Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:23
Received 2 June 2003
Mr Alastair Milroy
Chief Executive Officer
Australian Crime Commission
GPO Box 5260
SYDNEY NSW 2001
☎02 9373 2100 🗎02 9373 2199
E-mail:

Inquiry by the Parliamentary Joint Committee on the Australian Crime Commission

The @CC role in the Cybercrime Environment

Submission by the
Australian Crime Commission
May 2003

Table of Contents

GLOSSARY

ABCI	Australian Bureau of Criminal Intelligence
ACC	Australian Crime Commission
ACPR	Australasian Centre for Policing Research
ACS	Australian Customs Service
AFP	Australian Federal Police
AGEC	Action Group into the Law Enforcement Implications of E-commerce
AHTCC	Australian Hi Tech Crime Centre
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
AUSTRAC	Australian Transaction Reports and Analysis Centre
Cyber-forensics	Application of computer and digital technological systems investigation and analysis for determining potential evidence.
Digital Cash	A system of purchasing cash credits and storing the credits in a computer and spending them when making electronic purchases over the Internet.
Digital Signature	Systems that allow people and organisations to certify electronically such features as their identity.
DPP	Director of Public Prosecutions
EFT	Electronic Funds Transfer
Email	Electronic mail
FBI	(US) Federal Bureau of Investigation
FTP	File Transfer Protocol – A standard Internet protocol designed to exchange files between computers on the Internet.
FTR Act	Financial Transaction Reports Act 1988 (C'wealth)
HOCOLEA	Heads of Commonwealth Operational Law Enforcement Agencies.
Internet	The vast collection of inter-connected networks that all use the TCP/IP protocols.
Intranet	A private network inside a company or organisation, similar in principle to the Internet.
IP	Internet Protocol is the protocol of the TCP/IP suite that routes messages from one Internet location to another. Usually read as a series of numbers with decimal points (eg 123.456.78.90) and useful for tracking messages.
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LEA	Law enforcement agency
MOU	Memorandum of Understanding
NCA	National Crime Authority
NOIE	National Office for the Information Economy
NSWCC	NSW Crime Commission

OECD	Organisation of Economic Co-operation and Development
OGO	Office of Government Online
PC	Personal Computer – Generically any computer designed to be used by one person, specifically the IBM PC and others compatible with it.
SGE	Secure Gateway Environment – a secure extranet
SIM card	Subscriber Identity Module card
SMS	Short Messaging Service – wireless text messaging service
SSL	Secure Socket Layer
SVC	Stored Value Cards – also known as Smart Cards
SWIFT	Society for Worldwide Interbank Financial Telecommunications: Electronic Bank Transfer System
URL	Uniform Resource Locator –Eg http://www.address.com
World Wide Web	This hypertext-based form of communication allowed the Internet to become as popular as it has.

Attachments

1. Police Commissioners National E Crime Strategy.

2. 2003 Australian Computer Crime and Security Survey, AUSCERT, 2003.

3. Child sex Offender Networks on the Internet, ABCI Assessment, 2002. (PROTECTED)

4. The impact of emerging technology on fraud, ABCI Assessment, November 2001. (PROTECTED)

5. Organised Credit Card Skimming, ABCI Assessment, May 2002.

6. Long-Term Criminal Risks to the National Information Infrastructure (NII), OSCA, 2002. (IN-CONFIDENCE)

EXECUTIVE SUMMARY

> "*We should not be fighting crime of the twenty-first century with tools of the nineteenth*" (Jack Straw, Home secretary, United Kingdom, 1997)

The opportunity for criminals to use technology to further traditional crimes, and to commit new forms of crime, has emerged as a major challenge facing law enforcement, government and the community.

Hacking, online fraud, identity crime, money laundering and other technology related crimes, are now joined by terrorism, internet child pornography, narcotics, and other traditional offences which are furthered by criminal use of secure internet communications and encryption. Computer technology facilitates the commission of crime remotely, securely and anonymously. Cybercrime recognises no borders: national and trans-national investigations are not an exception in Cybercrime, but rather the rule.

The ACC's new national role is the collection and analysis of criminal intelligence, the establishment of National Criminal Intelligence Priorities, and the conduct of intelligence operations and investigations into nationally significant crime. The ACC plays a niche role in relation to Cybercrime. Manifestations of Cybercrime are present across the range of serious and organised crime which is the ACC's core business. As Australia's national criminal intelligence agency the ACC is well placed to make an important intelligence contribution to the national response to Cybercrime. The ACC also provides forensic and technical services to support its own operations and those undertaken with partner agencies.

Inherently, Cybercrime investigations are highly complex, as well as resource and expertise intensive. A high proportion of Cybercrime investigations also have significant jurisdictional issues. The ACC is well suited to bring a national perspective and specialist capabilities to this multi-jurisdictional work.

The recent establishment of the Australian Hi Tech Crime Centre (AHTCC), and the inclusion of the ACC as part of the Hi Tech Crime Managers Group (HTCMG), highlights the importance placed on national strategic partnerships. The AHTCC is intended as a coordinating centre for complex Hi Tech Crime Investigations, and will be a focal point for intelligence gathering in this area, and thus an important partner to the ACC.

This submission proposes a number of practical steps which are intended to enhance law enforcement capacities. The ACC's Cybercrime focus will include:

- Collection and coordination of Cybercrime intelligence, and provision of services such as the national criminal intelligence database to facilitate information sharing,
- Partnerships, particularly with the AHTCC and jurisdictions' Cybercrime task forces,
- Enhancing the electronic (Internet) intelligence gathering and data interception capability of the ACC,
- Increasing the national criminal intelligence capacity of the ACC in order to improve the service of information and intelligence, for example by incorporating trans-national internet paedophile intelligence,
- Law reform, including making the case for law enforcement agencies to conduct lawful interception of criminals' data via 'electronic search warrants'.

The PJC Submission Terms of Reference

In the following sections we will examine the NCA/ACC role in regards to the terms of reference set by the ACC Parliamentary Joint Committee, in their letter dated 11 April 2003.

The PJC terms of reference include:

- ⇒ Internet Child Pornography and paedophile networks,
- ⇒ Banking, including credit card fraud and money laundering, and
- ⇒ Threats to the National Electronic Information Infrastructure (Hacking).

Each section will address the past role of the ACC in each reference, an examination of the current environment, and future direction open to the ACC for input in these areas.

The last part of this submission will examine the ACC Cybercrime Toolbox and the practical strategies which could be utilised by the ACC in the LEA intelligence development and investigation of Cybercrime and criminal use of technology to further traditional crimes.

A Brief Introduction to the Cybercrime Environment

The Australian Centre for Police Research (ACPR) defined Electronic Crime as:

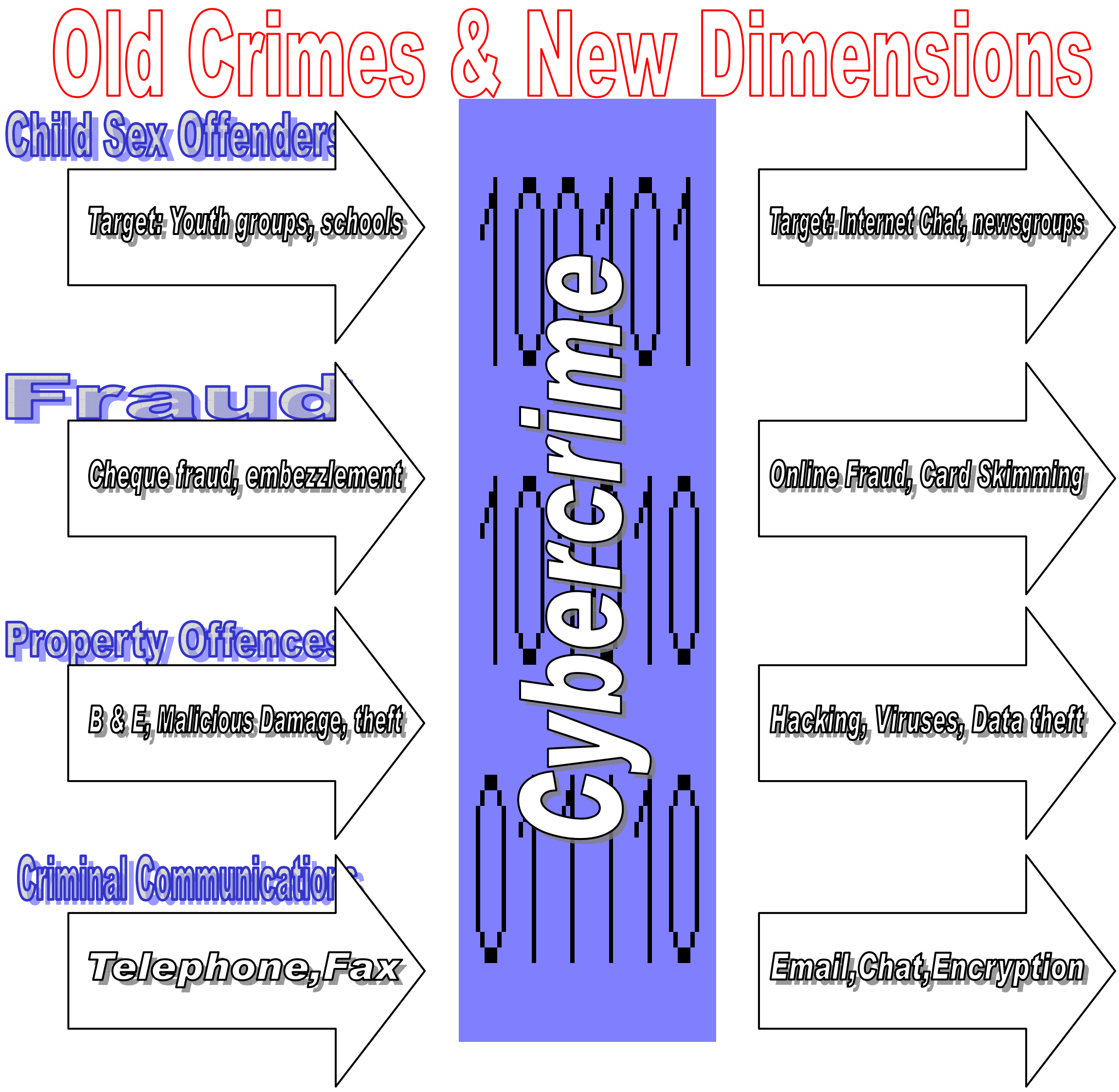
"*Offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence*".

It has also been variously described as Cybercrime, E-Crime, Computer Crime and most recently Hi Tech Crime. Whatever the identifier, most agencies agree that the burgeoning criminal use of emerging technology is a national/transnational significant threat which requires a coordinated response.

This submission will focus on the Cybercrime related areas of Internet Child Pornography and paedophile networks, Hi Tech Fraud including online banking vulnerabilities, organised credit card skimming and money laundering, and threats to the National Electronic Information Infrastructure (Hacking). Further, we shall examine some emerging trends in those crime areas, and Australia's Law Enforcement Response.

Whilst this new Cyber aspect of crime appears to be the realm of technical experts and "computer geeks", it must be also be acknowledged that many of what has be referred to as the "old crimes", may now have a Cybercrime equivalent.

This is especially relevant in the continuing sophistication in the criminal use of communications in serious crime including drug importation and distribution.


Old Crimes & New Dimensions
Child Sex Offenders
Target: Youth groups, schools
Fraud
Cheque fraud, embezzlement
Property Offences
B & E, Malicious Damage, theft
Criminal Communications
Telephone,Fax
Cybercrime
Target: Internet Chat, newsgroups
Online Fraud, Card Skimming
Hacking, Viruses, Data theft
Email,Chat,Encryption

Some examples of Cybercrime;

- Critical Infrastructure Attack (Hacking, cyber-terrorism and malicious programs like viruses)
- Fraud (Credit card Skimming, “page jacking”, SPAM “Nigerian” letters)
- Online Money Laundering
- Criminal use of Internet communications (Email, Instant Messaging, secure encryption)
- ID Fraud (Computer generated Identification, theft of identity personal information from internet connected computers)
- Use of computers to further traditional crimes (Such as child pornography or paedophile activity)

In March 2001, the Police Commissioners Conference, Electronic Crime Steering Committee, released the *2001-2003 Electronic Crime Strategy*[1].

[1] National Electronic Crime Strategy, March 2001.

Many of the guiding principles of that strategy, including partnerships, structured high level coordination, and information and intelligence exchange, are cornerstones of the ACC role. This Electronic Crime intelligence collection, analysis and dissemination role of the ACC is further complimented by partnerships.

The submission will examine the genus and development of the ACC Cybercrime Program, the specialised tools it has available, and explore the future role of the ACC and Cybercrime. This submission is not intended to be an exhaustive analysis of Cybercrime, but rather the ACC's exposure to those focus areas, the current ACC response and some suggested future strategies.

The Private Enterprise Response

Private enterprise has embraced the challenge of the Cybercrime environment, especially in the areas of network protection and providing computer forensics.

However, rather than focussing of the investigation and prosecution of cybercrime offenders, private enterprise emphasis is on prevention and after incident recovery. Even in the area of computer forensics, private enterprise concentrates on supplying services to clients who do not necessarily want to prosecute offenders.

One private enterprise organisation that has a defined role in the Australian Cybercrime Environment is AUSCERT.

AUSCERT

Private enterprise has also emphasised the importance of identifying Electronic Crime Threats and Opportunities, through intelligence collection and partnerships.[2]

AUSCERT, Australia's national Computer Emergency Response Team (CERT), is an independent, not-for-profit organisation, based at The University of Queensland.

AUSCERT covers its operating costs through member subscriptions and the provision of affordable computer security training and education and consultancy services. The Commonwealth government currently provides funding for certain parts of AUSCERT's operations.

AUSCERT monitors and evaluates global computer network threats and vulnerabilities from numerous sources throughout the year, including after hours when Coordination Centre staff remain on-call to respond to new information in a time critical manner. As a result, AUSCERT publishes security bulletins, drawing on material from a variety of sources, with recommended prevention and mitigation strategies.

The Commonwealth government currently provides funding for certain parts of AUSCERT's operations. Australian Law Enforcement is now working in

[2] 2002 Australian Computer Crime and Security Survey, AUSCERT, 2002

partnership with AUSCERT and the ACC is directly supporting the AUSCERT incident reporting and alerts scheme.

The Law Enforcement Response

In recent years Australian law enforcement agencies have identified a dramatic increase in the use of emerging technology by national/trans-national criminals and organised criminal groups. This includes hacking, electronic fraud, card skimming, encrypted and secured internet communications, and identification fraud.

The draft 2001 Law Enforcement Planning Document (LEPD) *A Strategic Plan for Commonwealth Law Enforcement* identified Australia's law enforcement vision as being "a coordinated and integrated approach to dealing with an increasingly sophisticated and dynamic criminal environment that threatens our social and economic infrastructure and to achieve the flexibility to enable a rapid and effective strategic response to emerging criminal threats, in order to provide a safe and secure Australia".

All law enforcement agencies, state and federal, have responded to the need to deal with Cybercrime at various levels. All have some form of forensic Computer examination capacity, though some are better equipped and funded than others. This disparity can somewhat be addressed through partnerships with other agencies. Though relatively young, the ACC National Cybercrime Unit has assisted a number of state and federal agencies in this manner in recent times.

The Australian Hi-Tech Crime Centre (AHTCC)

As part of the Police Commissioners' E Crime Strategy, all law enforcement agencies have sought to strengthen their own internal capacity to deal with the emerging threat of Cybercrime. However, what was lacking, was a coordinating national body as a central focus for Cybercrime referrals and threat response.

In 2002, the senior officers group approved a model for the establishment of the Australian Hi-Tech Crime Centre (AHTCC). The AHTCC model approved is hosted by the Australian Federal Police (AFP) on the basis of their existing expertise and resources in this area. It will also include staff seconded from other Law Enforcement Agencies.

The AHTCC was created to provide a "24/7" point of contact and investigative capacity for National and transnational major Cybercrime incidents. It is still in its infancy and therefore has a limited investigative and intelligence capacity. To function properly, the AHTCC must work in partnership with the ACC, private enterprise, jurisdictions and other Commonwealth agencies.

The ACC can offer to the AHTCC its multi jurisdictional special powers, and national criminal intelligence functions.

This provides an excellent opportunity for the ACC and AHTCC to work on a coordinated response and preliminary discussions have already been held in regards to this end. This includes the possibility of ACC staff seconded to the AHTCC to assist with Cybercrime intelligence gathering, dissemination, and operation of the E Crime Desk by the AHTCC.

The ACC Response

In 2001, the NCA received funding to advance its capacity to deal with electronic crime under its "Cybercrime Program".

The program sought to;

- Develop a National Cybercrime Intelligence gathering and analysis regime
- Establish an advanced in-house forensic computing capacity
- Create an effective Cybercrime training program for staff and investigators
- Assist in the establishment of a National Cybercrime Resource (AHTCC)

In 2002, the core of the ACC Cybercrime Program, the ACC National Cybercrime Unit (NCU), was created to implement and develop that program.

A more detailed look at the role and achievements of the ACC National Cybercrime Unit will be found in this submission under the heading of "The Cybercrime Toolbox".

Term of Reference:

CHILD PORNOGRAPHY AND ASSOCIATED PAEDOPHILE ACTIVITY

Definition of Child Sex Offender

A child sex offender (CSO) is a person who commits a sexual offence against a child. A child is a person under the age of consent in each police jurisdiction, usually under 16 years of age. A sexual offence ranges from actual physical assault through to producing and exchanging child pornography (ABCI, 2001a).

"The term CSO is used instead of 'paedophile', which is a clinical term with no basis in legislation", (ABCI, 2001b, p.7).

CSO's and the Internet

Internet Child Pornography in Australia

The ABCI produced an intelligence assessment '*The Scale of Internet Child Pornography in Australia*' in January 2001. It found that 'Child sex offenders have embraced emerging technology to transmit and receive pornography, to network with other offenders and to access potential victims' (ABCI, 2001b, p.16).

The assessment made a series of tactical and strategic recommendations, and highlighted the need for legislative reform to ensure law enforcement has the capacity to 'keep pace with criminal use of technology' (ABCI, 2001b, p.16).

Accessing CSO networks

The Internet provides people with considerable anonymity and access to literally thousands of chat rooms and newsgroups. This fact in itself provides a snapshot of existing and potential problems that confront the law enforcement community.

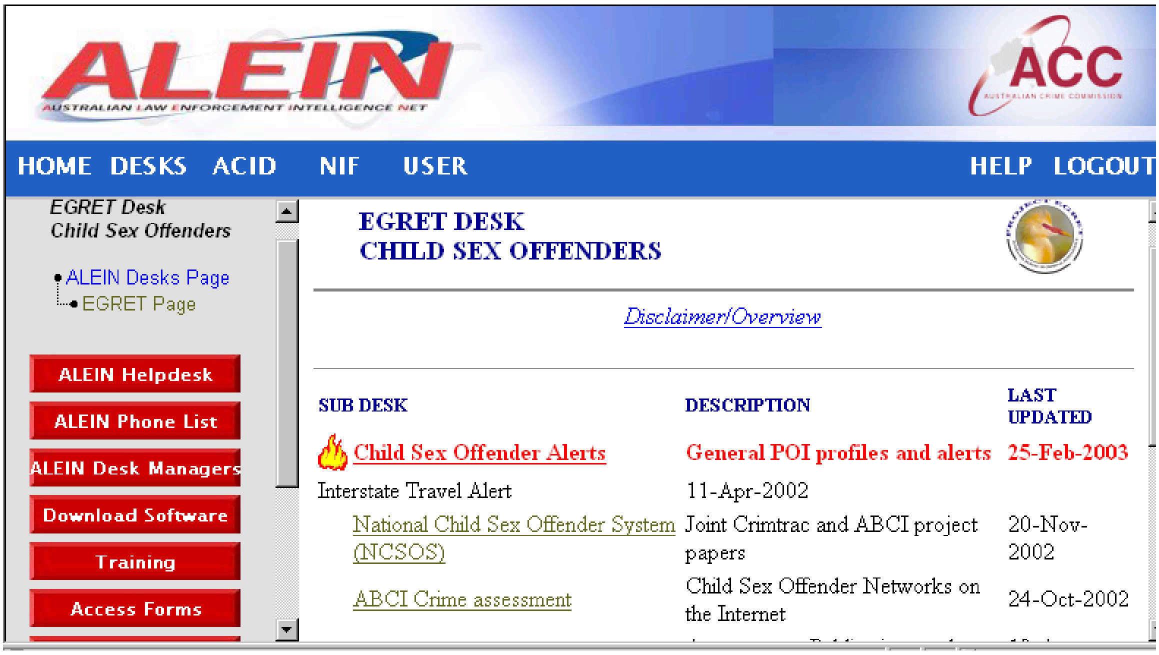
The Internet has exposed a traditional offence such as the sexual exploitation of children to the 'rubber neck' factor. Australian investigators have used this term for people who, through the use of the Internet, can now explore their sexuality with minimal chance of police detection.

The report indicated the following key findings on how CSOs use the Internet **(**ABCI, 2001b, p.23**).**

1. Child sex offenders have embraced information technology and the internet to transmit child pornography, network with other offenders and access victims.
2. Child sex offenders are active in most areas of the internet, specifically internet relay chat (IRC) and associated FServes, chat rooms and Usenet groups (newsgroups). Email and FTP sites are used to a lesser extent.
3. Offenders almost exclusively use IBM clone computers with fast clock speeds, large amounts of hard drive memory and RAM.
4. Computer peripherals utilised by offenders include removable storage media, CD-ROM writers, digital cameras and scanners.
5. The majority of offenders are collectors of child pornography who produce very little, if any, of their own material.

6. Despite the risks of interception, offenders order child pornography from commercial sites on the internet, which results in dispatch of physical products.

History of CSO desk and project Egret



EGRET DESK
CHILD SEX OFFENDERS

Disclaimer/Overview

SUB DESK	DESCRIPTION	LAST UPDATED
Child Sex Offender Alerts	General POI profiles and alerts	25-Feb-2003
Interstate Travel Alert	11-Apr-2002	
National Child Sex Offender System (NCSOS)	Joint Crimtrac and ABCI project papers	20-Nov-2002
ABCI Crime assessment	Child Sex Offender Networks on the Internet	24-Oct-2002

In 1989 the Australian Bureau of Criminal Intelligence (ABCI) initiated a national project into child sex offenders named Project Egret. The aim of the Project was to give: priority to paedophilia and act as a national coordinator of criminal intelligence; provide for collection, evaluation, collation and dissemination of intelligence; and research legislative constraints and opportunities.

The Australian Crime Commission (ACC) now continues this responsibility in the form of the CSO desk.

Overview of current ACC CSO desk

The CSO desk coordinator maintains a CSO desk on the Australian Law Enforcement Intelligence Net (ALEIN). The desk contains offender alerts and profiles, intelligence assessments, information on Australian and international operations, open source data and a link to Interstate Travel Alerts from the NSW Child Protection Register.

The ALEIN CSO desk provides for a central location for storing processed reports on CSO matters accessible by all jurisdictions. It provides a coordination point for Project Egret and CSO matters nationally including reference sources and materials on issues national and international.

Overview of CSO – Project Egret data on ACID

Jurisdictions upload data to the Australia Criminal Intelligence Database (ACID) under the title of Project Egret for storage of raw data and information related to CSO matters. Some information is caveated and accessible only by officers actively working within this environment. ACID enables officers to search and retrieve information at a national level. This information may relate to CSO suspects and offenders, including Internet related offences.

There are approximately 9470 documents in ACID directly related to Project Egret consisting of information reports, intelligence assessments, open source information and incident reports.

The National Index Facility (NIF) on ACID provides a specific list of 2454 identified CSO suspects and offenders. Approximately 70 names have been added since February 2002.

Information related to CSOs using the Internet is also placed on ACID. This information consists of finalised case reports through to intelligence reports identifying CSOs nicknames, email address and chat room details. This information is valuable because it provides police with a central location to search for information on CSO Internet offenders. It also provides an opportunity to review such holdings to see if any links can be identified between nicknames, Internet Service Providers addresses, chat rooms and offender methodologies.

There are many documents in ACID related to child sex offences or issues. However for unknown reasons, not all have been linked to Project Egret or the NIF (A recent review identified 544 CSO related documents in the system not linked to Project Egret). Furthermore, different searches on ACID can reveal different results depending on the search criteria used. For this reason it is difficult to accurately quantify the amount of CSO data on ACID apart from what has already been indicated.

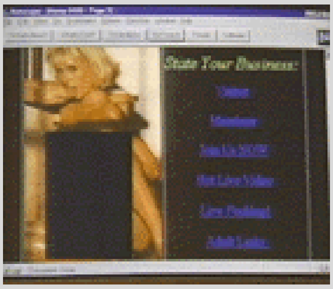
Australian Crime Commissioners Forum Working Party

These key findings were used to establish an Australasian Crime Commissioners Forum (ACCF) working party into on line Child abuse which first met on 20 November 2001. The working party is made up of representatives from state and territory police services, Australian Federal Police, Australian Customs Service and the Commonwealth Attorney General’s Department. The ACC participates in this working party, which will report to the next Senior Officers Group (SOG) meeting in May 2003.

This working party seeks to develop a national coordinated approach to dealing with CSO using the internet. This includes developing national minimum standards for on line investigations, methodologies for proactive targeting, increasing national / international liaison, coordination and communication.

The working party initially planned to examine of the value and feasibility of establishing a child pornography image library for Australian law enforcement agencies, similar to those created by Europol, Interpol and law enforcement agencies (LEAs) in the United Kingdom. However, it was decided by the working party early on to wait to see if Australia could link into any of these established image libraries.

<u>CASE STUDY</u>: Corrupt ISP's, Organised Crime and Internet Pornography



There has been a recent evidence of a trend by criminal groups to use secure "chat" programs for communication. These programs are very popular with the public, and are now being used by organised criminals to arrange criminal activities. Although they support voice and file sending, they principally involve exchanges of text, similar to SMS on mobile phones, but easier to use.

Persons of interest have been detected using these communications for arranging pornography sites, "spamming" (junk email), organising the sale of illicit commodities and drug related activities. Programmed used include ICQ and MSN Messenger. Secure chat programs and newsgroups are also a fertile hunting ground for Paedophile groups.

There has also been evidence of persons of interest operating their own Internet Service Provider (ISP), which further frustrates normal LEA responses. (There is currently no licensing for ISP operators and the equipment can be operated from a suburban house.)

Australian Law enforcement issues

The ABCI assessment *'Child Sex Offender Networks on the Internet'* built on the previous ABCI assessment by examining various national and international CSO internet cases.

The assessment found that CSO networks operated in Australia. Some were initiated and controlled from overseas, but at least one network was identified as having been created in Australia. These CSO networks were found to utilise security measures in an attempt to disrupt police investigations. It was also identified that CSO's exploited the legislative inability of LEAs to trade child pornography, thereby limiting the methodology by which to catch offenders (ABCI, 2002).

Australian and International Operations

In May 2002, Queensland Police initiated an international investigation into a CSO network created by an Australian citizen. Until then, Australian LEAs had primarily investigated CSOs, involved in networks, through assisting international investigations that were initiated by overseas LEAs. These international Operations include Cathedral, Eye of a Needle and Landmark (ABCI, 2002).

Since this time there has been a significant increase in the number of international investigations assisted by Australian LEAs. This includes operations Avalanche (USA Customs), E-Circles.com (FBI), Macron (USA), Mondo (German Police), Kinderschultz (German Police), Auckland (United Kingdom), Southside (US Customs) and Candyman (FBI). All of these operations have resulted in the arrests of large numbers of offenders around the world, with many suspects linked to Australia. So far, Operation Candyman has identified 57 Australian suspects (Wright, 2003).

Operation Knell was the result of a national effort to locate an Australian male suspected of committing child sex offences. The British National High Tech Crime Unit had referred child pornographic images to the Australian Federal Police to assist in identifying the offender depicted in the images.

The AFP coordinated a national effort to identify the offender including appealing to the public, through the media, for assistance. The resulting public response led to the arrest of a male in Far North Queensland. The investigation identified involvements in Queensland, Tasmania, NSW and Victoria. To date he has been charged with 88 offences relating to child sexual abuse. The international and trans-border factors faced by investigators demonstrate some of the continuing issues in investigation this type of criminal activity.

CSO networks with international links have significant implications for Australian LEAs. These implications include the difficulties in conducting and coordinating international investigations, to gather evidence outside of Australia’s jurisdiction and to gather or coordinate intelligence to lead these policing decisions (ABCI, 2002, p.5). These issues demonstrate that this criminal activity is a resource intensive area for LEAs.

Legislative Changes

One improvement that occurred recently which will assist Australian LEAs was the announcement by the Commonwealth Government that the downloading or transmitting of child pornography would become a federal offence. The electronic trading in child porn will be treated in the same way as physical trading under the Customs Act, which will carry a maximum penalty of 10 years.

Current services of the ACC in relation to CSO and the internet

Currently the ACC provides the following services:

- The ACC CSO desk coordinator provides a national coordination service for CSO matters. This includes the production of assessments, management of ALEIN CSO desk, and liaison between jurisdictions and agencies engaged in CSO investigations.
- ALEIN provides an avenue for processed information and intelligence assessments to be disseminated to all jurisdictions nationally on CSO internet issues. This is managed by the ACC CSO desk coordinator.
- ACID provides the facility for all jurisdictions to contribute and share information on CSOs and the internet nationally (over 9470 documents).
- The National Index Facility (NIF) located within ACID provides a list of 2454 CSO suspects and offenders (both internet and non-internet related).
- The ACC provides a representative on the ACCF 'on line child abuse' working party, working increase Australia's law enforcement capabilities in relation to CSOs using the internet to commit offences.

Future Direction

Depending on resource, financial and managerial issues, the following are some future possibilities for the ACC in relation to CSOs and the internet:

1. That the ACC continue to support law enforcement agencies in the development of best practice models for investigation and intelligence management relating to CSO networks with cross-jurisdictional and international membership.
2. That the models for best practice are developed by the ACC, in consultation with the ACCF 'Online Child Abuse' Working Party.
3. That the ACC produce further crime assessments in relation to CSO networks using the internet, with a focus on the Australian connection and also the exposure of children to CSO networks on the Internet. These assessments may be used to advise strategic decision makers on the implications for Australian LEAs.
4. That the ACC work with the ACCF in examining of the value and feasibility of establishing a child pornography image library for Australian law enforcement agencies.
5. That the ACC continue to liaise with the AFP National Hi-Tech Crime team, providing support on CSO internet issues as required.
6. As the ACC has representation in all major capital cities throughout Australia, there is potential for the ACC to expand its capability to actively target CSOs using the internet at a national level. This could include acting on information received from international agencies. There would have to be a high degree of national/international organisation evident for this to appropriately be an ACC matter.

Term of Reference:

BANKING, INCLUDING CREDIT CARD FRAUD AND MONEY LAUNDERING

Cashier jailed 30 months for card fraud

She used a magnetic card reader, given by her husband, to get card data from customers at petrol kiosk

By SELINA LUM

A CASHIER at the Shell pet rol kiosk in Coronation Driv used a magnetic card reade to get data fr customer credit ca

ice fr sed dica at

ge. rict court hea showed his wife ho use the device, a Magst Card Reader, when she him in Johor this March

He told her to get hol some credit cards at the S petrol kiosk where worked and swipe t through the device. She

March 27 and

Another 26 attempts were made to use these cards in Taiwan, Malaysia, Japan, Australia and France to make another $51,395 in purchases.

The scam came to light in May this year when the OCBC card centre alerted the ntre that credit

Mr Choo said because young daughters to look after, and asked the court to impose a short sentence so that she could take care of them.

Internet banking passwords stolen

Kirsty Needham
Consumer Writer

Internet bank customers hav been warned

notify the bank if they have any queries."

A spokesman for the NSW id the matter was stigated by the fraud he urged bank cus er to disclose their

s appear to have because the email n an administrator wealthbank.com".

Luke Connolly, a Commonwealth Bank customer who works for an internet service provider, received the email on Monday, along with 10 per cent of the ISP's customer base. Mr Connolly said he was suspicious of its poor grammar, but was brushed off by the bank when he reported it.

"It looks quite genuine because it has the Netbank logo

Cyber scams target banks

Past Role of the NCA/ABCI and ACC

Throughout its lifespan, from May 1984 to December 2002, the investigation of money laundering and tax fraud was fundamental to the NCA's efforts to counteract major organised crime in Australia. This work will continue to underpin ACC initiatives to strengthen Australia's national law enforcement infrastructure.

The ACC, like the NCA, employs specialist financial investigators with accounting and commercial qualifications and experience to support and lead financial aspects of money laundering and tax related investigations and to assist relevant agencies responsible for recovering proceeds of crime and tax fraud.

The ACC will continue to refine and use financial intelligence and financial investigation strategies that have proved successful under the NCA Swordfish and Agio task forces over the last six and eight years respectively. The Agio task force combined financial intelligence from AUSTRAC with criminal intelligence, analytical and investigation capabilities of other Commonwealth agencies to identify money laundering and tax fraud related to major crime. Agio intelligence was regularly referred to a range of Commonwealth, State and Territory law enforcement agencies, including the Tax Office.

In the six years since June 1997 Operation Swordfish led to the recovery of more than $80 million in ill-gotten gains pursuant to proceeds of crime and tax legislation. Both Swordfish and Agio, like other NCA operations, made extensive use of coercive powers to identify and expose money laundering transactions associated with ongoing and serial criminal enterprises that had otherwise escaped detection by law enforcement or other government agencies.

Also, like most NCA and ACC investigations and intelligence operations, work of the Swordfish and Agio task forces was conducted in cooperation and with the assistance of other law enforcement and government agencies that had overlapping interests and responsibilities in relevant areas.

Major money laundering and tax fraud investigations can be expected to remain a high priority for the ACC. The ACC intends to continue the multi-disciplinary and multi agency intelligence and investigation strategies that proved successful under NCA operations Agio and Swordfish. These strategies will be further refined and improved under ACC Operation Midas, for which special funding ($30 million over four years) was announced in the Government's May 2003 Budget.

The ACC also intends to continue the valuable work of the ABCI in operating the National Fraud Desk. The desk provides Australian LEA, in particular the jurisdictions, with access to National Fraud Alerts, strategic assessments and tactical data. This includes information of online and credit card fraud.

AUSTRAC: Regulating the cash to electronic barrier.

There is a wide range of legislation relevant to electronic banking, including banking and corporations law, through to the recently enacted *Proceeds Of Crime Act 2002*. However the fundamental regulatory framework from a law enforcement perspective is provided by the *Financial Transaction Reports Act 1998* (FTR Act), which established the Australian Transaction Reports and Analysis Centre (AUSTRAC).

In broad terms, the FTR Act provides for the monitoring of the conversion of cash to electronic financial records. Some key provisions of the Act are;

- Identification of persons opening accounts;
- Reporting of significant cash transactions ($10,000 or more);
- International Funds Transfer Instructions (IFTIs); and
- Reporting of cash suspect transactions.

Reports are made to AUSTRAC, and may be made available to revenue and law enforcement agencies including the ACC.

The reporting regime has a number of uses for law enforcement. In particular the transition from cash to electronic banking, directly impacts on the ability of criminals to conceal monies electronically.

On a more sophisticated level, electronic analysis of the AUSTRAC database itself through programmes such as AUSTRAC's TargIT programmes can provide strong indicators of unlawful activity (including significant tax evasion). The Australian Crime Commission, and the National Crime Authority before it, has successfully sought to exploit this information specifically through the Agio and Swordfish Task Forces, and more generally through other operations.

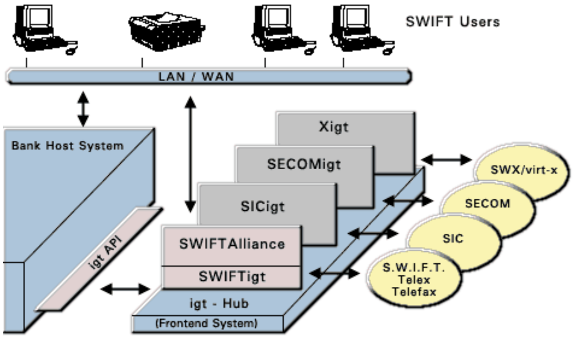
The ACC has documented significant instances where this behaviour is suspected of involving serious tax evasion, or money laundering. At this point the monitoring fails, arguably in a similar way to when false identities are used, and the completion of the unlawful conduct through electronic means is facilitated.

Electronic Banking: SWIFT or INTERNET Banking?

What is the SWIFT Transfer System?

SWIFT is the industry-owned cooperative supplying secure messaging services and interface software to 7,000 financial institutions in 198 countries. SWIFT provides messaging services to banks, broker/dealers and investment managers, as well as to market infrastructures in payments, treasury, securities and trade.

Security is provided at a number of layers, including identification of participants, by use of software, and an authorising regime. Compromise of the system (or the possibility of committing fraud against the system itself) would entail at the least connivance of a number of persons, and the probability of easy detection and identification.



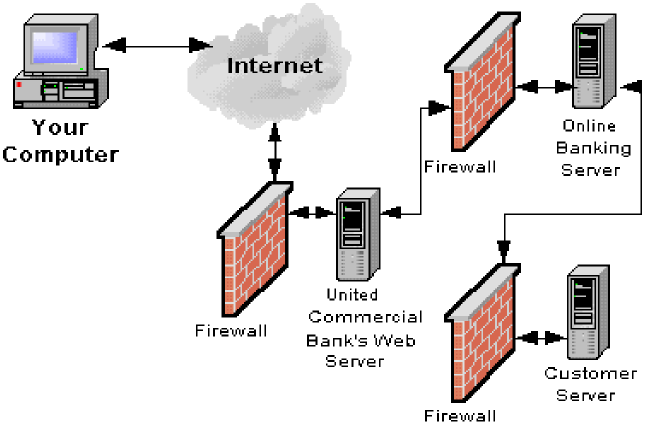
This system is the most commonly used system by Australian banks for providing advice electronically of international funds movements.

International Fund Transfer Instructions (IFTI's) are reportable to AUSTRAC, provided that they are undertaken by a cash dealer. Most of the IFTIs reported to AUSTRAC are from information electronically extracted from SWIFT messages.

This information is available to law enforcement and the Australian Taxation Office, and was the starting point for a number of successful investigations undertaken by the National Crime Authority and its partner agencies.

What Is Internet Banking?

Internet banking is just what you might guess: You access a bank's Web site over the Internet and enter a user ID and password. This gives you access to your account information over a secure server.



The most basic online banking sites let you see account balances, transfer money between accounts, view transaction statements, and pay bills electronically. Some online banking sites let you apply for new accounts and loans, order new cheques, stop payments, and many other services.

A further though less common method of electronically transferring funds is through the use of proprietary systems. These have been available from a number of banks for some time such as HSBC Hexagon accounts.

These were originally used predominantly by businesses with large turnover and /or operating internationally, and users range from merchant banks through travel industry to trustee companies and nominee companies.

Frequently these transactions do not pass through the banks' normal systems and thus in those instances the banks do not report the transaction to AUSTRAC, thus potentially facilitating money laundering and serious tax evasion and avoidance.

Scope for money laundering and other unlawful activity

Internet banking is subject to all the same financial transaction reporting, proceeds of crime and taxation laws as other banking services.

The main significance for regulatory and law enforcement agencies lies in:

> (1) The additional opportunities internet banking, as opposed to face to face banking, provides for criminals to launder proceeds of crime and/or commit fraud and
>
> (2) The additional skills and capacities law enforcement agencies need to successfully investigate money laundering and fraud offences that involve use of internet banking services.

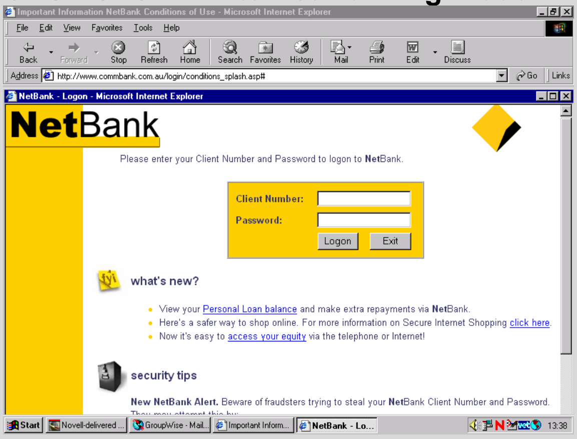
In relation to (1), most financial institutions are conscious of the additional vulnerabilities electronic banking can cause for their organisations. They generally include a number of electronic and procedural safeguards in conjunction with the internet banking services they offer.

Although there is a prevalence of money laundering related sites on the internet, such as tax havens and "how to" sites, the ACC is not aware of any significant money laundering cases where use of internet banking services has played a key facilitating role.

The main attraction internet banking services offer money launderers is the ability to conduct transactions from remote locations and without face to face contact with banking staff. However, many other banking services also offer these facilities. In fact it has become more common in recent years for ordinary bank accounts to be operated without face to face contact between customers and bank staff. It is also not unusual for Australians to operate bank accounts in other countries using telephone and fax instructions. Similarly non-residents operate bank accounts in Australia from overseas for legitimate private and commercial purposes, sometimes without ever travelling to Australia.

In some recent cases, such as the following, safeguards have been bypassed by sophisticated criminals who have successfully defrauded banks or their customers of significant amounts.

CASE STUDY: Internet Banking Fraud



Important Information NetBank Conditions of Use - Microsoft Internet Explorer

http://www.commbank.com.au/login/conditions_splash.asp#

NetBank - Logon - Microsoft Internet Explorer

NetBank

Please enter your Client Number and Password to logon to **Net**Bank.

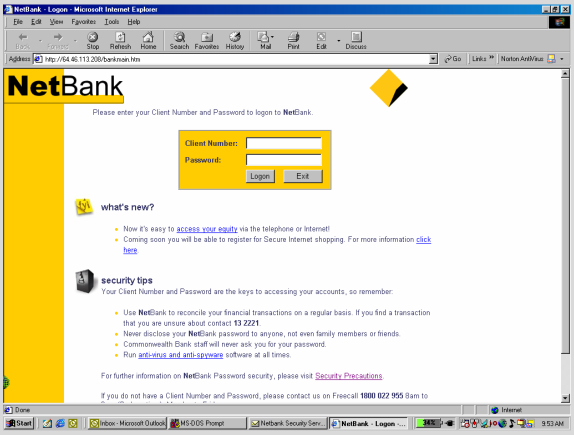
what's new?

- View your Personal Loan balance and make extra repayments via **Net**Bank.
- Here's a safer way to shop online. For more information on Secure Internet Shopping click here.
- Now it's easy to access your equity via the telephone or Internet!

security tips

New NetBank Alert. Beware of fraudsters trying to steal your **Net**Bank Client Number and Password.

Real Commonwealth Site



NetBank - Logon - Microsoft Internet Explorer

http://64.46.113.208/bankmain.htm

NetBank

Please enter your Client Number and Password to logon to **Net**Bank.

what's new?

- Now it's easy to access your equity via the telephone or Internet!
- Coming soon you will be able to register for Secure Internet shopping. For more information click here.

security tips

Your Client Number and Password are the keys to accessing your accounts, so remember:

- Use **Net**Bank to reconcile your financial transactions on a regular basis. If you find a transaction that you are unsure about contact **13 2221**.
- Never disclose your **Net**Bank password to anyone, not even family members or friends.
- Commonwealth Bank staff will never ask you for your password.
- Run anti-virus and anti-spyware software at all times.

For further information on **Net**Bank Password security, please visit Security Precautions.

If you do not have a Client Number and Password, please contact us on Freecall **1800 022 955** 8am to

Bogus Site

In early 2003 a number of Australian Internet Banking sites, including the Commonwealth Bank and ANZ, were the subject of fraudulent compromise.

In each case bank internet customers received emails purporting to be from their Banks, advising of a temporary change of internet address for online banking. Customers would then log onto a bogus site constructed by the offenders which was identical to the Banks Internet Bank logon page.(See screen captures above)

As a consequence the customers would provide their internet bank logons and password to the Bogus site. The offenders would then use those logons and password to transfer funds to another account.

Examples such as this illustrate these ease with which criminal groups can manipulate the electronic environment to perpetuate fraud. Significantly, many online frauds contain a money laundering element; where as electronic funds are transferred to other real or bogus bank accounts. These monies can then be transferred to other electronic media, such as “E Gold”. However, most cash dealers worldwide still require sufficient Identification to withdraw these funds in cash.

Most focus of law enforcement agencies concerned with the effect internet banking services may have on their ability to counteract money laundering and fraud has been on the second area referred to above, i.e., the additional skills and capacities law enforcement agencies need to properly deal with cases that involve computers and/or the internet. Clearly additional skills and capacities are required.

<u>The nexus between ID Fraud and Money Laundering in the Electronic age</u>

This is of serious significance to the ACC, law enforcement, commerce, and the community generally. It is intertwined with the conduct of illegal activity including drug trafficking; the commission of fraud including credit card fraud; damaging the credibility of and faith in systems such as banking and reducing the effectiveness of combative mechanisms such as the regime in place by virtue of the FTR Act.

The ABCI established an Identity Fraud project in 2001, which is continuing under the ACC. Over 2000 recent fraudulent identities have been recorded on the database, which can facilitate linking of offenders with real identities and to crimes.

Future Direction

Depending on the constraints that do or may in the future apply to the ACC, such as resources, some future possibilities for the ACC in this area include the following:

1. Consultation with other agencies, especially AUSTRAC; and with banking and related industries, to monitor appropriateness of current identification and reporting regimes. Maintain consultation in light of current proposals to vary the 40 recommendations of the Financial Action Task Force (FATF); seeking to obtain alternative means to the deterrence and detection of illegal activity including money laundering as it relates to the use of internet banking. Recommend, if appropriate, legislative reform.
2. Consultation with AUSTRAC and the finance industry generally to determine current use of proprietary systems to establish whether or not they may the subject of direct or indirect usage for illegal activity, and consider and recommend changes to allow monitoring of transactions made through proprietary systems, and to facilitate an appropriate reporting regime.
3. Continue the use of Task Forces such as the Agio task Force to identify and commence investigation of money laundering through the internet. Investigative techniques to include use of ACC Special Powers for production of "documents" and examination of witnesses.
4. Continue work with AGEC (The Action Group into the law enforcement implications of Electronic Commerce) to assess the threats and risks for money laundering posed by alternative electronic payment systems and other developing technologies
5. Continuation of the former ABCI Identity Fraud register, to collect data, analyse trends, and facilitate investigations by law enforcement agencies.
6. Continued involvement in consultations to devise methods of verification of identity documents, and to provide integrity of those documents themselves.
7. Establishment of a Task Force to investigate identity fraud.

Credit Card Fraud

Background

Card Skimming[3] has increasingly become one of the predominant crimes facilitated by technological advancement and criminal use of hi-tech knowledge. Following a major incidence of organised ATM skimming in Sydney and Melbourne, and the seizure of, among other things, a skimming device planted in an ATM in Sydney during October-November 2002, the growing problem of fraud based on skimming technology has been highlighted and has attracted attention from law enforcement and Government.

The term "Card Skimming" is used as a more encompassing term than credit-card skimming, because skimming is committed on any card which provides an opportunity for criminal profit-making, such as Medicare cards, credit cards, debit cards, and others.

Card skimming has caused significant losses to the Australian banking industry in the last twelve months. These losses, according to a paper released by the former Office of Strategic Crime Assessments (OSCA), are estimated to have increased 400 per cent primarily from credit card skimming. However, as is presently the case for Identity Crime, there is no dedicated national law enforcement capability to address the matter. Card skimming is a complex criminal activity that is closely linked to Identity Crime (identity theft in particular). In this context it deserves high priority attention from law enforcement.

On 12 December 2002, the Minister for Justice and Customs met with representatives of peak banking and credit card organisations, and law enforcement and regulatory agencies. The meeting examined recent card skimming trends and methodologies with a view to establishing effective fraud prevention, detection and investigation measures. Participants agreed on a number of points which were released in a joint communiqué[4].

Included in this communiqué was an agreement from Senator Ellison to raise the need for new Commonwealth and State offences with his colleagues on the Australasian Police Ministers' Council (APMC) and the Standing Committee of Attorneys-General (SCAG), and to consult APMC on the possible involvement of the ACC in a national approach to credit and debit card skimming issues.

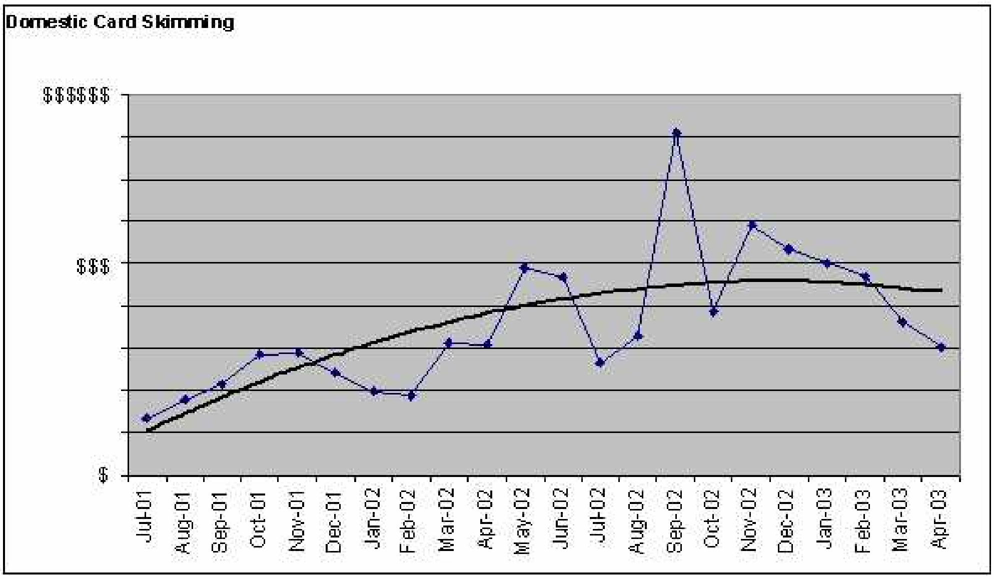
Sophistication and Scope of Activities

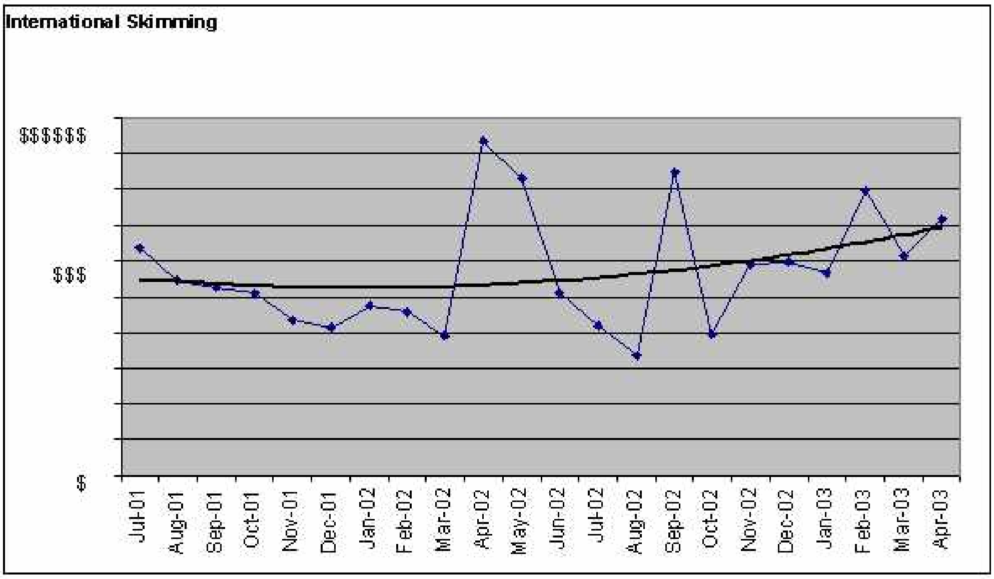
Australian law enforcement investigations have identified that organised crime has embraced technology in a number of ways to facilitate their criminal activities, including card skimming. Rapid advances in technology and e-commerce have made a wide range of highly technical devices available, providing opportunities for criminal exploitation. For instance, using components readily available in Australia, a person with technical knowledge can easily adapt a magnetic strip

[3] Card Skimming is a process whereby data are electronically captured from the magnetic strip of legitimate cards and then re-encoded onto a counterfeit card.

[4] Communiqué, Senator Chris Ellison, Minister for Justice and Customs, Initiatives to Deal with Credit Card and Debit Card Skimming, 12 December 2002, Parliament House, Canberra.

reader designed for legitimate purposes to operate as a portable skimmer.[5]





Current statistics on Domestic and international skimming

Consequently, law enforcement agencies are faced with the pressing need to employ technical and specialist resources and use advanced technical tools to address criminally abused technology. This is resource intensive in terms of the acquisition of current technology and requirement for ongoing training of staff.

Police investigations, particularly in NSW, indicate that organised criminal groups have been using portable skimmers to obtain credit card data for some time through service stations, restaurants and taxis. In an interstate ATM skimming operation, a sophisticated skimming device including a miniaturised camera to record PIN details was inserted into or attached to an ATM in Sydney.

[5] Magnetic Strip Readers have numerous legitimate commercial and private sector uses.

Although the term skimming derives from the early method of merchants reading card details using skimmers, new methods of obtaining credit card and debit card data are being devised. In addition to Internet banking fraud, information from Canada, Malaysia and Europe indicates that criminals are now using ‘wiretapping’ to intercept data cables from commercial premises such as department stores to copy credit card and EFTPOS information and transmit it overseas for fraudulent use. There are also reports of computer programs being downloaded into ATMs to capture card details and allow them to be transferred to a laptop computer.

Law enforcement intelligence suggests that organised criminal networks, especially Asian groups, involved in card skimming have strong overseas links particularly with Malaysia, Indonesia, Hong Kong, and Thailand.[6] Most skimmed credit card data is transmitted overseas, usually to South-East Asia. There, the data is recorded on plastic credit cards embossed with Australian bank logos, which are sold or used for retail purchases; advantage is taken of the delay in processing international transactions before the victim or his/her bank becomes aware of the fraud.

Some locally skimmed data is loaded onto forged credit cards in Australia but most forged cards used in Australia are loaded with data skimmed overseas. However, current intelligence indicates a trend towards local usage of data skimmed in Australia.[7]

Card skimming is considered a high impact threat because:

- Card skimming is increasingly being perpetrated by organised crime groups in conjunction with other criminal activities such as drug trafficking, money laundering, identity crime, and potentially arms trafficking[8].
- Credit card skimming has inflicted a 400 per cent increase in losses on the Australian banking industry during the past twelve months alone. The sharp increase in this criminal activity is potentially going to experience further dramatic increase over the next one to two years.
- Credit card skimming is estimated to cost the Australian banking industry as well as businesses and consumers more than $300 million per year.[9] It also reduces confidence in the financial institutions operating under Commonwealth law and the integrity of modern commercial systems.
- The social implications of card skimming are serious. Victims of Card Skimming experience personal distress as they are left with debts to pay until they can establish their bona fides and restore their credit reputation. The rising incidence of credit card skimming is leading to the introduction of new controls that would shift the onus of harm from the financial sector to individuals. Such countermeasures are likely to impact adversely upon individuals.
- The existing limitations in the Australian national law enforcement response capability to card skimming is likely to provide opportunity for criminal exploitation, especially to trans-national criminal groups who can potentially

[6] R. Smith, *Plastic Card Fraud,* Australian Institute of Criminology “Trends and Issues Paper No. 71”, July 1997; and ABCI, *Organised Credit Card Skimming*, May 2002.

[7] ABCI, *Organised Credit Card Skimming*, May 2002.

[8] OSCA, *Fraud – Credit Card Skimming*, No. 01/02, September 2002.

[9] ABCI, *Organised Credit Card Skimming*, May 2002.

shift their card skimming activities to Australia. Factors include the increasingly tighter controls being introduced in North America, Europe and Asia; and the lax legislative and deterrence environment in Australia in terms of associated criminal penalties and jurisdictional differences.

<u>CASE STUDY:</u> Corruption and counterfeit credit card syndicates.

On 19 September 2002, the Taiwan Ministry of Justice (MJIB) announced the neutralization of a major counterfeit card syndicate. An initial series of raids led to the arrest of 9 males, <u>including 2 senior IT engineers from one of the main financial institutions in Taiwan</u>. Also seized were 28,000 base cards, and recovery of some 16,000 credit card track data. One of the suspects arrested has alleged that over 1 million sets of customer full track data was sold to criminal syndicates. The prosecutor in charge of this investigation has authorized the dissemination of the 16,000 account data to affected issuers.

Australian State and Federal agencies have identified that Asia/Pacific criminal groups are also targeting Australia with this activity.

Recent matters such as this highlight the willingness of organised trans-national criminal groups to employ emerging technologies and to infiltrate financial institutions.

<u>Card Skimming: Simplicity in the Cyber Age</u>

Card skimming is now no longer the domain of technicians or highly qualified individuals. With advances in technology and the proliferation of commercial software and hardware in the domestic market, card skimming is now within the capacity of the average computer user.

The proliferation of Card Skimming is now less about technology and more about opportunity and organisation. The equipment and training is readily available on the internet, as the following diagram illustrates;

Anatomy Of A Skimmed Credit Card.

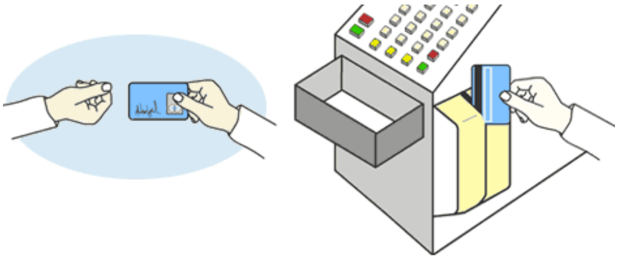


Figure 1 (Card taken by shop assistant for swiping on EFTPOS transaction)

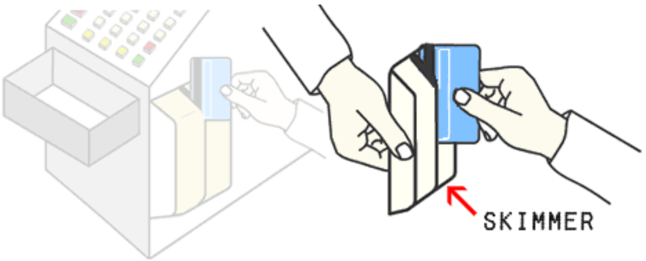


Figure 2 (Card data is then “Skimmed” in portable device)

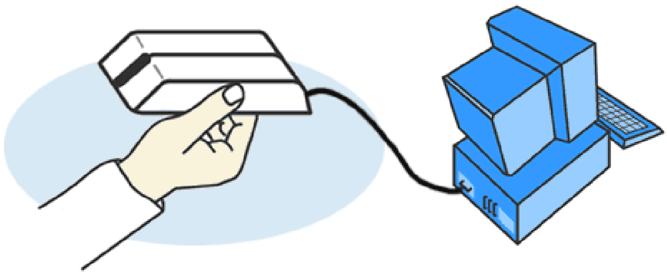


Figure 3 (Card data downloaded to skimming device to PC for copying)

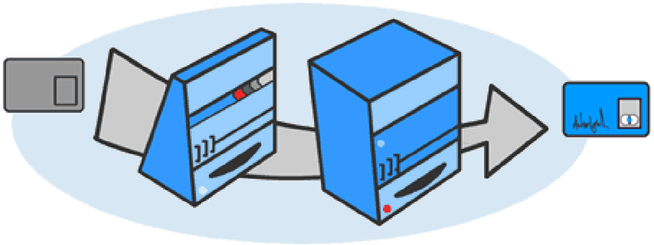


Figure 4 (A blank card is embossed with the card holder details from PC)

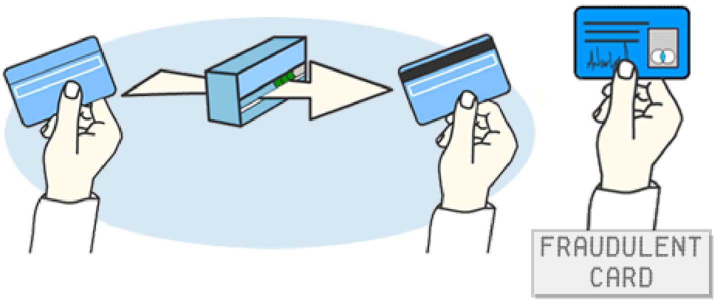


Figure 5 (New card is then re-encoded with stolen card data, ready for use)

Overview of Current Intelligence

Although card skimming appears to operate at a number of levels, it is being perpetrated by innovative and sophisticated organised crime groups in conjunction with other serious cross-jurisdictional and trans-national criminal activities including drug trafficking, money laundering, and potentially arms trafficking.

Investigations by the former NCA revealed a growing use of fraudulent and skimmed credit cards by organised crime groups. Thailand and Malaysia were found to be the main sources of skimmed credit cards. Card Skimming has been identified in recent intelligence assessments by the former ABCI as being one of the technology-driven emerging national threats.

New South Wales is now the centre of law enforcement investigations into credit card skimming, with two specialised NSW Police Service task forces investigating domestic and international manufacture of forged credit cards using skimmed Australian credit card details.

Normal jurisdictional restrictions limit the effectiveness of their investigations beyond State boundaries. Victoria is also establishing a similar task force. While there is close cooperation between the major credit card companies and the NSW Police Service, there is no current coordinated national mechanism for intelligence gathering on banking and credit card and debit card fraud.

The former OSCA predicted in 2002 that the threat of card skimming would continue to rise dramatically in Australia over the next year or two.[10] OSCA based its assessment on a number of contributing factors, including:

- Lack of legislation to restrict the importation of credit card blanks, embossing machines, skimmers and counterfeit paraphernalia.
- Lack of uniform jurisdictional agreement on what comprises an offence and lack of deterrence factors in associated criminal penalties.
- As a result, the opportunity for criminal exploitation of jurisdictional differences is readily available for unimpeded cross-jurisdictional criminal operation.
- Lax merchant practices and systemic weaknesses in associated banking practices including card fraud investigation practices.
- Lack of, and perceived delay in introducing, card chip technology is highly likely to contribute to the problem.
- Lack of consumer awareness of card security.
- An identified gap in Australian law enforcement intelligence holdings as well as an acknowledged need for a national coordinated intelligence gathering mechanism by law enforcement to address card skimming.

Relevance of Criminal Activity

Card skimming meets the key criteria for federally relevant criminal activity as defined in the *Australian Crime Commission Act 2002*. It substantially impacts on the banking system, which is regulated by Commonwealth law and fraudulently

[10] OSCA, *Fraud – Credit Card Skimming,* No. 02/02 September 2002.

obtained cards are often imported into Australia. Skimmed cards may be used to defeat Commonwealth social security systems.

Card skimming has been demonstrated to be multi-jurisdictional and trans-national in nature, often involving interstate and international trafficking of stolen personal and financial data, as well as credit and other cards.

The experience of law enforcement agencies in Australia and overseas has shown that the use of special powers, applied to complement other traditional investigation methods, is likely to provide an enhanced capability to investigate this type of criminal activity. It will lead to effective prosecution and proceeds action, intelligence development, as well as reform, regulatory and policy action.

ACC Response to Card skimming

The ACC may be in a position to contribute to a national response to this problem by:

- focusing on the multi-jurisdictional and national dimensions of card skimming;
- utilising specialist financial investigation resources to complement the expertise of partner agencies;
- using cybercrime investigation methods and forensic techniques;
- provision of a national intelligence database on card skimming for enhanced intelligence exchange. This role would fill a gap in current law enforcement arrangements on card skimming;
- providing enhanced insight into the problem and undertaking intelligence collection and target development; and
- contributing to appropriate legal, administrative and policy responses.

Future Direction

1. Card Skimming has increasingly become one of the predominant crimes facilitated by technological advancement and criminal use of hi-tech knowledge.

2. Loss associated with card skimming has increased 400 per cent in the last 12 months, primarily from credit card skimming.

3. Card skimming is increasingly being perpetrated by organised crime groups in conjunction with other criminal activities such as drug trafficking, money laundering, identity crime, and potentially arms trafficking.

4. Card skimming is multi-jurisdictional and transnational criminal activity. It has economic, political and social implications of national significance which require further detailed analysis.

5. Although many of the specific offences associated with card skimming are fraud under State Criminal Codes, card skimming is appropriately regarded

as federally relevant criminal activity and will require priority attention from national law enforcement.

6. ACC's current assessment is that further intelligence work is required before card skimming could be deemed to satisfy the Phase 1 requirements of the Evaluation Model.

7. In May 2003, the ACC board approved National ACC "Intelligence Operations" for both Identity Crime and Card Skimming.

Term of Reference:

THREATS TO NATIONAL CRITICAL INFRASTRUCTURE

Lucas Heights - No Nuclear Reactor protest
Glen Lockitch '98
WE DEMAND INDEPENDENT PUBLIC INQ INTO REACTOR ACCIDENTS NOW!
NYSE
Melissa Virus

The ACC Role In Electronic Critical Infrastructure Protection

Historically, the NCA's narrow role in the investigation of complex national organised crime, has precluded any active participation in the investigation of electronic critical infrastructure attack. However, since the commencement of the ACC Cybercrime Program in 2001, the ACC has taken a more active interest in this area because of possible threats posed by organised criminal activity to both the Australian information and the physical infrastructures.

With the new functions in the ACC Act for the ACC to advise the ACC Board on national criminal intelligence priorities, the ACC has even more reason to maintain its liaison and intelligence work in these areas, as they could pose targets for serious and organised crime.

Tools such as the ACC coercive powers and national criminal intelligence framework could be invaluable in regards to investigating critical infrastructure attacks, especially those against government institutions.

There is also evidence that criminals are willing to use such electronic attacks to gather intelligence, and to further their enterprises. The ACC's multi jurisdictional focus on the high-end of criminality, and on emerging threats, provides a unique tool to Australia's response to this high risk and emerging form of criminality.

CASE STUDY: Cyber-terrorism a mouse click away?

Between December 1999 and April 2000, the sewerage treatment facilities of Maroochydore Shire Council, Queensland, came under sustained electronic attack. That attack resulted in an environmental disaster which saw millions of litres of raw sewage spill into rivers, parks and the grounds of a Hyatt Regency hotel. The matter was forwarded to the Queensland Police for investigation.

As a result an ex employee, Vitek Boden, was intercepted by police in a vehicle which contained a laptop computer, with wireless access to the sewerage control system. He was later charged found guilty on 30 charges involving computer hacking, theft and causing significant environmental damage, in what was described as the world's first environmental vandalism case[11].

[11] R v Vitek Boden

The Vitek Boden case is now used world wide as an example of critical infrastructure (hacking) attack and the opportunities for Cyber-terrorism. Whilst Boden's motive was more related to financial gain than terror, this case has highlighted the fact that the convenient use of Information Technology, outstripped the possible consequences of breaching that technology.

The fact is that all computer systems connected to the internet, or with remote access, have been or will be, subject to electronic attack or probing at some point. Although this probing is silent and innocuous, a resulting successful malicious electronic attack can be devastating. Further, the target and attacker could be in the same building, or separated by continents. This is the world of hacking.

Malicious electronic attack can take a number of forms including;

1. Hacking into a computer network by an individual,

2. Distribution of malicious software (such as viruses) which enter computer systems in order to execute a payload,

3. Denial of service attacks, where the internet ports or email of the target computer system is bombarded with data to prevent it from communicating,

4. Redirection, or spoofing, of website traffic away from its intended destination.

Regulation of the Internet electronic environment to prevent such attacks is currently non-existent. Some jurisdictions in the world cater for such activities with specific criminal offences, many jurisdictions, notably the third world, do not..

Historically, the NCA/ACC has not investigated Critical Infrastructure attacks unless they related to organised crime. There has been anecdotal evidence in the past, of suspected organised crime electronic probing of Commonwealth Internet gateways.

In December 2002 OSCA released a strategic assessment addressing the *Long-Term Criminal Risks to the National Information Infrastructure (NII).*[12]. That assessment emphasised the risk not only from electronic attack, but also *exploitation*.

Exploitation of software or procedural vulnerabilities is arguably the route taken by all electronic attacks. This also includes the “social engineering” of staff members to obtain passwords, which is particularly relevant for organisations with information systems such as the ACC, which may be the target of organised crime.

These types of threats have meant that the ACC must look to partnerships and protect its own systems from the possibility of malicious electronic attacks.

[12] Long-Term Criminal Risks to the National Information Infrastructure (NII), OSCA, 2002.

ACC Response to Electronic Critical Infrastructure Attack

The ACC recognises that its electronic intelligence assets are a tempting target which requires physical and electronic protection. This includes maintaining a protective regime for the ACC electronic assets against such attacks, in partnership with other organisations, such as AUSCERT.

Only by vigilance and maintaining an effective IT Security framework can the ACC protect its own assets from malicious electronic attack.

Whilst the ACC does not normally investigate these types of attacks, it recognises that its National Criminal Intelligence role means it must maintain strong partnerships with stakeholders in this area. Some key groups which the ACC has joined in partnership include;

- AGEC (the Action Group into the law enforcement implications of Electronic Commerce) chaired by AUSTRAC, which has a focus on banking, money laundering and electronic payment systems
- Information Infrastructure Protection Group (IIPG) chaired by AGD, with a focus on threats to the national critical infrastructure information
- Electronic Security Coordination Group (ESCG) chaired by NOIE
- AUSCERT (Australian Computer Emergency Response Team) who have recently been contracted to provide Alerts and Warnings, and an Incident Reporting Scheme

The ACC has also recently provided intelligence support to the AHTCC and jurisdictional Cybercrime Task forces which have been examining the "hacker" community in Australia. Persons on interest to these investigations have been linked to a number of electronic attacks on Australian and overseas, on both private and government computer systems.

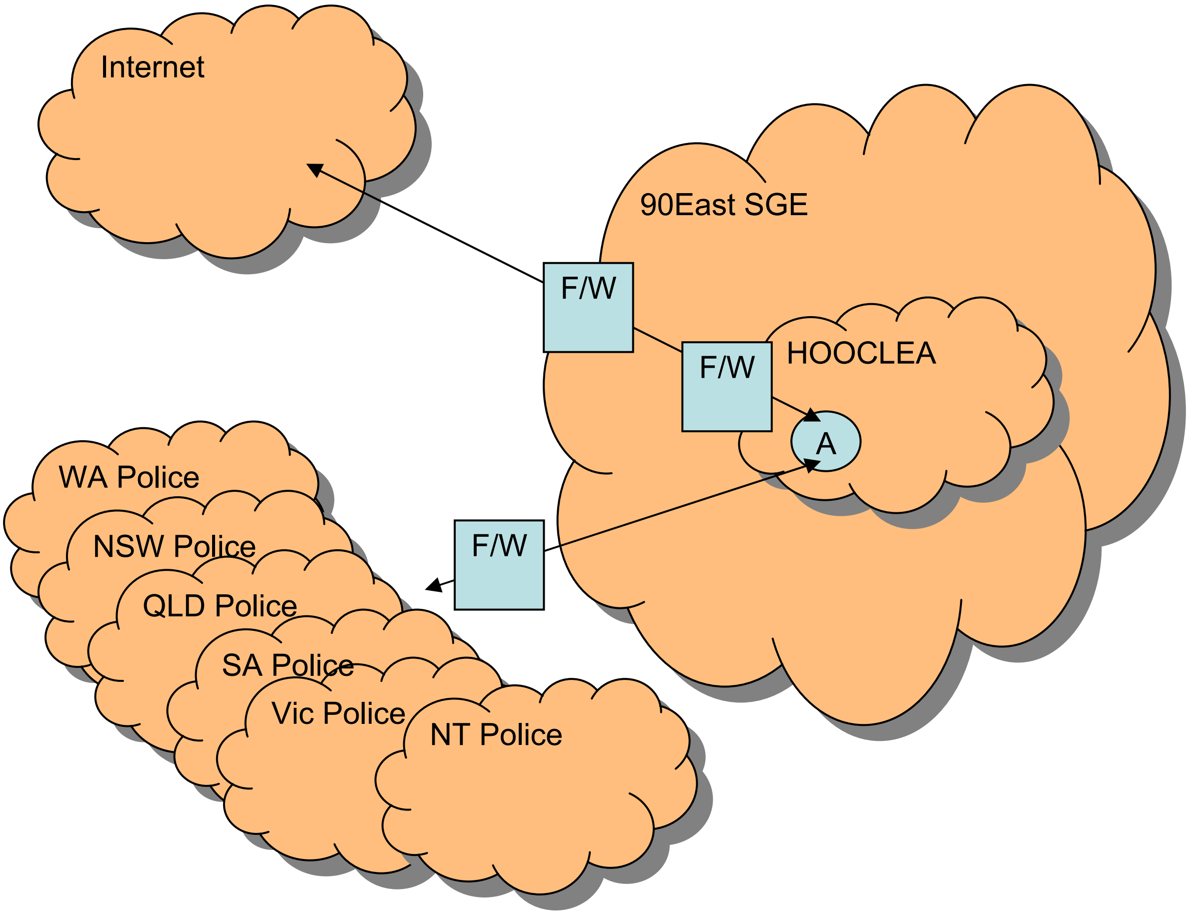
Protecting Our Electronic Assets

With the establishment of the Australian Crime Commission (ACC) on the 1st January 2003, one of the first priorities from an IT Security perspective was the bringing together three technically different environments.

The NCA had a classified national network at the Highly Protected (HP) level. The ABCI had a national network linking all State and Territorial Police jurisdictions together, the infrastructure at the HP level. The current IT activities are focused around creating a single national network to meet the business needs of the ACC.

From a network architecture perspective, this new environment will have the primary internet access through the 90East Secure Gateway Environment (SGE) which has been accredited by Defence Signals Directorate (DSD). The ACC and other law enforcement organisations sit within a segregated environment known as the HOCOLEA controlled area.

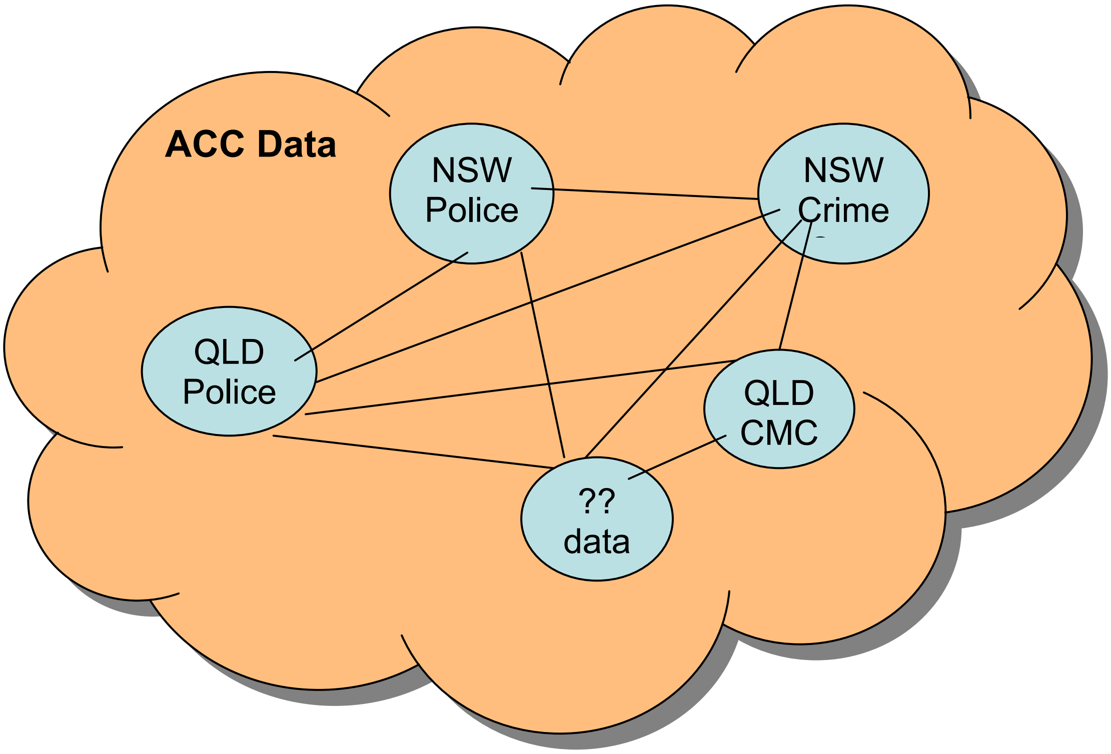
Outline of ACC Network



Information Management

Within this multi facetted environment we have the information flows of jurisdictional information and security models that do not necessarily reflect the Commonwealth Protective Security Manual. A new model needs to be developed that fits the nature of the ACC business together with those of our Partner organisations.

Current and New Information



This model gives an example of the jurisdictional information sets held on ACC IT Systems that the ACC may not be the owner of, but is the custodian of.

IT Security and Cybercrime aspects

If we look at the business of the ACC, we must protect our operations from attack from those criminal elements that we target who would wish to compromise our operations and information.

To do this we have an environment that is protected from the internet by a series of Firewalls (F/W) and monitoring systems, which are designed to provide an alert should anyone try to penetrate our systems. These systems are undergoing a review currently to look at the Threat and Risk assessment and then to redesign the environment to mitigate those threats and risks.

Both the current and next generation of Applications being developed for the ACC additionally require an enhanced monitoring capability to combat the future threats, and to provide the ACC with enhanced capabilities.

Future Direction

In particular the ACC’s role of National Criminal Intelligence coordination means that it must now consider;

1. An enhanced contribution to sharing of intelligence relating to electronic critical infrastructure attacks, through continued liaison and intelligence sharing with key agencies and groups,

2. Promote and participate in a proactive “hacker” intelligence gathering regime,

3. Promotion of electronic attack reporting and information management, not only in government, but also in private enterprise, and

4. Continue to develop protection for the ACC electronic information systems to prevent compromise.

5.MAINTAINING THE CYBERCRIME TOOLBOX

Intelligence

Partnerships

Computer Forensics

Legal and Policy

Research and Development

Training

Electronic Evidence Trends

The ACC has seen an increase in computer seizures, and examination of electronic evidence, of 360% since 1998. A base level of cyber-forensic capability and protection of technology is essential to the ACC. The ACC also requires a capacity to investigate crimes on the ACC's main menu which utilise computers, as well as a capacity to investigate crimes against computers.

The ACC response to Cybercrime has been based on the sound principles of the *Police Commissioners 2001-2003 Electronic Crime Strategy*. These strategies include includes

In maintaining the holistic approach to combating Cybercrime, the ACC has identified four key areas in which it and the LEA community must develop.

These focus areas include;

⇒ National Cybercrime Intelligence collection and analysis,
⇒ Partnerships,
⇒ Maintaining a technical response capacity, and
⇒ Policy and legal reform.

1. National Cybercrime Intelligence Collection

The *Australian Crime Commission (ACC) Act 2002* defines the functions of the ACC under section 7A. Some of these functions will require the ACC to maintain an active interest in Cybercrime as well as other crime areas to be able to perform its functions, including:

⇒ *to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence;*
⇒ *to provide strategic criminal intelligence assessments, and any other criminal information and intelligence, to the Board;*
⇒ *to provide advice to the Board on national criminal intelligence priorities;*

To maintain this national database, prepare strategic and other intelligence assessments, and continuously assess the issue of Cybercrime in context with other crime types, the ACC will need to maintain close working relationships with Commonwealth, State and Territory agencies, taskforces and related forums involved in Cybercrime. To solely rely on external agencies to provide the information and intelligence on Cybercrime is to risk the effectiveness and efficiency that the information and intelligence processes need to be timely and accurate.

Outside of the requirements of the Act, the ACC recognises that most modern sophisticated crimes all have components of technology such as computers and

Outside of the requirements of the Act, the ACC recognises that most modern sophisticated crimes all have components of technology such as computers and the Internet, that require the ongoing development of operational expertise and capability to gather intelligence and investigate. For these reasons the ACC will remain actively involved in monitoring Cybercrime to make sure it is able to be involved in addressing crimes involving technology both proactively and reactively.

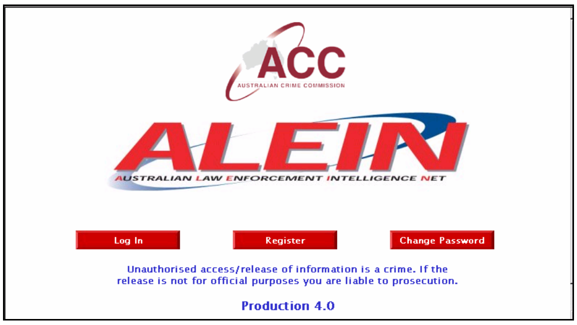
In Cybercrime as in other crime areas, the quality of the ACC's service of information and intelligence greatly depends on input from other agencies (in response to the National Criminal Intelligence Priorities and Collection Requirements). As such much of the ACC intelligence production programme will necessarily be reliant on information provided through other sources. In relation to Cybercrime the key partner, and conduit through which much of the input will come, is the AHTCC.

Cybercrime Information management and the ACC National Desks

The integrated ALEIN National Information Desks provide the ACC with an information sharing and notification tool, accessible to all of the jurisdictions.

The strengths of the Information Desks include a User friendly interface assessable in all jurisdictions, a secure intranet for LEA intelligence product and alerts, a collation point for intelligence product from all jurisdictions, and the ability to "broadcast" Alerts to the jurisdictions.

The desk cover a board range of crime areas, which in turn have all had exposure to the criminal use of emerging technology.


ACC
AUSTRALIAN CRIME COMMISSION
ALEIN
AUSTRALIAN LAW ENFORCEMENT INTELLIGENCE NET
Log In
Register
Change Password

Unauthorised access/release of information is a crime. If the release is not for official purposes you are liable to prosecution.

Production 4.0

These Desks are an important tool not only in National information and Intelligence management, but also in promoting partnerships with the jurisdictions. As such, the ACC is currently facilitating the management of the "E Crime" Desk in partnership with the Australian Hi Tech Crime Centre.

All of these desks will continue to be a vital tool, which is available to the ACC to combat Nationally significant threats such as Cybercrime and criminal use of technology in traditional crimes.

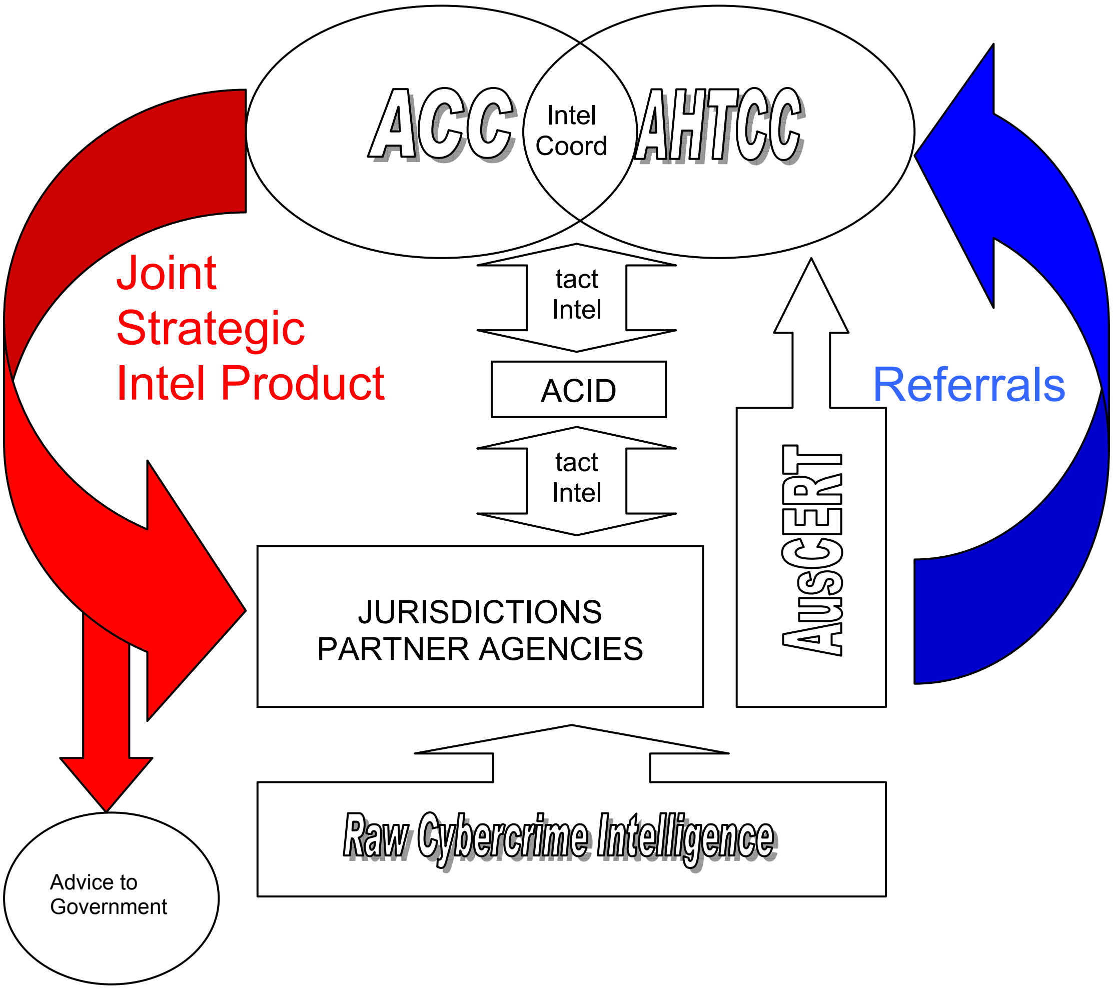
ACC Cybercrime Taskforces and Liaison Relationships

The ACC is a small agency with an important role for criminal intelligence in Australia. It cannot hope to do a good job of assessing national criminal intelligence priorities and the underlying data without having close and intelligent liaison and involvement in operational work with the greater law enforcement and regulatory community. Cybercrime intelligence being a part of criminal intelligence can only hope to achieve success through close working relationships with the relevant technical areas of this community.

The ACC and the Australian Hi Tech Crime Centre

The recent forming of the Australian Hi Tech Crime Centre (AHTCC), and the inclusion of the ACC as part of the Hi Tech Crime Managers Group (HTCMG), highlights the importance placed on national strategic Intelligence partnerships. The AHTCC is intended as a coordinating centre for complex Hi Tech Crime Investigations, and will be a focal point for intelligence gathering in this area, and thus an important partner to the ACC.

The diagram below illustrates the proposed Cybercrime intelligence relationship between the ACC, the AHTCC, AUSCERT and jurisdictions.

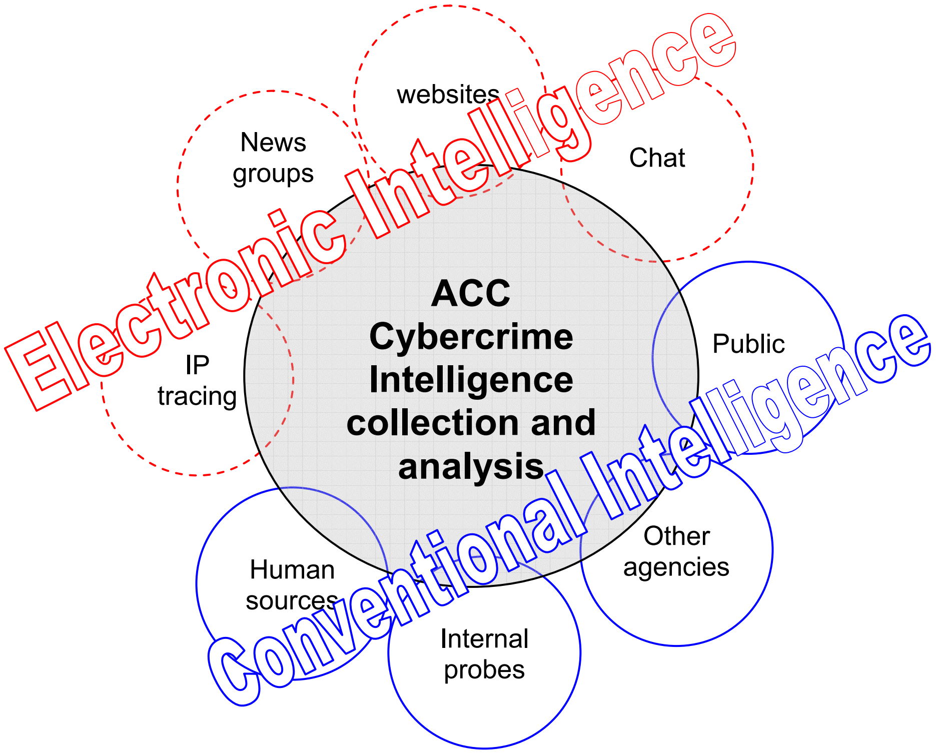

ACC
Intel Coord
AHTCC
Joint Strategic Intel Product
tact Intel
ACID
tact Intel
Referrals
AusCERT
JURISDICTIONS PARTNER AGENCIES
Raw Cybercrime Intelligence
Advice to Government

However, whilst the relationship between the ACC and AHTCC is important in coordinating Cybercrime intelligence, the backbone of intelligence gathering in this area is the jurisdictions and the general public. There is a direct relationship between the raw intelligence gathered by the jurisdictions and the ability of the Commonwealth to predict Cybercrime trends and provide a coordinated response.

ACC Cybercrime Intelligence Gathering

To deal with crimes involving or being facilitated by technology the ACC seeks to remain at the forefront of intelligence gathering to collect, correlate, analyse both the developing technologies and related criminal uses. Presently this is being done through:

- open source information collection involving a heavy Internet focus.
- regular liaison and involvement with other government agencies and forums involved in Cybercrime related intelligence and investigative work, described in detail below.
- supporting and being directly involved in joint law enforcement agency operations to gather intelligence on and investigate Cybercrimes.
- attendance at new technology industry conferences, presentations and exhibitions to help assess the latest and soon to be released developments.



Sources of Cybercrime Intelligence

From this work it is recognised that there are further opportunities to strengthen the ability collect and manage Cybercrime information and intelligence, predominately through improvements in adopting new technology.

Improving ACC On-line Intelligence Gathering

Open Source Information/Intelligence (OSI) is one area that is of great importance in Cybercrime intelligence gathering. The Internet also provides many forms of OSI, some public but many others effectively private by the nature of the software used.

The efficient and effective collection, exploitation and management of OSI is emerging as a key and enduring challenge for all agencies of the community, and one that could benefit from a coordinated and cooperative approach. The ACC will also need to provide the national mechanisms to harness the community's distributed OSI-related knowledge and experience, and make it more readily accessible for the benefit of all.

OSI material is readily available on the internet from a number of different sources including;

- Websites,
- IRC (Internet Relay Chat),
- Newsgroups, and
- Emailing lists.

Internet Search engines, such as Google, offer the internet user a tool with which to trawl this massive data base.

Some of the many internet search engines.

From an intelligence gathering perspective, Internet communications, much like open source information, offer a rich opportunity to gather intelligence that is not as yet being properly utilised. The amount of intelligence available on the internet is also a large and growing threat to efficient lawful interception capability.

Online investigations and intelligence gathering is an essential part of many Cybercrime Investigations. Currently law enforcement agencies undertake this role in a passive sense. The ACC NCU currently deploys a covert internet capacity for passive OSI gathering.

However, overseas law enforcement agencies are more aggressive in the manner they collect this intelligence online. Several software tools are currently under development, such as the FBI system, which aggressively search the internet for intelligence and evidence.

The development of Australian LEA orientated automated internet intelligence gathering software, should be pursued as a means to identify those criminal elements which make the internet their home.

Future Direction

The ACC role in National information (Intelligence) management is of critical importance in the area of Cybercrime. Because of the fluidity and speed of Cybercrime attacks, timely intelligence product is essential.

In order to keep pace with the intelligence responsibilities associated with the criminal use of technology the ACC proposes to;

1. Continue to develop information management plans with the jurisdictions to enable a rapid National consistent collection of Cybercrime related intelligence,

2. Pursue working partnerships with other agencies and private enterprise to improve the flow of Cybercrime related intelligence, and

3. Improve the Electronic (Internet) intelligence gathering and analysis capacity of the ACC through the use of advancing searching software and hardware.

2. Partnerships

To improve its own intelligence, policy and law reform work in respect to Cybercrime, the ACC is partnered with the following agencies, committees and groups that reflect the forefront of Australian Commonwealth efforts to deal with technology related crimes. They are:

- AFP and the evolving Australian Hi-Tech Crime Centre (AHTCC)
- State and Territory Police Cybercrime forensics and intelligence areas
- AGEC (the Action Group into the law enforcement implications of Electronic Commerce) chaired by AUSTRAC, which has a focus on banking, money laundering and electronic payment systems

- Information Infrastructure Protection Group (IIPG) chaired by AGD, with a focus on threats to the national critical infrastructure
- Electronic Security Coordination Group (ESCG) chaired by NOIE
- Telecommunications Interception groups and committees such as LEAC (Law Enforcement Advisory Committee), SNC (Special Networks Committee), IATG (Inter Agency Technical Group) and ICC (Interception Consultative Committee) chaired by ACA, ASIO, AFP, and AGD respectively
- AUSCERT (Australian Computer Emergency Response Team) who have recently been contracted to provide Alerts and Warnings, and an Incident Reporting Scheme

These relationships exist now and are being strengthened, but Cybercrime is still a relevantly new, growing and rather misunderstood area of crime. Consequently this work is not without problems – reflecting the situation being faced all around the globe. As with the technology itself it is fair to say that any law enforcement or regulatory agency will be facing similar intelligence and forensics challenges even though their focuses may be different.

In response to this Cybercrime groups and committees have formed to share the collective experiences, expertise and perspectives of agencies to facilitate intelligence sharing on methodologies and techniques, as well as to develop tools, procedures and capabilities to address the many issues.

Only by maintaining and developing these relationships with key agencies and forums, will there exist the timely flow of information and intelligence to feed into trend, threat and opportunity analysis, alerts and early warning systems.

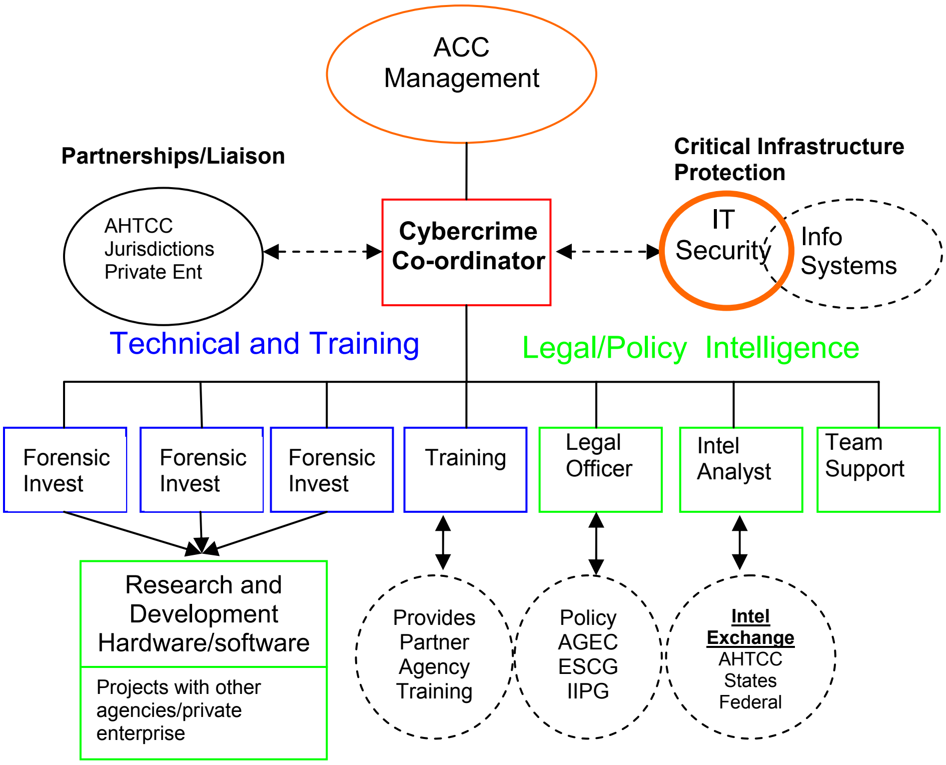
3. Maintaining a Technical Response capacity

The ACC Cybercrime Program has successfully developed an integrated holistic response for the ACC in regard to the criminal use of emerging technology. This coupled with an improved data interception capability, will significantly enhance the ACC ability to respond to its National role.

This section examines the two practical Cybercrime interfaces of the ACC;

⇒ The National Cybercrime Unit, and
⇒ Data (Internet and Email) Interception.

The ACC National Cybercrime Unit (NCU)



The role of the ACC NCU is to act as an “interface” for the ACC in matters of criminal related use of emerging technology, and support the ACC global outcomes.

The NCU has developed a multi-disciplinary team response, and is an integrated support tool of the ACC. This multi disciplined response provides a unique holistic response to the criminal use of emerging technology, including providing solutions to criminal use of encryption and internet secure communications.

This holistic approach includes the key areas of:

1. Cybercrime Intelligence

The intelligence function of the ACC is well defined under the ACC Act. The ACC NCU intelligence unit collects and analyses Hi Tech Crime intelligence from all sources, internal and external, to provide advice on threats and opportunities.

This intelligence role includes:

- Production of Cybercrime strategic intelligence
- Cybercrime operational intelligence, including target development
- Identification of emerging technology threats and opportunities
- Maintaining Cybercrime intelligence partnerships with other agencies.

The ACC and Australian Hi Tech Crime Centre (AHTCC) have drafted an MOU to allow a closer working relationship in the area of Cybercrime. The MOU allows for the provision of ACC Cybercrime intelligence support to the AHTCC. This symbiotic relationship will increase the flow of national Cybercrime intelligence and should enhance both organisations' capabilities.

2. Forensic Computer Examination

The in-house Forensic computer examination capacity of the NCU, fulfils one of the cornerstones of the ACC Cybercrime program. This capacity allows the ACC not only to retrieve and analyse electronic evidence, but also to work as part of a coordinated response with partner agencies as the need arises.

The NCU Forensic Computing capacity includes:

- Three primary forensic support laboratories, Brisbane, Sydney and Melbourne with a capacity to support other offices nationally as required,
- Latest technical and software tools enabling retrieval and examination of electronic evidence and password encryption cracking,
- Three highly qualified computer forensic examiners, with dual roles of Research and Development, and Cybercrime training,
- An advanced and respected technical research and development program.

The NCU forensic computing capacity is also backed by established laboratory and electronic evidence handling procedures.

3. Technical Research and Development

Technical Research and Development is essential to keep pace with the rapidly changing Cybercrime environment. The NCU has a research and development program which includes hardware and software, methodologies and work practices. An integral part of this program is a cooperative effort, by also supporting worthwhile projects undertaken by other agencies.

The NCU Technical Research and Development program has included support for:

- The NSWPOL SMART forensic imaging software project,
- Support of the annual Australian Computer Crime Managers Group, 2002 Computer Forensics Workshop,
- Development of a portable imaging device for Law Enforcement and,
- IT Security, Personal Digital Assistant (PDA) Project.

4. Cybercrime Training

The unit has developed a training package in conjunction with the AFP, for all staff, including seconded staff, to enable them to identify and deal with cybercrime issues. The course consists of a four week on-line component, and a two day hands on workshop.

The ACC Cybercrime training program is well on target with 40% of all operational staff having completed the course. This includes a number of external partner agencies including ATO, ACCC, NSWCC, state police and AUSTRAC.

Additional training partnerships are also being fostered with regulatory bodies in the law enforcement community to ensure the exchange of information and training techniques to combat of cybercrime.

5. Forming Partnerships

The NCU represents the ACC in a number of important National Cybercrime Forums including the AHTCC High Tech Crime Managers Group (HTCMG), Electronic Security Co-ordination Group (ESCG), Information Infrastructure Protection Group (IIPG) and Action Group into the law enforcement implications of Electronic Commerce (AGEC).

As previously mentioned the ACC and Australian Hi Tech Crime Centre (AHTCC) have drafted an MOU to allow a closer working relationship in the area of Cybercrime. This is a critical partnership for both agencies, as it allows for the coordination of intelligence to and from the Commonwealth and jurisdictions

In this respect the ACC NCU is already working closely with the AHTCC and the jurisdictions on a number of joint projects relating to Australian Hacking groups and serious network intrusions.

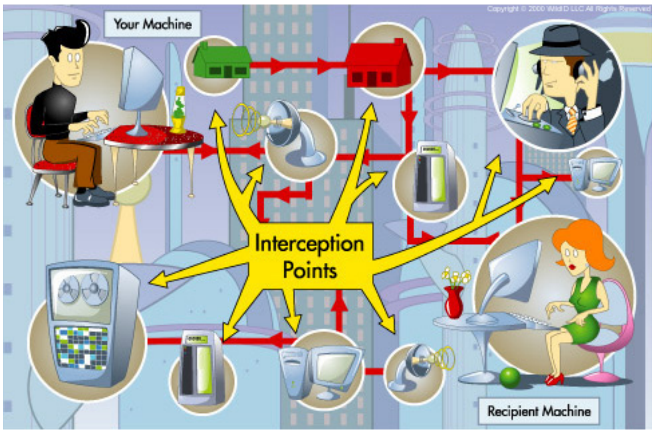
6. Critical Infrastructure Protection

One of the first key goals on the ACC Cybercrime program was that of protecting the ACC Electronic information assets, from malicious electronic attack or electronic probing. This includes the purchasing and installation of hardware and software to monitor and protect the integrity of the ACC Electronic Information systems.

In 2002, the ACC Cybercrime program financed the employment of a full time IT security adviser. This adviser works closely with ACC IT and security, to ensure the integrity of the ACC electronic information system, provide timely advice of electronic attack and coordinate incident response.

The ACC is also assisting in the funding of the AUSCERT/Attorney General’s Department Incident Reporting Scheme.

Data Interception



Points of internet data interception

The capability of the Internet to transfer text, images and data around the globe instantaneously is attractive to criminals and also impacts upon interception capabilities.

Interception of Internet communications is possible and is currently undertaken by the ACC’s Telecommunications Interception Section. However, these communications can be concealed through encryption and other techniques designed to keep them secret.

The ACC has encountered a limited number of cases where it is aware that criminals have utilised encryption to evade interception. It is likely that cryptography will be utilised increasingly by criminals, especially as it becomes a standard component of software.

The expanding use of the Internet and the exponential increase in Internet frauds, supports a case for extending the range of offences for which Telecommunications Interception warrants may be obtained. This recognizes the fact that the Internet is not simply used to assist the perpetration of offences, but is the very means by which the offences are committed.

An ACC investigation involving the use of emails illustrates the difficulties of countering the international dimensions of contemporary organised crime.

CASE STUDY: Internet E-mails and Cyber cafes

An established criminal network was involved in well planned and methodically executed importation of ecstasy into Australia and its distribution throughout Sydney on the wholesale and retail markets.

The network was totally conversant with modern forms of communication. The members of the network communicated via the American-based 'hotmail' email system and the SMS text message facility on their mobile telephones. A member of the group used Internet Cafes to send emails. Upon identifying this method of communication, attempts were made to establish subscriber details for those addresses.

This request proved fruitless, as the offences did not relate to the United States (either to or from), where the email service provider was based. One member of the group was an employee of a telecommunications service provider and he would facilitate the provision of new mobile telephones and/or SIM cards for group members. He also used work email to arrange the supply and distribution of narcotics to other staff members.

Future Direction

The fast paced area of data interception is one in which all agencies must maintain technological pace with industry. This is for both offensive and defensive purposes:

1. New telecommunications services require an interception capability for law enforcement. For example, Internet Protocol (IP) traffic is being utilised in new generations of mobile phone technology, new mobile phone features like MMS, GPRS web surfing, and 3G...etc are based on IP. This kind of communication (camera mobile-->email-->internet) is getting popular and easy to use, and handsets are getting relatively cheap as well.
2. Any agency such as the ACC, which puts great emphasis on its specialised electronic tools such as telecommunications and data intercepts, could be vulnerable to attack.

4. Legal and Policy

Cybercrime Policy and National Consistency.

Debates concerning the regulation of computer networks particularly the Internet tend towards the extreme because communications on these networks eliminate physical limits to the activities of individuals and law enforcement.

Mechanisms for policing the Internet such as for obtaining encrypted material and tracing communications can appear to overreach acceptable law enforcement because of a lack of understanding of the threat and because they raise the spectre of the ‘surveillance society’.

The challenge is to keep the legislators of cyber-crime ahead of the fast moving technological curve. There is also a need to criminalise damage caused by authorised persons and company insiders who are reckless or negligent and steal confidential information. Even in instances where the act can be regarded as a prank with no intention to cause harm unauthorised access should still be prosecuted and penalised.

There is also a lack of uniformity in Commonwealth and State laws as they apply to Internet Content Hosts (ICH) and Internet Service Providers (ISP). Commonwealth law applies to ICH but not to content providers, creators or ordinary internet users. The law requires Australian ISP and ICH to delete content from their servers that is deemed objectionable on receipt of a takedown notice from the government regulator, the ABA.

State legislation applies to content providers and ordinary Internet users enabling prosecution of ordinary internet users, and other content providers for making available material that is deemed objectionable and for downloading content that is illegal to possess.

ACC Examinations and Cybercrime

The creation of the NCA and its evolution into the ACC is a testament to the ongoing importance and value of a national law enforcement agency with the power to compel production of documents and examine witnesses.

When the ACC is conducting a special operation/investigation into federally relevant activity which has been determined by the ACC Board it has a number of special powers available to it that are not available to traditional police services. These special powers are conferred on the ACC by the *Australian Crime Commission Act 2002.*

To further intelligence operations and investigations the ACC is empowered to conduct examinations of individuals (s.28). Attendance at the examination is compulsory and it is an offence to refuse to answer questions. The individual is entitled to legal representation during an examination but is precluded by nondisclosure provisions in the statute from disclosing the attendance at the examination to a third party.

The extraordinary powers available to the ACC provide law enforcement and investigative agencies across Australia with a complementary and invaluable resource to facilitate investigations and develop intelligence. The coercive powers can be exercised in support of all Australian law enforcement agencies under the terms of reference provided by the ACC Board and the Intergovernmental Committee (IGC), and by persons with quasi-judicial authority – the Examiners.

The use and potential of the ACC's coercive powers and the benefits that can be derived from their use can be considered in the context of law enforcement's investigation of Cybercrime.

Anonymity is a key advantage of the internet in the commission of offences and the ability of offenders to remain anonymous presents a huge challenge for investigators as most web surfers have a handle, a false name or identity.

The ACC coercive powers could be exercised to summons a person who it is believed has a critical piece of information such as an encryption key or a password that will facilitate the course of the investigation and potentially prevent the commission of further offences.

The summonsed witness can be directed to answer questions or suffer a substantial penalty ranging from a fine up to $20,000 or imprisonment for a period not exceeding 5 years.

Electronic Warrants in the Cyber-Age

The *Cybercrime Act* 2002 contains amendments to the investigation powers contained in the *Crimes Act* (*Cwth.)* and *Customs Act* relating to the search and seizure of electronically stored data. This legislation brings the investigative powers of law enforcement in Australia into line with many aspects of the Council of Europe Convention to Cybercrime and reflects the need to bring existing provisions up to date with technological developments and the rapid uptake of computer technology by organised crime.

The amendments are intended to provide law enforcement with the necessary powers to detect and investigate crime involving the use of computers through enhancing traditional search and seizure powers so as to extend to stored data especially across computer networks.

As most business computers are networked across a number of locations it is critical that law enforcement agencies in executing a search warrant are able to search not only material on computers contained within the search premises but also material accessible from those computers but located elsewhere if there are reasonable grounds to believe that the remotely held data may contain evidential material.

However the investigative utility of the amended search warrant provisions of the *Cybercrime Act* are limited to the period of the warrant – generally 7 days or 48 hours for telephone warrants. Additionally the material seized under an executed warrant cannot be retained indefinitely – usually 60 days- unless charges have been laid.

The search warrant is an essential Law Enforcement tool, which is legislatively protected from abuse. Similarly, a number of other investigative tools have developed from this concept on the back of technology. These include listening Devices, Telephone Intercepts, video surveillance and tracking. Though intrusive, these tools controlled through rigorous legislative restrictions.

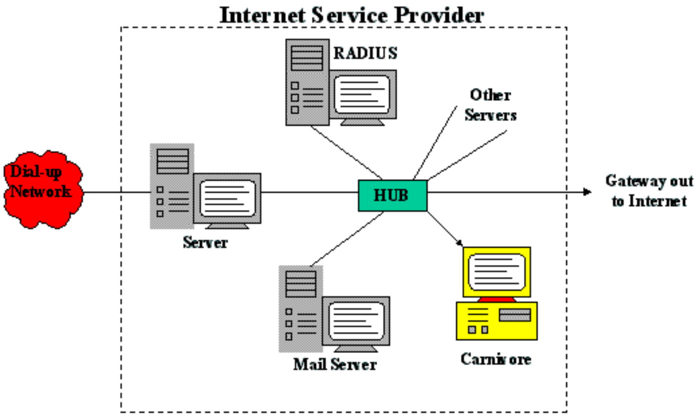
Cyber Search Warrants

A tool of emerging technology with implications for Law Enforcement, which has not been fully developed, is that of on-line investigations. This includes the ability to legally electronically access an offender's computer remotely, for the purpose of gathering evidence. Ironically, computer hackers have been doing just that illegally, for the last 20 years.

Monitoring warrants that allow real time surveillance of computer based activity - under s25A of the *ASIO Act* 1979 as distinct to conventional search warrants operate so as to allow ongoing searches of computer data for a period up to 6 months subject to the issuing Minister being satisfied that there are reasonable grounds for believing that access to the data in the target computer will substantially assist the collection of intelligence in respect of a matter that is important to national security.

Such a monitoring warrant enables law enforcement to use investigative tools such as DCS-1000 - an electronic surveillance device used by the FBI with a surgical ability to intercept and collect the communications of the subject of the warrant while ignoring those communications which the authorisation to intercept does not cover. The FBI's technology operates as a network diagnostic tool similar to those used by ISP's except that it provides the FBI with the unique capacity to distinguish between communications that can be intercepted lawfully and those which may not.

For example, if a court issues a warrant that provides for the interception of email but excludes other communications such as online shopping the FBI technology can be configured to intercept only those emails transmitted from one named subject to another.



DCS-1000 internet interception tool

Analogous to telephone intercept warrants in all material respects computer monitoring warrants, issued subject to the same administrative and judicial requirements and safeguards as telephone intercept warrants – would significantly enhance the investigative toolkit available to law enforcement.

In its report entitled “The Law Enforcement Implications of New Technology” August 2001 at pg 15ff the PJC addressed the need for improved regulation of Internet Service Providers to provide law enforcement with interception capability and evidentiary assistance in terms of proper record retention; subscriber checks and the maintenance of traffic data. There has been some progression in this area since the PJC discussion of the issue by the commendable efforts of LEAC (Law Enforcement Advisory Committee) and the development of an industry and law enforcement *Cybercrime Code of Practice.*

Similar cooperative arrangements between telecommunications carriers, ISP’s and law enforcement have proven previously to be ad hoc and arbitrary. Such self regulating and voluntary regimes are likely to be adopted inconsistently across the industry as is the experience with similar codes relating to telecommunications carriers. Regrettably this inconsistency creates an opportunity for organised crime to exploit to their advantage by utilising the services of a carrier or ISP who elects, usually for cost based reasons, to not comply with the record management protocols provided for in the industry codes of practice.

Improved regulation of ISPs must commence with regulatory requirements regarding the mandatory preservation of records and the availability of preservation orders to be applied for by law enforcement to ensure that data and records are not destroyed by an ISP or indeed a subscriber. Such provisions are consistent with legislation in the United Kingdom and the provisions of Chapter 2 (Articles 14-21) of the *Council of Europe Cybercrime Convention* including the expedited preservation of stored data, traffic data and content data; production orders; real time collection of traffic data and interception of content data. Non member states who have signed the Convention include the United States and Canada.

.

Future Direction

1. The ACC will continue to study the policy and legal implications of Cybercrime, and to offer advice on potential reform.

2. In particular, consideration should be given to law reform in the area of law enforcement ‘electronic search warrant’ powers.

3. The availability of the ACC’s coercive powers, subject to authorisation by the Board, could be an important component in the ACC’s contribution to Cybercrime work.

CONCLUSION: THE WAY AHEAD

The ACC role in the national response to Cybercrime is shaped by the following factors:

- ⇒ National intelligence collection, analysis and dissemination, is a cornerstone of the ACC role. (Operational, Strategic and E-Crime Desk)
- ⇒ Cybercrime is now an inextricable dimension in many forms of serious and organised crime, and hence is part of the ACC's intelligence focus
- ⇒ The multi jurisdictional nature of Electronic Crime is suited to the ACC model (national agency in partnership with State and Commonwealth agencies and private enterprise)
- ⇒ The special powers of the ACC could be invaluable in supporting an effective response to Electronic Crime threats of national significance

Partnerships between the ACC, the AHTCC, the jurisdictions and E Crime Taskforces will be essential in collecting, analysing and distributing Cybercrime intelligence. Also, the AHTCC is intended as a coordinating centre for complex Hi Tech Crime Investigations for the jurisdictions, and will be a focal point for intelligence gathering in this area, and thus an important partner to the ACC.

This coordinated approach can be further complemented through national Cybercrime reporting on the ACID system, and incorporation of Cybercrime and related issues in the ACC's national criminal intelligence products and services.

All agencies, including the ACC, must also continue to retain a technical capacity to deal with Cybercrime, as per the National E Crime Strategy. The ACC National Cybercrime Unit currently provides the ACC with this technical capacity, along with training, intelligence support and Cybercrime specialised advice.

An effective law enforcement response to Cybercrime depends on the ability of agencies to have a technical capacity, flexibility, innovation and a partnership driven approach.