: Search and seizure

Two Russian computer hackers who allegedly stole large numbers of credit card details and attempted to extort money from account holders were investigated by the FBI in the United States. In an undercover operation, FBI agents posed as representatives of a security firm and made contact with the accused, ostensibly to discuss employment prospects in the United States. The two accused demonstrated their hacking expertise for the agents who then invited them to come to the United States. While in the United States the FBI agents used a key logging program to discover the accused persons' passwords in order to get access to their computers in Russia. The suspects were then arrested and charged with various offences. In order to preserve the computer evidence in Russia, the FBI agents immediately copied data from the servers in Russia via the Internet prior to obtaining a search warrant in the United States. The defence raised various objections to this, arguing the search was unconstitutional as it breached the Fourth Amendment which requires warrants to be issued prior to searches being conducted. The court held that the Fourth Amendment did not apply to these actions as the data had been obtained outside the United States. The court also held that there had been no seizure of the data as it had merely been copied but not read prior to the warrant being obtained (*United States v Gorshkov* 2001 WL 1024026 No CR-550C; WD Wash 23 May 2001).

Box 4: Encryption

In a 1998 investigation of a paedophile network, Operation Cathedral, police in 15 countries uncovered the activities of the W0nderland [sic] Club, an international network with members in Europe, North America and Australia who used the Internet to download and exchange child pornography including real-time video images. The Club used a secure network with regularly changed passwords and encrypted content. In Europe alone, over 750,000 images were recovered from computers, along with over 750 CDs, 1,300 videos and 3,400 floppy disks. The encryption devices were circumvented because one member of the Club cooperated with police and provided access to the files. This led to approximately 100 arrests around the world in September 1998 (Australasian Centre for Policing Research 2000: 126).

persons as this would entail the illegal distribution of obscene materials. In the United Kingdom, the Possession of Unlawful Items Act could be used to enable police to dispose of child pornography that had been found on computers, but this is not yet in force (see also the English Police Property Act 1894).

Problems of encryption

A difficult problem facing high tech crime investigators concerns data that have been encrypted by accused persons who refuse to provide the decryption key or password (see Box 4).

Access to encrypted data may, alternatively, be achieved in some countries by installing a key logging program onto a computer to detect the password used for decryption. The installation of such a program, of course, must be done without the knowledge of the accused, and a special warrant must be obtained for this. In one case in the United States, evidence obtained by key logging was challenged on the grounds that it involved the illegal interception of wire communications. It was held, however, that the key logger only operated when the computer's modem was not connected, thus excluding any interception of telecommunications (*United States v Scarfo*, 2001—see www.epic.org/crypto/scarfo.html). In Australia, the Surveillance Devices Bill (No. 2) 2004 may, if enacted, enable police to apply for warrants to install key logging programs remotely. If all else fails, investigators may seek to break encryption codes, although this is difficult, time-consuming and costly, and would be inappropriate in all but the most serious of matters.

Some computer crime legislation is beginning to expand the range of investigatory powers available to law enforcement agencies, for example, by making it an offence for a person with knowledge of a computer system to refuse to divulge passwords or to refuse to provide information about encryption. The Australian *Cybercrime Act 2001* (Cth), for example, provides a maximum penalty of six months' imprisonment for failure to comply with a magistrate's order to provide such information to investigating officials (see s 3LA, *Criminal Code Act 1995* (Cth) and s 201A, *Customs Act 1901* (Cth)).

Mutual assistance

In order to facilitate international criminal investigations, use is often made of mutual assistance treaties. These provide a legal basis for authorities in one country to obtain evidence for criminal investigations at the request of authorities in another country. Instruments of this kind cover a range of activities including:

- identifying and locating persons;
- serving documents;
- obtaining evidence, articles and documents;
- executing search and seizure requests; and
- confiscating proceeds of crime.

Each year Australia is the originator of over 100 mutual assistance requests, and receives a further 100 requests by other nations pursuant to the *Mutual Assistance in Criminal Matters Act 1987* (Cth). At present, very few of these requests concern high tech crime, although as the prevalence of transnational high tech crimes increases the problems associated with using mutual assistance arrangements are likely to escalate. The central difficulty is the slow and cumbersome nature of official requests. There are also problems with the direct transmission of documents as mail can only be faxed in an emergency and to a court tribunal. It is also difficult to use direct requests for assistance unless the person seeking assistance knows specifically to whom the request should be sent.

Costs associated with mutual legal assistance are borne by the party providing assistance. This creates hardship for small countries that process many requests for assistance from large countries but rarely seek assistance themselves. This means these small countries are subsidising the legal process of much larger nations. In the case of large countries, other problems emerge. In the United States, for example, requests from around the globe for information concerning email accounts of companies such as Hotmail or Yahoo are dealt with by the FBI, which sends requests to corporate head offices located in the United States rather than local branches. This has the effect of over-burdening the FBI with the administration of such requests.

Obtaining evidence in high tech crime cases through the use of formal mutual assistance arrangements between nations can be exceedingly slow and ineffective. Often searches need to be conducted immediately in order to preserve evidence held on servers. The prospect of waiting weeks or even months for official diplomatic procedures to be complied with is daunting.

Logistical and practical barriers

Finally, conducting investigations across national borders raises many practical problems that delay matters and increase costs. In addition to the issues already referred to, some other problems include:

- investigators having to contact people on the other side of the globe at inconvenient times;
- documents having to be translated, particularly if required for diplomatic purposes; and

Box 5: Successful cooperative action

In March 2003, an Australian man was charged in the United States with one count of conspiracy to commit criminal copyright infringement and one count of criminal copyright infringement. The charges were in connection with his alleged involvement in an illegal Internet software piracy group founded in Russia in 1993 which operated globally. The group produced and distributed some US$50 million worth of pirated software, movies, games and music. Another 20 offenders have been convicted in the United States and others charged in the European Union in relation to the group's activities (US Department of Justice 2003).

- witnesses from non-English-speaking countries needing the assistance of interpreters, which can be expensive and can slow down investigations.

Countries also have different priorities in terms of the importance of high tech crime investigations. Economic crimes committed using computers may be at the bottom of the hierarchy in countries where, for example, violent crime is prevalent. The result is that requests for assistance in some cases may simply be given a much lower priority, especially if they have come from a country with no history of cooperative action.

Despite these barriers, cooperative action can nonetheless result in successful investigations, as occurred recently in Operation Buccaneer (see Box 5).

Solutions

How, then, can these problems be overcome? The solutions lie in harmonising laws and procedures globally, improving the technical capabilities of investigators, and finally in sharing information between public and private sector investigators to enhance international cooperation. The key strategies are summarised in Table 1.

Harmonisation of laws

The continuing harmonisation of laws and the adoption of international conventions on high tech crime and transnational and organised crime will make prosecutions easier and will greatly improve mutual assistance and extradition of offenders. Already this is starting to occur with the adoption in November 2000 of the United Nations Convention Against Transnational Organised Crime (which commenced on 29 September 2003—see http://www.unodc.org/unodc/en/crime_cicp_convention.html). Another recent treaty is the Convention on Cybercrime adopted by the Committee of Ministers of the Council of Europe on 8 November 2001, and which commenced on 18 March 2004 (see http://press.coe.int/cp/2004/135a(2004).htm). These conventions contain the following provisions:

Table 1: Impediments to high tech crime investigations and response strategies

Impediment	Response strategy
Suspect identification	Advanced technologies of user authentication and verification with issuing authorities
Criminal law and extradition	Implementation of treaties and harmonisation of high tech crime laws
Choice of jurisdiction	United Nations protocol on the determination of jurisdiction in cross-border criminal cases
Search and seizure	Legislative reform of powers of search and seizure and targeted use of warrants
Encryption of evidence	Legislative reform to compel disclosure of keys and to allow police to undertake covert key recovery activities
Mutual assistance	Streamlining mutual assistance procedures, increasing resources to agencies to respond to requests, and delegating requests to branch offices of organisations
Logistical and practical problems	Enhanced international cooperation and increased funding to expedite investigations

- criminalisation of certain conduct;
- the provision of special investigative techniques;
- witness and victim protection;
- cooperation between law enforcement authorities;
- exchange of information;
- training and technical assistance; and
- prevention at national and international levels.

The Australian Parliament has recently enacted the *Cybercrime Act 2001* which commenced operation on 21 December 2001. This Act inserts a new Part into the Commonwealth *Criminal Code Act 1995* and largely follows the provisions of the Council of Europe's Convention on Cybercrime. However, the Australian legislation applies only to certain federal law enforcement agencies and not to corporate investigators or private sector consultants who deal with the vast majority of Australia's high tech crime (Ghosh 2002).

Although the convention and the Cybercrime Act resolve problems to do with copying data from hard drives on premises and remotely, obtaining access to encrypted files and seizing aggregated data, questions still remain concerning the scope of warrants, data not held on the accused's premises, extra-territorial searches, and the scope of mutual assistance orders (Ghosh 2002). In addition, there is a need for as many countries as possible to enact local legislation in order to prevent safe havens from continuing to exist where criminals can base their operations.

Improving technical capabilities

The investigation of cross-border high tech crime also requires adequate forensic and technical expertise. This implies the formulation of training programs and the development of investigative software tools. International training programs could be developed and expertise could be shared between different nations. The United Nations, under its crime program, could examine the desirability of reviewing its manual on computer crime and further support the work already undertaken by other international organisations.

The level of funding required for training and also for upgrading equipment is not inconsiderable. This ultimately leads to an increase in costs associated with investigations. The result may be that in the future only large-scale criminal activities will be investigated (a problem that already exists in many countries).

One solution may be to share the investigatory burden between public and private sector agencies. Already, specialist high tech crime units have been established within police services in many countries. As these continue to expand they will become a repository of expertise that the private sector could use. One way in which this could be done would be for private sector personnel, such as bank investigators, to be located within high tech crime centres to help police with complex electronic banking matters. This is already being undertaken at the Australian High Tech Crime Centre. Similarly, law enforcement agencies are continuing to outsource specialist forensic tasks to the large accounting consultancy companies who often have former police-trained personnel working for them.

Sharing information

Finally, there needs to be greater sharing of information between investigators, within both the public and private sectors. This already occurs in the public sector but openness also needs to be encouraged in the private sector, even where commercial competitive interests may be at stake. Considerable expertise exists within global consulting and accounting practices, as well as industry bodies in telecommunications, finance and intellectual property. Their skills could be used constructively to supplement public sector law enforcement initiatives.

It is important at the outset for organisations to establish networks of information so that when an investigation begins, contact can be made immediately with the appropriate person in another country. Secure intranets, such as that used by the Australian Crime Commission (which now has jurisdiction over cybercrime) are an excellent way in which this can be achieved. Subject to the constraints of privacy legislation, these could be used in the private sector as well.

Initiatives such as the establishment of Europol in 1998, the G-8s High Tech Crime Group, and a Working Group on Information Technology Crime in the Asia-Pacific region have all been beneficial in sharing information across national borders, although at present coverage is somewhat limited. In Australia the Australian High Tech Crime Centre provides a coordinated means of responding around the clock to computer crimes, particularly those with a transnational component.

There is, accordingly, an extensive range of initiatives being undertaken to respond to high tech crime within Australia and globally. Armed with the latest information and techniques, investigators should be well placed to respond in a timely way to the vast range of challenges that high tech crime has created for the international community.

Acknowledgments

An earlier version of this paper appeared in the Council of International Investigators' *International Councillor* 2(18) June 2003: 17–19.

The author gratefully acknowledges the helpful comments of two anonymous reviewers and an officer of the Australian High Tech Crime Centre.

References

Australasian Centre for Policing Research 2000. *The virtual horizon: meeting the law enforcement challenges scoping paper*. Adelaide: Australasian Centre for Policing Research

BBC news 2003. Briton may sue after FBI bungle. *BBC news online* (UK edition) 26 February. http://news.bbc.co.uk/1/hi/england/2801673.stm

Bell RE 2002. The prosecution of computer crime. *Journal of financial crime* 9(4): 308–25

Commonwealth Director of Public Prosecutions 2003. *Annual report 2002–03*. Canberra: Commonwealth Director of Public Prosecutions

Council of Europe 2001. Convention on cybercrime. *European treaty series* no 185, Budapest 23 November 2001. Strasbourg: Council of Europe. http://conventions.coe.int/treaty/EN/projets/projets.htm

Forde P & Armstrong H 2002. The utilisation of internet anonymity by cyber criminals. Paper presented at the International Network Conference. Plymouth: University of Plymouth 16–18 July. http://www.cbs.curtin.edu.au/Workingpapers/other/Utilisation%20of%20Internet%20Anonymity%20by%20Cyber%20Criminals.doc

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

Ghosh A 2002. The Cybercrime Act 2001: implementing the European Union's cybercrime convention. Paper presented at the RSA conference San Jose 16–22 February

McConnell International 2000. *Cybercrime and punishment? archaic laws threaten global information*. http://mcconnellinternational.com/services/CyberCrime.htm

Smith RG, Grabosky PN & Urbas GF 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press

Sussmann M 1999. The critical challenges from international high tech and computer-related crime at the millennium. *Duke journal of comparative and international law* 9(2): 451–90 http://www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf

US Customs Service 2002. Operation Artus. Media release 20 March. http://www.usdoj.gov/criminal/ceos/OperationArtus.htm

US Department of Justice 2003. Defendant indicted in connection with operating illegal internet software piracy group. Media release 12 March. http://www.cybercrime.gov/griffithsIndict.htm

Dr Russell G. Smith is Principal Criminologist at the Australian Institute of Criminology

General editor, Trends & issues in crime and criminal justice series: Dr Toni Makkai, Director, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601

Note: Trends & issues in crime and criminal justice are refereed papers

The AIC is a statutory body with a Board of Management comprised of federal, state and territory government representatives, administered under the *Criminology Research Act 1971*