

**Parliamentary Joint Committee on the
Australian Crime Commission**

Inquiry Into Cybercrime

Submission No:29

Received 20 July 2003

Mr Greg Melick

Maurice Byers Chambers

Level 60 MLC Centre

19-29 Martin Place

SYDNEY NSW 2000

☎ 02 8233 0300 📄 02 8233 0333

E-mail:

Introduction

LAW ENFORCEMENT IN CYBERSPACE

Greg Melick

National Crime Authority, Australia

Introduction

1. International organised crime groups are also cashing in on the opportunities offered by the Internet and e-commerce. Internet crime is already a reality and tools such as encryption are finding practical application in the criminal environment. No doubt such encounters will be more common in the future.
2. Organised crime is now a global phenomenon, and organised crime entities are becoming increasingly sophisticated both in the way they operate and the crimes they commit. There is no doubt that in the future this situation will be perpetuated, if not exacerbated by technological advancements such as the Internet and electronic commerce. It is also clear that these groups are highly aware of criminal laws in various jurisdictions. They are not confined by jurisdictional boundaries, in fact they frequently capitalise on the lack of symmetry between jurisdictions both domestically and internationally.
3. The money trail is law enforcement's main entry point into organised crime. The difference now is the scale of which investigations must take place and the level of cooperation required with other law enforcement agencies, both within Australia and internationally to draw these investigations to a successful conclusion.
4. No country by itself can tackle organised crime. If we are to remain effective in the next century we must work not just with our own countries law enforcement agencies, but, through our international efforts, with agencies all over the world.
5. The Internet and electronic commerce in general has created enormous problems in law enforcement and it would be impossible to discuss even a few of such aspects in a comprehensive manner in this paper. However, I intend raising some of what I consider to be the more significant issues in the hope that they will contribute to some ongoing discussions in many jurisdictions.
6. There are many extremely useful references in relation to this topic and I list below three which I found particularly helpful, but it is important to realise that this is a global problem and it cannot be solved by jurisdictions acting alone.
7. The role of organised crime is to generate profits, whether it be by racketeering, prostitution, drug trafficking or electronic fraud. At the end of the day such activities will generate large amounts of cash (either in paper or electronic form) and criminal groups are always looking for ways to launder such proceeds, both from more traditional criminal activities and in the case of electronic crimes, to skim off such funds in a manner they cannot be traced.
8. Cyberspace also offers incredible opportunities to organised criminal groups to communicate with each other in a way that their communications cannot be intercepted and/or interpreted by law enforcement agencies. What I propose to do in this paper is to deal with the use made of cyberspace by organised criminal groups to launder monies, to examine some of the methods that can be used by criminal groups to prevent interception and/or interpretation of their communications, and then to consider some methods used in the commission of electronic crimes.

Money Laundering

9. Money laundering is a significant problem it having been estimated that approximately 3.5 billion dollars leaves the Australian economy on an annual basis. There is a very wide range of estimates of the size of the underground economies, as a percentage of GDP, for example, for Australia, 4-12 per cent; Germany, 2-11 per cent; Italy, 10-33 per cent; Japan, 4-15 per cent; United Kingdom, 1-15 per cent; and the United States, 4-33 per cent.
10. Law enforcement officers love cash. The smaller the better. Many successful arrests have been made and may

Introduction

networks disrupted or disbanded because of the difficulty connected with "laundering" large sums of cash. People are apprehended at barriers with suitcases full of it. They are detected when depositing large amounts of it into bank accounts prior to electronically transferring it overseas and because most nations deliberately adopt a policy of having the maximum size note commonly available in circulation of approximately \$100 is very bulky and difficult to deal with in large amounts. (Note that Singapore has a \$10,000 note and the largest denomination and the new Euro currency will be 500 Euros which will equate to approximately \$2,000 Australian.)

11. However, cyberspace is about to change this and make life very difficult for law enforcement officers. A lot of the changes are being pushed upon a commercial basis and obviously make good commercial sense except that at the end of the day if such a system creates a larger underground economy the very commercial system that is sought to be enhanced may well collapse. Accordingly, there needs to be a balancing of tensions between the commercial requirements of modern day commerce and law enforcement concerns.

Law enforcement's love of paper, whether it be cash or an audit trail has forced the entrepreneurial criminal to adopt other methodologies and electronic commerce offers a perfect alternative.

13. Typical recent comments in relation to this problem are as follows:

"It is very difficult for law enforcement to have all the resources they need to carry out the investigation appropriately and secondly, we do not have a common set of laws to deal with it," he said.

"Therefore the very smart crooks are employing unscrupulous lawyers and accountants and saying "where are the gaps in the law or what is the easiest way for me to get away with it?"

The question in many instances was where did the crime occur, what was the crime and whose laws were going to apply?"

"Interpol Secretary General Ray Kendall said his organisation had been pressing for years for cooperation with the private sector as technological advances made it clear crimes such as money laundering, electronic fraud and industrial espionage would boom in the Internet age. "Frankly, we are not prepared for this explosion", he said, "but the private sector will be able to move more quickly, directing finance to purchasing the necessary equipment to tackle the problem."

14. As all the participants of this seminar would be aware there are now many and varied ways of electronically conveying cash in such a manner as to ensure there is no (paper) trail for law enforcement agencies to follow.

"E-cash is designed for secure payments from any personal computer to any other workstation, over e-mail or Internet. The technique involves giving even very small payments of a few cents the level of security that was once reserved exclusively for large value wire transfers. Account holders visit a virtual ATM, authenticate ownership of an account and withdraw money directly from a bank account into an e-cash "purse". From this purse electronic payments can be made to one another or to on-line merchants. One advantage is that a large number of transactions can be dealt with at low cost, and a high level of security is provided to protect every 5 cent e-cash payment - the same that is routinely relied upon for authenticating requests to move huge sums between banks and even for national security.

"One significant feature is anonymity - the "blinding" carried out by the user's own device makes it impossible for anyone to link payment to the payer. Users can however prove that they did/did not make a particular payment without revealing anything more."

15. Stored Value (SVC or Smart) Cards cause concern such as noted at page 11 of the Report of the Electronic Task Force of the Commonwealth Law Enforcement Board: "The potential for the value to be passed from card to card and therefore person to person over the Internet without the intermediation of a financial institution has excited the interests of the law enforcement agencies and others". Whether this potential is realised is another matter ..."

Introduction

16. At present if a drug dealer sells a pound of heroin for \$70,000 a typical method of operation would be for him to go to eight different banks and make cash deposits of under \$10,000 and electronically transfer those funds directly offshore. This not only leads an audit trail but also means the money has to go into the banking system often in such circumstances that it may lead to the arousal of suspicion and accordingly provide an appropriate lead to a law enforcement agency. Imagine how complex the task would become if the trafficker merely exchanges money from card to card with his customer.

17. Automated financial transactions can make life extremely difficult for law enforcement agencies as co-noted at pp 83 of the RGEK report.

"Automation also makes some types of otherwise unwieldy financial transactions more feasible. An automated transfer process makes transferring money to 10,000 accounts just as easy as transferring to a single account once they have been set up and automated.

This problem is made worse if new banking and financial facilities outside of the traditional banking system are made available. Detecting large numbers of 'micropayments' may not be possible with techniques that are effective for detecting large transfers. Automation makes it quite feasible to perform 10,000 transactions of \$20, each of which may escape the attention of the appropriate authorities. The implications of this are that law enforcement and revenue agencies need to work closely with the financial sector to ensure that appropriate technologies and systems which may detect such behaviour are implemented.

Hiding a large financial transaction using automation "

Cryptography and Steganography

18. Cryptography and Steganography are potential major problems for law enforcement agencies trying investigate

Introduction

organised criminal networks. Any legitimate business can make very good use of cryptography and there is a world wide debate raging between those with heavy commercial leanings who suggest there should be no government regulation of these techniques and those in law enforcement who say that such systems should not be sold without law enforcement's access to the encryption keys which would allow interpretation of the data sent over such systems.

19. Until recently there was only one major form of encryption and that utilised two public keys where both the sender and the recipient had to be in possession of the same key to allow the message to be encrypted and decrypted.

20. However, the recent development of asymmetric encryption has created more potential problems because the recipient can publish his public key and retain his private key and still allow the same level of protection without the cumbersome mechanisms needed to ensure that both parties have the same key. The essential difference between public and private keys are as follows:-

E-commerce demands a relatively sophisticated cryptographic infrastructure. This is because of the openness and accessibility of the Internet. However, as well as attacking this infrastructure, criminals can utilise it for their own ends. This will continue to create a tension: it is appropriate for government to encourage the use of cryptography by the general community. However, it is also in the community's interests for law enforcement and revenue agencies to have access to the contents of encrypted communications when warranted.

22. If the cryptographic infrastructure available on the Internet is made too weak, in order to allow for interception of criminal activity, criminals themselves may exploit such weaknesses to attack legitimate e-commerce. However, even if only weak cryptography is employed, the greatest risks to law enforcement and revenue capability will be the deployment of cryptographic hardware and software to facilitate illegal activity.

23. Legitimate users of cryptographic tools will benefit from improvements in hardware and software which will allow them to more easily employ these tools. Nevertheless, in the mean time, the major risks in the legitimate deployment of cryptography will lie in skill shortages. Criminals will also benefit from this growing ease of usage.

The RGEC report also notes at pp 102-106:

" Criminal Use of Cryptography

Criminals will use cryptographic infrastructure to communicate and conspire, and even establish complex e-commerce networks of their own (such as underground banking networks).

There are three primary mechanisms they may use to do this:

Off-the-shelf hardware and software;

Custom cryptography using stronger versions of standard algorithms;

Exotic custom techniques such as steganography and chaffing and winnowing.

Some criminals will use off-the-shelf hardware and software, once they become widely available. Until that time, it is likely that they will not use any form of encryption. However, a minority of criminals will use customised, strong encryption.

Following is a table which outlines the short, medium and long term outlooks for the exploitation of this characteristic of the Internet.

Introduction

Short term	In the short term, while Web sessions for transactions will be protected by SSL, e-mail will continue to be unencrypted and unsigned, awaiting the widespread availability of individual certificates. There will be a degree of vulnerability due to inexperience at configuration and deployment of cryptography.
Medium term	In the medium term, driven by the availability of certificates, it will become standard practice to sign and encrypt e-mail. More web sessions, but not the majority, will use SSL and a proportion will use client certificates to identify users. Experience with deployment of cryptography will grow. Smartcards will start to be used more widely.
Longer Term	The longer term will be as for the medium term, except that the majority of Web sessions, as well as e-mail, will be encrypted, and there will be widespread competence in the deployment of cryptography. Smartcards will be widely used. "

Cryptography and steganography provide the basic tools for sending protected and hidden information securely across open networks. Steganography provides protection by hiding valuable data so that it can pass unnoticed. Cryptography makes it difficult to recover information that has been encrypted without access to the appropriate keys.

Introduction

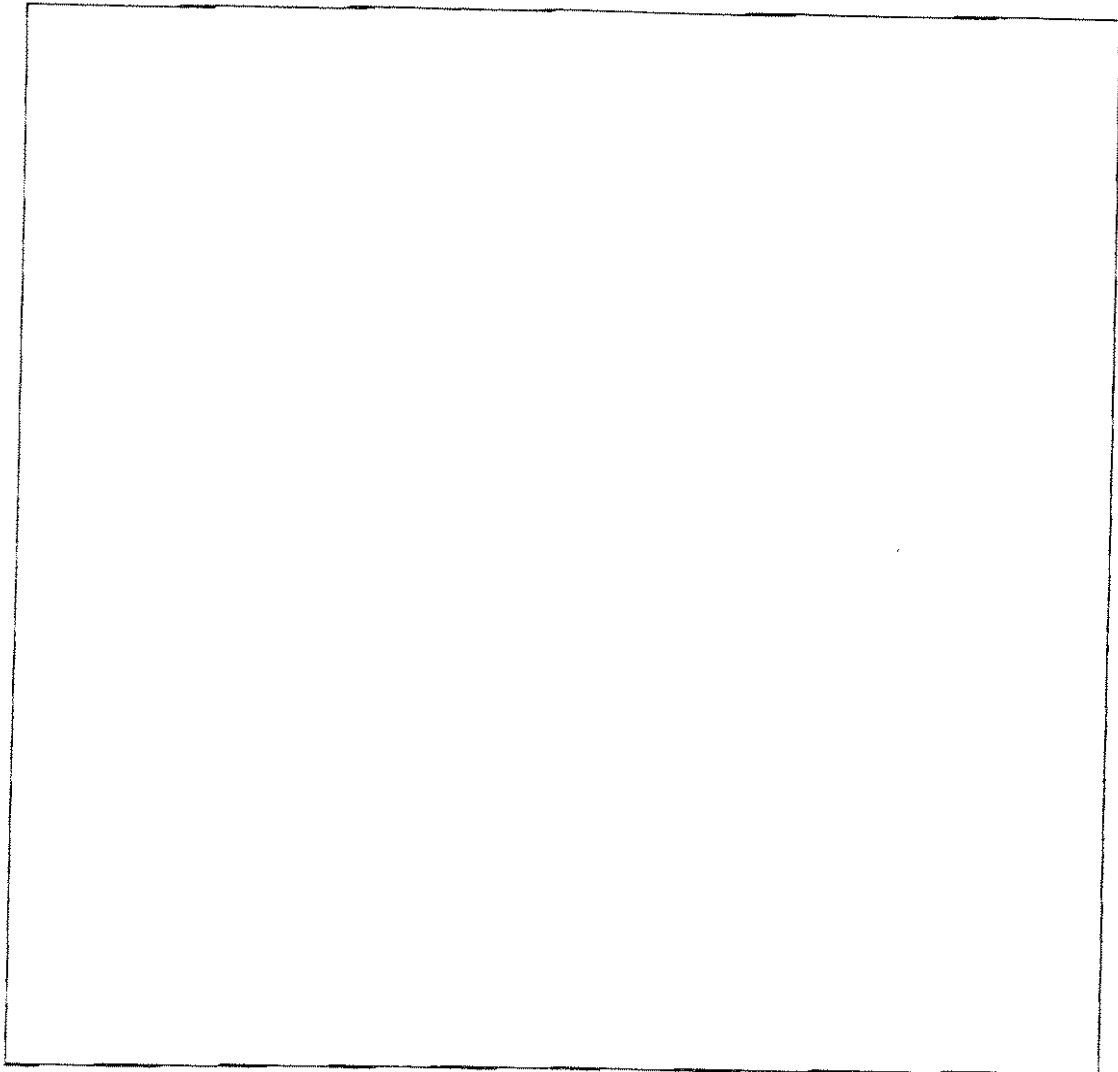


Figure 3.19 – Interception and encryption

Figure 3.19 illustrates the problem that encryption raises for law enforcement and revenue agencies. The sender and recipient of the message know the shared encryption key and so can exchange messages easily and securely. A law enforcement or revenue agency intercepting the same message may not be able to decrypt it because they do not have access to the key and the use of strong encryption makes brute force decryption infeasible.

Steganography is also a technique that can be used to hamper law enforcement and revenue agencies. Files, such as drug delivery schedules can be hidden in other innocent looking files, such as photographs, and sent over the open Internet. Agencies may intercept the carrier file but would not necessarily even suspect that anything of interest was hidden inside it. The hidden files may also be encrypted, just to make interception more difficult. That is, through sophisticated methods of deception, code can be written into what appears on the surface to be legitimate correspondence.

Introduction

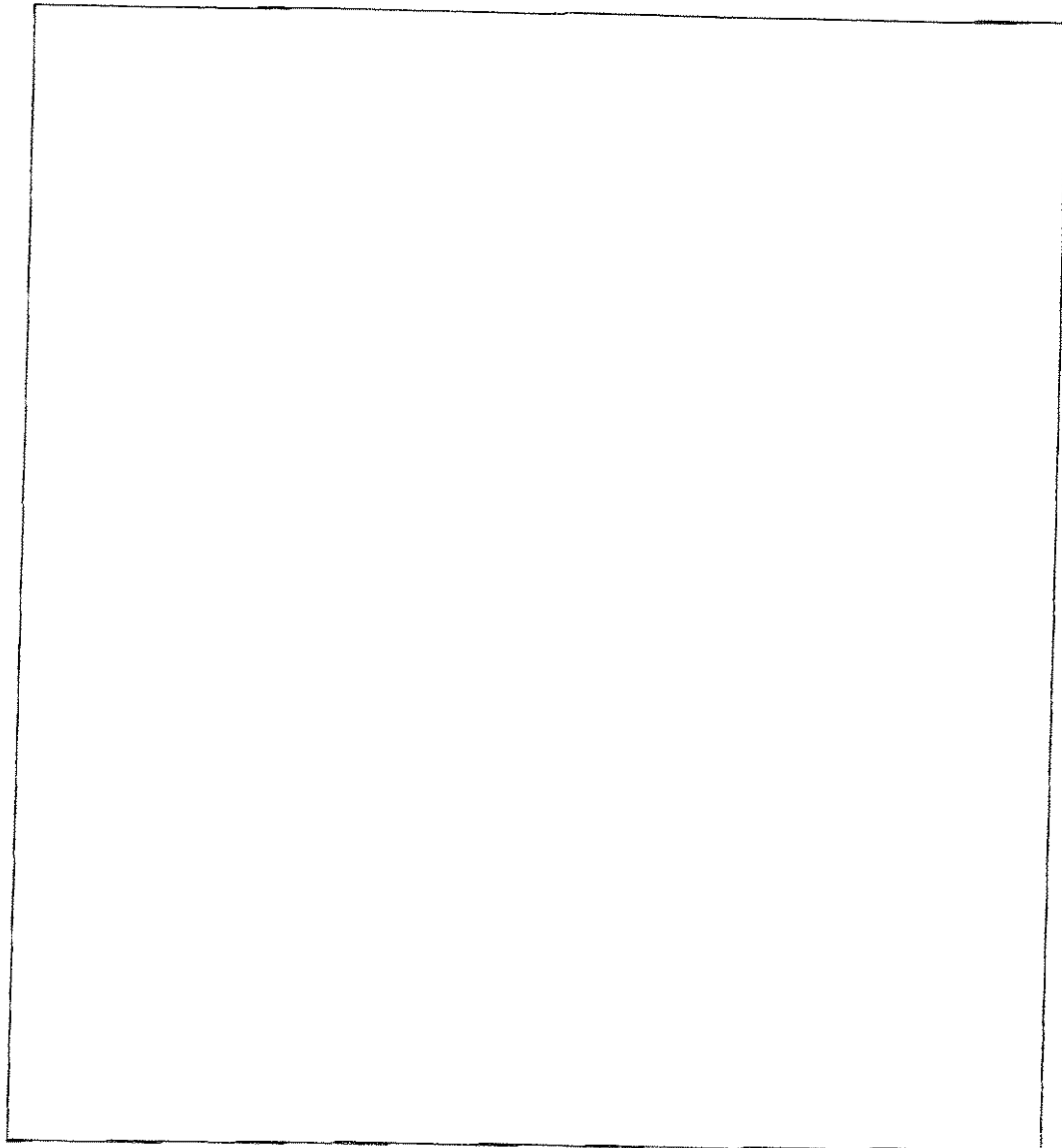


Figure 3.20 – Steganography and interception

Figure 3.20 shows the use of steganography to hide a text file within a photograph. The message is intercepted by an agency but it is unaware of the hidden message and so fails to extract it.

Chaffing and winnowing is a steganographic scheme that provides 'confidentiality without encryption' proposed by Ron Rivest in 1998. The premise on which it is based is very similar to that of Transmission Control Protocol (TCP). TCP headers include a checksum field that can be used to check the integrity of the packet, and a sequence number that allows reassembly of the packets. Under TCP, if a checksum does not match, the packet is simply thrown away."

25. There is considerable debate as to how encryption will impact upon law enforcement capabilities. Figures from the US indicate that encrypted data is now encountered in about 7-9% of cases compared to 1% a few years ago. It is typically found in cases involving child pornography. The use of encryption is encountered more often in relation to data (files and emails) than voice. The general feeling is that the compression provided by ISDN provides adequate privacy. However, while the number of encrypted voice communications cases is small, there is an upward trend (from 3 to 6 to 12 cases per

Introduction

year in the last 3 years).

26. Current indications are that use of encryption is confined to international criminal groups. There is little indication of its use in general crime networks. Why is unclear, but it is suggested that this may be because of a lack of agreed standards, disciplines and/or knowledge. Off the shelf encryption (Pretty Good Privacy) is typically used, although niche systems may have been developed by some crime groups.

27. Criminal use of encryption impacts on law enforcement in two ways – it may stop an investigation, it may increase investigation costs to crack encryption. To take the example of a readily available 128 bit key: using a 'brute force' approach – with a billion computers that are able to try a billion keys per second (which is far beyond anything available at present) - it would still take the decrypter 10,000,000,000,000 years to try all of the possible combinations. That is something like a thousand times the age of the universe".

28. Various solutions have been suggested, including the US policy of the development of key recovery encryption through government purchasing and pilot projects, and a draft policy in the UK relating to the establishment of Trusted Third Parties, with mandatory access for LEAs (however, this latter policy has since been abandoned).

Electronic Fraud

29. The use of cyberspace to commit crimes commenced almost as soon as the Internet. All of you no doubt are aware some early "crimes" were committed when clever programmers transferred the "rounded off" fraction of a cent on daily transactions from banks into a separate "private" account. This system would allow them to accumulate many millions of dollars whereas the most any particular individual or institution was out of pocket was a fraction of a cent. Until the relevant criminal statutes were amended in many jurisdictions this was not even an offence.

30. There was a boom in credit card fraud commencing in the mid 1980's which peaked in the early 1990's when criminals mastered technology of skimming – which is the transferring of electronic data on a credit card's magnetic strip to another card. As noted by Brian Bayliss, Mastercard Vice President for Security and Risk Manager (Europe, Middle East and Africa), devices enabling criminals to carry out these operations are becoming increasingly sophisticated and compact. He stated, in the International Police Review, July/August 1999, at page 39:

"A handheld 'skimmer' had been developed, he said. It was battery operated and small enough to fit in a pocket. It had a microchip that was able to store the data of at least 20 cards, which could be downloaded onto a laptop computer.

With one swipe in a restaurant, a corrupt waiter could store the details of a magnetic strip on a skimming device.

These electronic codes could be sent via a modem anywhere in the world, where they could be imprinted on another card. Mr Bayliss said that in this way a card skimmed in London could have its details sent to Japan and, in eight hours, a duplicate credit card could be used to buy high value resaleable goods in Tokyo.

Organised criminal groups from Hungary, the UK, Italy, Japan, Australia, the US and Canada are among those involved in this type of crime, he said.

In the past, counterfeiting has been responsible for 30 to 40 per cent of card fraud, compared with lost and stolen card fraud, identity fraud and application fraud, but these proportions are now roughly equal worldwide, he said. Delegates were told that former communist countries in central Europe were seen as future boom areas, given that the use of credit and charge cards had been limited until recently. With undeveloped legal and judicial systems, little police knowledge of card fraud and unsophisticated bank security systems, the new soft underbelly of Europe's banking sector is already being attacked."

31. Furthermore, cyberspace can allow criminals to attack sites, usually financial institutions anywhere in the world, usually they will deal through a number of Internet service providers (ISP's) in many countries which not only makes

Introduction

tracing extremely difficult but each step in the process requires the cooperation of local agencies and law enforcement personnel to trace the perpetrator.

32. This will also involve the cooperation of site administrators, many of whom are merely interested in signing up as many customers as possible to ensure they can on-sell this customer base to a larger company for a significant profit. As yet no formal identification is needed to commence an Internet address and I believe that time is well overdue to acquire an appropriate system of identification of an Internet user prior to allowing them to access an ISP. I can already hear the howls of derision from those telling me the horse has well and truly bolted. The same criticisms were raised when the Australian banking industry was required to conduct a 100 point check before opening a bank account. Those banks now recognise that it is the best thing that ever happened because it also allows them the security of knowing with whom they are dealing and has reduced their exposure to fraudulent attacks.

33. Such a system should be introduced for all ISP's throughout the world, although obviously they would need a reasonable time to catch up with the millions of people already connected.

Jurisdictional Issues

34. This leads me to the next issue which is the legislative and jurisdictional problems that have been created and I will use my own country as an example.

35. Criminal behaviour in Australia is regulated by separate Criminal Codes or Crimes Acts applicable to each State and Territory and also to the Commonwealth of Australia. There are often significant differences between elements of an offence and both statute and common law have evolved from an era long since gone. For example considerations of the initiation of criminal conduct go back to the days of writing letters and the laws have been progressively moulded to encompass firstly telephone technology and now in some instances computer technology.

36. Cyberspace creates many problems, especially if one is trying to determine in what jurisdiction an action occurred, whether it amounts to an offence in that jurisdiction and whether or not matters occurring between various States can be dealt with by an overarching Commonwealth jurisdiction. The Commonwealth Crimes Act expressly claims jurisdiction throughout the whole of the Commonwealth and Territories and in some cases beyond the Commonwealth and Territories. (See section 3A)

37. However, State laws only apply to criminal conduct which occurs within the boundaries of that State except in certain limited circumstances and accordingly even if the offender and victim are both residents of Queensland if a fraud was committed in New South Wales it could not be prosecuted under Queensland law. In some circumstances Commonwealth law has developed to determine where an offence is committed if relevant conduct occurs in more than one jurisdiction. However, it can be extremely difficult to work out where an offence has been committed. For example, if a criminal in the United States uses the Internet to cause a bank in Western Australia to withdraw funds from a New South Wales account holder's account there are arguments that the offence could have occurred in any one of the three jurisdictions.

38. As noted by Geoff Gray from the Office of the Commonwealth Director of Public Prosecutions (Australia):

"It is not an offence against Victorian law for two people to plan a fraud which they intend to carry out in NSW (*R v Hamilton-Byrne* [1995] VR129. However, there may be a Victorian offence if the parties put the fraud into effect by sending a communication from Victoria to NSW (*R v Waugh*) [1909] VLR379. If it is not clear where a relevant communication actually originated, it may be impossible to say whether or not there is any offence against Victorian law."

39. I am aware of *DPP v Stonehouse* [1978] AC 55, but I'm not sure if the circumstances in that case provide a good basis for the problems created by cyberspace.

40. In 1952 the United States overcame this problem by the enactment of section 1343 of the Federal Criminal Code. This provision which is commonly known as the wirefraud provision states it is a federal offence to use any part of the telecommunications system to commit any element of a criminal offence.

Introduction

41. Australia arguably has the constitutional power to enact such under the telecommunications power but further problems are created by section 80 of the Constitution which provides as follows:

80. The trial on indictment of any offence against any law of the Commonwealth shall be by jury, and every such trial shall be held in the State where the offence was committed, and if the offence was not committed within any State the trial shall be held at such place or places as the Parliament prescribes.

42. If a federal wirefraud offence was prosecuted on indictment it would be necessary to determine where the offence was committed in order to determine where the trial should take place. The onus would be on the prosecution to show location although the standard of proof would be on the balance of probabilities rather than proof beyond reasonable doubt. (*Thompson v R* (1989) 169 CLR 1). This places the onus on the prosecution to show the location of the offence in order to enable to determine where the trial should take place.

43. There then become further problems to consider when actions take place outside of Australia and section 3A of the Crimes Act does not apply.

44. Many countries are attempting to exert extra territorial jurisdictions as broadly as possible especially with increasing internationalisation of many activities. However, as we are all aware there are many countries who want to have no part in such international schemes and sustain their economies by allowing refuge for a vast array of criminal activities especially money laundering.

45. It has been suggested that because of the many similarities between cyberspace in the high seas conventions and laws applicable to the high seas could be adopted and control operations in cyberspace. For example, a corporate entity could be required to submit to the jurisdiction in which it was created and the nationality of a natural person could determine the jurisdiction relating to them. However, the laws of the high seas are often confused by the flags of convenience and it would not be difficult to imagine Internet service providers flocking to jurisdictions with little regulation.

46. Even if we have law which can assert jurisdiction over an offence there are major practical barriers associated with actually bringing the offender before the courts. There are also problems with securing and obtaining the necessary evidence from overseas jurisdictions and such evidence will quite often have to be obtained through mutual assistance arrangements. As many of you are no doubt aware the extent to which these arrangements are timely and effective depends upon the nature of arrangements existing between countries and if the audit trail takes us through many countries organised criminals will no doubt be sensible enough to make sure that at least some of those countries have no treaties or are notoriously difficult from which to obtain evidence.

Conclusion

I don't pretend to know the answers to the above problems, but unless all countries start acting in a timely and cooperative manner those organised criminal groups which have no respect for national boundaries will cause havoc, possibly destroying the economies of many nations causing major disruption to even the strongest world economies.

48. There also has to be a sensible resolution to the ever present tensions between commercial and law enforcement imperatives, and governments cannot absolve themselves of the responsibility for making unpopular decisions to ensure the appropriate balance is struck.