Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:21
Received 2 June 2003

Action Officer Mr Anton Schneider
Strategic Law Enforcement Branch
Attorney-General's Department
Robert Garran Offices
Nation Circuit
BARTON ACT 2600
☎02 6250 6778 🗎
E-mail: anton.schneider@ag.gov.au

The Attorney-General’s Department Submission

Parliamentary Joint Committee on the Australian Crime Commission Inquiry into Cybercrime

Introduction

This submission on Cybercrime was prepared by the Attorney-General's Department. It provides an overview of the roles, concerns and initiatives of the Commonwealth in the area of Cybercrime. It is not intended to be an exhaustive treatment of the issue.

Cybercrime is a term that encompasses a variety of offences associated with the use of information and communication technology. The use of the term Cybercrime is synonymous with the term electronic crime (e-crime) and is used as such throughout the submission.

Background

Significance of Cybercrime

Cybercrime is a significant challenge facing law enforcement today. The Australian Institute of Criminology estimates that crime costs Australia $19 billion per year. Fraud and financial crime alone account for $5.88 billion of this figure. In addition to the direct costs of crime, the indirect costs amount to another $13 billion per year. This gives Australia a national crime bill of around $32 billion per year. This is the equivalent of $1,600 for each and every Australian and represents 5 per cent of GDP. While the cost of Cybercrime is believed to be only a small part of this total cost, its potential to adversely affect Australia requires all Australian governments and the private sector to work together to put into place effective prevention, detection, investigation and prosecution procedures.

At its broadest, Cybercrime can include:

- criminal targeting of computers
- crimes conducted across the internet, and
- the facilitation of crimes in the physical world.

An effective response to each of these problem areas requires a coordinated response. The Commonwealth has encouraged a national approach to Cybercrime. The Australian Crime Commission (ACC) and the Australian Hi-Tech Crime Centre (AHTCC), hosted by the Australian Federal Police (AFP), provide a significant national response to the law enforcement aspects of Cybercrime. In addition, the Commonwealth has promoted partnerships between government and the private sector in the areas of prevention, risk awareness and intelligence collection. The Commonwealth is responsible for ensuring that an appropriate legislative structure is in place that deters crime and facilitates business activity. The Commonwealth can not be responsible for the security of every computer network in Australia; State, local government and the private sector have complementary responsibilities to put into place procedures that minimise the likelihood of Cybercrime.

Criminal targeting of computers includes both attacks against the national critical infrastructure and industrial espionage against private sector systems and data. Crime conducted across the internet provides a new environment for traditional crimes, such as on-line fraud, as well as new variations of traditional crimes such as child pornography and associated paedophile activity. Cybercrime can also facilitate crime in the physical world – this includes crime associated with illegal technologies and software such as credit and debit card skimming – and covert criminal and terrorist communications and financing.

The incentives for criminals to embrace e-crime are substantial:

- virtual anonymity
- rapidly disappearing evidence trails
- by nature, Cybercrime tends to be multi-jurisdictional, frequently international and difficult to police
- lack of understanding of computer crime by the community
- reluctance of business to report incidents to law enforcement, and
- potential to accrue large proceeds of crime with relatively minimal risk.

All of these elements are compounded by the rapid speed of technological change - today individuals can use mobile phones, computers, broadband, wireless, and wireless LANs to connect to the internet and engage in electronic commerce (e-commerce). The rate of technological change in the fields of information and communications technology (ICT) has been phenomenal throughout the 1990s. The degree to which new technologies and innovations are introduced in the future and the ability of law enforcement to access new tools and capabilities will impinge on our ability to counter Cybercrime.

Deterrent to Electronic Commerce

Consumers, businesses and governments around the world are embracing the internet as a medium for conducting commerce and delivering services. As more people have been exposed to computers through education and work, initial public wariness of the technology has dissipated. The uncertainty generated by Cybercrime remains, however, a major deterrent to the uptake of e-commerce. The ability of both government and industry to manage both the perception and the reality of Cybercrime will dictate the successful expansion of e-commerce in the future.

Threat to National Information Infrastructure

Cybercrime is a significant issue in relation to the national information infrastructure (NII). The NII includes the information systems that underpin the operation of key infrastructure, including electricity and gas supplies, water supply systems, air-traffic control systems, banking and finance systems, telecommunications, transport systems and others. The failure of any of these systems would seriously impact on the Australian economy and potentially threaten the safety and security of Australians. All of these systems are increasingly - if not exclusively - controlled by computers. Consequently, the Commonwealth is putting in place arrangements to ensure that the computer systems underpinning national critical infrastructure remain secure, particularly from terrorists and politically motivated organisations that may target national critical infrastructure in the future.

Potential for organised crime to exploit new technologies

Cybercrime is significant because of its potential to be exploited by a range of offenders including serious organised crime. As the technology market and its users continue to mature, and the billions of dollars being spent on securing open network systems begins to take affect, the threat Cybercrime poses to electronic commerce will continue to diminish. However, there is increasing scope for organised criminals to exploit new technology to engage in a range of crimes including money laundering, other financial crimes, drug trafficking, and to use encrypted communications to evade police investigations. The ability of law enforcement to continue to successfully fight organised crime relies to some extent on how well it responds to the uptake of new technologies by criminal networks.

Trends in E-Crime

One of the difficulties in identifying the scope and size of Cybercrime was the reluctance by some private sector institutions to report computer related crime, particularly where it related to financial fraud. The lack of adequate statistics on Cybercrime, complicated by definitional issues, has in the past made it difficult to conduct realistic Cybercrime threat assessments.

Government agencies and financial institutions are overcoming these problems as part of new partnership arrangements. It is envisaged that the operations of the AHTCC and the ACCA will result in improved information and intelligence flows between private sector organisations and law enforcement agencies. Both Government and the financial institutions have committed themselves to improved cooperation and information exchange.

Some relevant statistics in the Australian Computer Emergency Response Team (AusCERT) *2003 Australian Computer Crime and Security Survey* were released recently. The survey is based on anonymous responses from a survey group consisting of Commonwealth, State and Local government, large and small business, the education sector, and IT security professionals. The collection period was January and February 2003 for the 2002 Calendar year.

The key findings of the survey are:

- 42 per cent of respondent organisations experienced one or more computer attacks which harmed the confidentiality, integrity or availability of network data or systems.
- Despite overall lower levels of incidents being reported, only 11 per cent of respondents felt they were managing all computer security issues reasonably well. 67 per cent of organisations increased expenditure on network security in the last 12 months as a result of computer security incidents or concerns.
- The trend shows a continuing shift towards a greater occurrence of externally-sourced harmful attacks and fewer internally-sourced harmful attacks. Of those who experienced attacks which harmed data confidentiality, integrity or availability, 91 per cent experienced externally sourced attacks and 36 per cent experienced internally-sourced attacks.

- Total losses for 2003 are more than double the quantified losses for 2002 (about $12 million, compared to about $6 million in 2002).
- Financial fraud, laptop theft and virus, worm and trojan infections are the largest source of computer crime losses.
- Despite high use of anti-virus software and policies for developing controls against malicious software, 80 per cent were infected with a virus, worm or trojan and 57 per cent suffered financial loss as a result – an increase on last year.
- Only a minority of respondent organisations hold specialist IT security certifications; with industry vendor IT security certifications at 36 per cent and vendor-neutral IT security certifications at 15 per cent.
- 38 per cent were dissatisfied with the level of IT security qualifications, training or experience within their organisations.

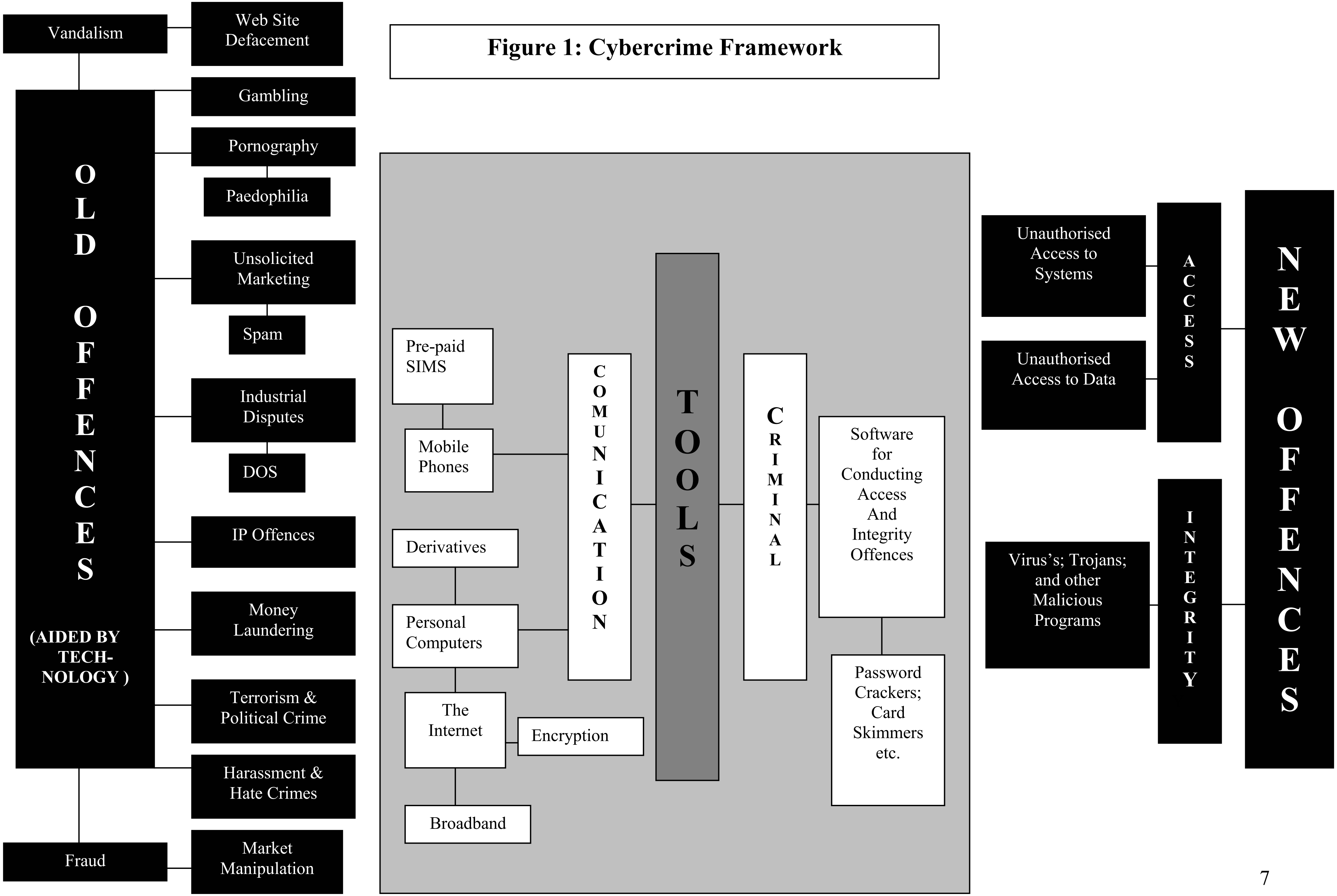
The survey highlights the importance, when developing responses to Cybercrime, of differentiating between offences that involve theft of computer or communication technology and the use of such technology to commit crime. Only the latter should really be classed as Cybercrime.

Conceptualising Cybercrime

It may be useful to provide a visual representation of the linkages between the methodology used to commit offences and the types of offences usually classified as Cybercrime. The following framework is loosely based on a model for examining identity fraud risks developed in the AGD publication *Who Goes There*?

The framework highlights that the majority of Cybercrime offences are traditional offences being committed using or being aided by modern technology. Forms of Cybercrime which can be considered “new” crimes are limited in numbers. They are divided into access offences - unauthorised access to systems or data - and integrity offences - crimes which corrupt the integrity of systems or data. In between the two types of offences is a range of tools, some of which are standard communication tools, others are what may be termed illegal technology.

Figure 1: Cybercrime Framework



International Response to Cybercrime

International Treaties

Cybercrime continues to be a focus of international attention.

United Nations Congresses on the Prevention of Crime and the Treatment of Offenders

Both the Eighth and the Tenth UN Crime Congresses have devoted considerable time to the question of how to prevent and control high technology and computer-related crime.

The 8th Congress (Havana, 27 August - 7 September 1990) produced the *United Nations Manual on the Prevention and Control of Computer-Related Crime*. The manual provided a broad overview of the newest forms of computer related crime and canvassed various solutions and reform initiatives. In particular Congress discussed:

- the nature and extent of computer and computer related crime
- the development of national law to deal with computer crime, and the international harmonisation of criminal law in this area
- crime prevention in the computer environment, and
- international cooperation.

The 10th Congress (Vienna, 10 - 17 April 2000) specifically discussed crimes related to computer networks.

UN Convention on Transnational Crime

The UN Convention on Transnational Organised Crime adopted by the General Assembly on November 15, 2000 does not directly apply to routine computer crime. The Convention aims to improve international cooperation against organised and transnational crime, such as money laundering, by simplifying the processes for investigators to obtain evidence, conduct searches and question suspects from foreign jurisdictions. It also contains a general basis for conducting joint investigations and measures for cooperating in special investigative procedures, such as electronic surveillance.

Lyon Group (G8)

The Lyon Group is a sub-group of the G-8, and is made up of a collection of senior experts who were given the task of reviewing and assessing existing international agreements and mechanisms to fight transnational organised crime. The Lyon Group met in Paris in April 1996 and produced a series of 40 recommendations on how to better combat organised crime. As a result of these recommendations a network of law enforcement contact officers was established enabling round-the-clock points of contact for urgent computer related crime queries. Interpol now has the operational responsibility for this network and the Australian Federal Police is Australia's point of contact with the network.

Council of Europe Cybercrime Convention

The Council of Europe Cybercrime Convention was opened for signature on 23 November 2001, and will come into force after ratification by five States, including at least three member States of the Council of Europe. To date 33 nations have signed the convention, although it has only been ratified by Albania, Croatia and Estonia.

The Convention is the first international treaty on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures for the search of computer networks and interception.

The main aim of the convention is to pursue a common criminal policy aimed at the protection of society against Cybercrime by adopting appropriate legislation and fostering an effective regime of international cooperation.

Commonwealth Response to Cybercrime

Cybercrime amendments to the Criminal Code

In December 2001 the cybercrime provisions in the Criminal Code commenced. This legislation created new computer offences and law enforcement powers that help protect Australia's national information infrastructure from cyber-terrorist attacks. Such attacks can seriously interfere with the functioning of the government, the financial sector and industry.

The offences target those who hack into protected information stored on computers, circulate destructive computer viruses or launch "denial of service" attacks to shut down websites. An offence was also created for the unauthorised use of a computer with intent to commit a serious offence, such as stalking, fraud or sabotage. These offences are based on those in the Model Criminal Code and were developed in close cooperation with the States and Territories.

Under the cybercrime provisions, electronic investigation powers were also enhanced to provide law enforcement agencies with greater capability to investigate crime involving the use of computers. The large amount of data that can be stored on computer drives and disks and the complex security measures, such as encryption and passwords, which can be used to protect that information, were particular problems targeted by the legislation. Powers to copy computer data and examine computer equipment and disks off-site were enhanced, as were powers to compel a person with knowledge of a computer system to provide the key to encrypted data.

Child pornography on the Internet

The Federal Government intends to introduce new offences to target people who use the Internet to transmit or download child pornography. The maximum penalty for the offences will be 10 years imprisonment.

The offences will complement State and Territory offences relating to the production and possession of child pornography, and offences in the *Customs Act 1901* for the importation and exportation of child pornography.

Commonwealth, State and Territory Police Ministers have agreed to develop a nationally consistent approach to the registration of child sex offenders. A Working Party, convened by New South Wales, is currently considering the matter.

The *Telecommunications (Interception) Legislation Amendment Act 2002* was amended in 2002 to include child pornography related offences as offences in relation to which a telecommunications interception warrant be sought. Section 5D of the *Telecommunications (Interception) Act 1979* was amended to include in the definition of Class Two Offences : "the production, publication, possession, supply or sale of, or other dealing in, child pornography; and consenting to or procuring the employment of a child, or employing a child, in connection with child pornography".

CrimTrac and the National Child Sex Offender System Project

CrimTrac was established in July 2000, to enhance Australian law enforcement with an emphasis on information-based policing facilitated through rapid access to detailed, current and accurate police information. A National Child Sex Offender System and the provision of rapid access to national operational policing data are two of the key deliverables funded from the $50 million capital injection. Addressing other emerging policing requirements across jurisdictions is also within the ambit of the CrimTrac charter.

The National Child Sex Offender System (NCSOS)

The purpose in developing the NCSOS is to improve the sharing of the information and intelligence of Australian law enforcement agencies about known and suspected child sex offenders, to enable greater protection for children. Stage 1 of the project is embedded within the parent project, the CPRS Minimum Nation-wide Person Profile (MNPP) project, currently being progressed with NSW and Vic police jurisdictions.

Although the project has not yet been fully scoped, Stage 1 of the project will provide police with improved factual information on child sex offenders, based on an agreed set of relevant offences. Confirmation of business and system requirements with jurisdictions is under way. Design and development activities will occur in conjunction with the MNPP Project, to enable the first phase of a nationwide view of convicted offenders to be available to police in early 2004. The system will only be for police use.

The Australasian Police Ministers Council (APMC) is currently considering how best to develop a nationally consistent approach to registration of child sex offenders. At present NSW alone has a Child Protection Register but other jurisdictions are examining their establishment. In addition to the NCSOS, CrimTrac may provide two distinct forms of assistance in the development of a nationally consistent approach to registration of child sex offenders:

- assistance in establishing the Child Protection Register (CPR) Application, and
- cross-jurisdictional sharing of information.

Assistance in establishing a Child Protection Register (CPR) Application

CrimTrac has prepared a capability development proposal for information system support to nationwide Child Protection Offender Registration, which will be considered as part of the report to APMC.

Following agreement on the general approach that jurisdictions want to pursue, CrimTrac would prepare the business case, including information delivery models, funding options and benefits. Benefits are expected to include reduced cost to jurisdictions in having only one application rather than each jurisdiction developing/customizing their own. It is not envisaged that funding for this initiative would come from existing CrimTrac project funds.

Cross-jurisdictional sharing of information

Facilitating information exchange between registers could be part of the NCSOS through:

- assistance in reporting and monitoring - CrimTrac could provide the mechanism to notify a jurisdictional register when a registered offender from another jurisdiction plans to move/travel to that state/territory, and
- case management - CrimTrac could assist police with their case management of individual offenders by providing the cross-jurisdictional informational support tool that might be required.

Cybercrime with particular reference to credit card fraud

On 20 December 2002, the Minister for Justice and Customs, Senator Ellison met with representatives of peak financial institutions to further develop a partnership between government and industry to counter financial fraud in particular credit and debit card skimming.

Skimming is the recording and storage of credit or debit card identification information, including Personal Identification Numbers (PIN numbers), by means of a technological device. The information is downloaded and stored on another form of media (eg a plastic card or parking ticket) with a magnetic strip to be used to illegally access credit or money.

A number of initiatives flowed from the meeting between Senator Ellison and peak financial institutions:

- Senator Ellison raised the need for uniform offences with the Standing Committee of Attorneys-General. SCAG has referred the issue of credit and debit card skimming offences to the Model Criminal Code Officers' Committee (MCCOC). MCCOC will consider existing legislation in this area and develop model offences.
- The Australasian Police Ministers' Council is to look into a national approach to card skimming.
- The Australian Crime Commission is to undertake an intelligence operation into card skimming. This complements the ACC's interests in ID fraud.
- A Commonwealth – New South Wales Task Force has been established to combat ID Fraud.
- The Australian Hi-Tech Crime Centre will work with the financial industry to progress serious or complex multi-jurisdictional investigations and to look into the complex issues associated with Hi-Tech crime.
- The Australian Bankers Association has established a Task Force into Fraud including representatives from Federal and state police forces. The Task Force has announced a series of initiatives including:
  - the development of voluntary Industry Standards on Security and Fraud Prevention
  - an Analytical Study of Identity Documents, and
  - the development of a Fraud Education Program for banking customers.

A second Ministerial forum was held on 14 May 2003, at which it was agreed to hold Biannual Ministerial Meetings with financial institutions to discuss fraud, in particular banking fraud. The meeting also supported a national approach to improve collection, analysis and dissemination of intelligence on skimming and associated frauds, and that further links between industry and law enforcement would be developed. The Ministerial meetings are a demonstration of the commitment by industry and government to work together to combat financial fraud.

Fraud offences in the Criminal Code

In 2000 the Commonwealth enacted a modern and transparent scheme for preventing and punishing instances of theft, fraud, bribery, forgery and related offences, against the Commonwealth Government and its officials. The Code contains fraud and forgery offences which specifically cover fraudulent conduct involving computers including where the agent involved in the transaction is a computer or machine rather than a human being.

Proof of Identity

There is no formal definition of the term "identity fraud", however it is commonly accepted that identity fraud occurs when an individual falsely represents him, or herself, as either another person or a fictitious person to an organisation for some benefit. This misrepresentation may be supported by fraudulently obtaining or falsely reproducing identity documents.

Identity fraud is a major component of many Cybercrimes, and identity verification is a fundamental component of all e-commerce. False identities can also be used by persons involved in serious offences to avoid detection. Law enforcement agencies involved in investigating card skimming indicate that it is increasingly being perpetrated by organised crime groups in conjunction with other criminal activities.

Typical scams often involve registering, or enrolling, false identities with organisations to defraud them of goods or services. This may be achieved by either manipulating fictitious identities to give them some apparent legitimacy or by stealing the identity of other people to facilitate the fraud ("identity theft"). Examples include tax and welfare fraud, acquiring bank loans in false names and using stolen credit card details to defraud retailers

Card skimming, loan fraud and related ID fraud offences are becoming more prevalent in Australia and account for significant business losses. There are no firm figures available on the extent or cost of identity fraud in Australia. However it is seems to be accepted by both public and private organisation around the world that the problem is growing. Informal advice from the banking industry indicates that losses associated with card skimming have increased 400 per cent in the last 12 months, primarily from credit card skimming.

Work to address identity fraud and theft is being undertaken by many Commonwealth agencies. The Commonwealth Government is coordinating this work to tackle the issue from a more cohesive, whole-of-government perspective.

The Attorney-General's Department is taking a lead role in developing a strategic direction for improved personal identification and authentication practices. Some examples of initiatives which the Commonwealth is undertaking that are in the public domain are:

- Work is being undertaken on assessing the costs of identity fraud to the community by the AUSTRAC Proof of Identity Steering Committee. The committee includes representatives from Commonwealth and State government agencies, as well as representatives from the banking industry, and has commissioned a study by the Securities Industry Research Centre of Asia-Pacific Ltd (SIRCA).
- The introduction by Customs of world first photo-matching Technology at Sydney International Airport has reinforced Australia's position as a leader in border security.
- The Department of Foreign Affairs and Trade is considering improvements to the Australian passport which might include adding a biometric identifier in the next passport series.
- The Australian Crime Commission (as the former Australian Bureau of Criminal Intelligence) has established a trial Identity Fraud Register that will improve law enforcement's intelligence holdings relating to identity fraud. The register records known offenders, fraudulent names used and lost or stolen documents.

Money Laundering

Whilst money laundering and its link with organised crime have been of long standing concern, the threat of terrorism has given money laundering a new global focus. At an international level peak organisations have turned their attention to the link between terrorist financing and money laundering, examining ways to prevent terrorist attacks and apply sanctions against those who support terrorist activity.

International Measures

Because criminals who launder money seek to exploit international financial markets and often launder the proceeds of crime through financial structures that lay outside the jurisdiction in which they operate, an international approach is necessary to make an impact. The Attorney-General's Department is actively involved in representing Australia's interests in this context.

The Financial Action Task Force on Money Laundering (the FATF), an international organisation of which Australia is a founding member, has played a key role in the development of international money laundering standards since the early 1990's. Compliance with the FATF Forty Recommendations, which form the basis of international money laundering standards, is enforced under a system of country by country peer assessments, with steps to impose sanctions against countries that do not comply.

The issue of world wide cooperation has been of key concern to the FATF. In 2000 this led to the establishment of the non-cooperative countries and territories (NCCT) initiative to reduce the vulnerability of the international financial system to money laundering by ensuring that all countries have adequate safeguards in place.

In this context the FATF has focussed on the technical and practical assistance to both member and non member countries. It convenes an annual typologies exercise in which law enforcement and regulatory experts examine recent trends in the techniques criminals use to launder money. The forum produces an annual report which is available at http://www.fatf-gafi.org/FATDocs_en.htm#Trends

In response to the tragic events of 11 September 2001 the FATF released 8 Special Recommendations on Terrorist Financing, calling upon nations to update their domestic legislative arrangements to ensure that the financing of terrorism did not go undetected. This framework accompanied United Nations measures, calling upon nations to ratify the 1999 United Nations International Convention on the Suppression of Financing of Terrorism and comply with Security Council Resolution 1373 in relation to the suppression of terrorist financing.

The FATF 40 Recommendations are currently under review due to international acknowledgment of the increased opportunities that exist to launder money through modern financial systems. Australia is actively participating in this process with officers of the Attorney-Generals Department and the Treasury representing Australia at the relevant FATF working group meetings.

Regional Measures

At a regional level the Asia Pacific Group on Money Laundering (APG) was established in 1997 as a FATF style regional body to provide a focal point for anti-money laundering cooperation in the Asia Pacific region. The APG has 26 member states, including Australia, and has placed great emphasis on providing technical support and assistance to countries in our region to encourage compliance with the FATF 40 Recommendations. In particular, the APG plays a coordinating role in the provision of technical legal and law enforcement experts to evaluate and advise countries in the region. In this context the Attorney-General's Department has provided significant direct support to Indonesia, which was placed on the NCCT list in June 2001.

Australia has taken a lead role in the establishment and support of the APG, providing funding assistance to the Secretariat which is located in Sydney and holding the position of permanent Co-Chair. The APG's fifth Annual General Meeting was hosted by Australia in Brisbane on 4-7 June 2002.

Domestic Measures

Two pieces of domestic legislation provide the key mechanism through which federal law enforcement officers combat money laundering in Australia.

The *Financial Transactions Reports Act 1988* (FTR Act) facilitates the collection and analysis of financial intelligence which may then be used to investigate money laundering, and other serious crimes, such as drug trafficking, which may be traced through financial transactions. The FTR Act contains mandatory provisions for financial institutions to report cash transactions above $10,000, suspicious transactions and international funds transfers, as well as requiring financial institutions to verify the identity of signatories to accounts and prohibiting the opening or operation of accounts in false names.

The FTR Act also establishes the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australia's Financial Intelligence Unit. AUSTRAC is tasked with the collection, analysis and dissemination of financial intelligence. It also works to ensure that financial service providers and the gambling sector comply with the mandatory reporting and customer identification provisions of the FTR Act.

The *Proceeds of Crime Act 2002* enables courts to freeze and confiscate assets where the Director of Public Prosecutions (DPP) can prove on 'the balance of probabilities' that a person has engaged in serious criminal activity in the previous six years, or that the property is the proceeds of a particular offence, punishable by at least 12 months imprisonment.

Both pieces of legislation were recently updated to keep in line with international trends and to ensure that Australian law enforcement officers are adequately equipped to deal with recent trends, including terrorist financing.

Mutual Assistance

Cybercrime has the ability to cross international borders and often requires a coordinated international response in the investigation and prosecution of offenders.

The Mutual Assistance Unit in the Attorney-General's Department is responsible for making requests for assistance in criminal matters to foreign jurisdictions on behalf of the Australian law enforcement authorities including the Australian Crime Commission. The Unit coordinates the provision of assistance from other countries for the investigation and prosecution of crime and the restraint and confiscation of assets of crime.

Australia is party to a number of bilateral Mutual Assistance in Criminal Matters treaties. Australia's domestic legislation, the *Mutual Assistance in Criminal Matters Act 1987* (MA Act) enables it to provide assistance to countries with which it does not have a formal treaty-based mutual assistance (MA) relationship. Assistance is provided on the promise of reciprocity in similar cases from the requesting state.

There are a number of restrictions in Australia's domestic legislation that prevent assistance being provided to other countries in certain circumstances, including death penalty cases and where telecommunications intercept (TI) and listening device (LD) material is requested. In particular, under the *Telecommunications (Interception) Act 1979* (TI Act), Australia cannot gather TI or LD material on behalf of another country. Australia can only provide telecommunications interception (TI) material to assist a foreign country where the material has already been obtained for an investigation of an Australian offence.

National Information Infrastructure

The key agencies with policy responsibility for implementing the government's E-Security National Agenda and ensuring steps are being undertaken to protect Australia's National Information Infrastructure (NII) are the Attorney-General's Department and the National Office for the Information Economy. The lead operational agencies in this area are the Australian Federal Police, in particular the Australian Hi Tech Crime Centre, the Australian Security Intelligence Organisation and the Defence Signals Directorate.

The implementation of particular initiatives in pursuing policy objectives has resulted in the involvement of a number of additional organisations including the Australian Securities and Investment Commission, the Australian Prudential Regulation Authority and the Australian Crime Commission. For example, the Australian Crime Commission has provided support to the establishment of the AusCERT National Information Technology Security Alert and Advice Scheme. This scheme, which is illustrative of the private and public sector partnership in the government's approach to protecting the NII, will provide, free of charge to the Australian community, alerts regarding potential threats and vulnerabilities in Australia's information environment and a mechanism whereby security incidents can be reported.

The purpose of the scheme is two-fold. Firstly, it is intended to raise the general level of awareness amongst business and consumers of the potential dangers posed by information security vulnerabilities. Secondly, it will provide trend information and data on information security incidents.

A number of Commonwealth agencies have combined resources to fund the scheme. The Australian Crime Commission is a financial contributor to the scheme and will be a recipient of the information generated from the scheme's operation.

The Australian Crime Commission is also a member of the Information Infrastructure Protection Group (IIPG). The IIPG is a strategic policy working group formed to identify and provide advice on the protection of Australia's NII with respect to incidents of a critical nature. It was formed as a result of a recommendation made by the Secretaries Committee on National Security (SCNS) in November 2000.

Another relationship between the ACC and the protection of the NII has come about through the work of the Office of Strategic Crime Assessments. In December of 2002 OSCA, which has since become a part of the new ACC, produced an assessment on the long-term criminal risks to the NII. This was prepared in response to requests from the Attorney-General's Department. This document provides a useful projection of likely future trends and is valuable background material for the development of future policy to protect the NII.

Privacy

The Attorney-General has portfolio responsibility for the *Privacy Act 1988*. It is worth noting that many initiatives in the area of Cybercrime have privacy implications.

The Privacy Act provides for an independent statutory office of the Federal Privacy Commissioner with responsibility for regulating privacy in both the public and private sectors. The basic framework under-pinning public sector privacy is contained in Section 14 of the Act, which sets out the Information Privacy Principles (IPPs) and that for the private sector is contained in schedule 3 of the Act, which sets out the National Privacy Principles. The IPPs and the NPPs govern the collection, retention, access to, correction, uses and disclosure of personal information. They are technologically neutral and regulate personal information in all media.

In addition to the Privacy Principles, the Act provides the Commissioner with a range of responsibilities, including for issuing guidelines, carrying out compliance audits, carrying out an educative role and considering and determining complaints.

Privacy and Spam

The Commonwealth recognises that electronic junk mail, commonly known as "spam", is a growing problem for many Australians. The Minister for Communications Information Technology and the Arts, Senator the Hon Richard Alston, announced in March 2002, that the National Office for the Information Economy (NOIE) would review the spam problem. NOIE released its report on 16 April 2003.

The report makes a number of recommendations but principally that the Commonwealth should regulate spam. It also urges the Privacy Commissioner to fully apply existing Commonwealth laws to spam and invites the Commonwealth to further consider the application of the *Privacy Act 1988* to this issue. In considering what the next steps should be, the Attorney-General's Department will cooperate with Communications, Information Technology and Arts portfolio, which has principal carriage for the report."

Information Economy

The Department is responsible for electronic commerce issues related to the Commonwealth's information economy policy. The *Electronic Transactions Act 1999* provides the regulatory regime for using electronic communications in transactions and is based on the recommendations of the Government's Electronic Commerce Expert Group, and the United Nations' Model Law on Electronic Commerce. In addition, the Department continues to work on authentication issues fundamental to the process of electronic commerce, such as digital signatures.

Investigation of Cybercrime

There is no single Australian law enforcement or policy body which has responsibility for Cybercrime matters. Stakeholders include law enforcement, regulatory authorities, research organisations, and national fora. The responsibilities of these organisations are diverse, and in most cases Cybercrime forms only a portion of their work. Each of these entities has different roles ranging from the development and coordination of policy, to the policing and prosecution of crime. The ACC and the AFP are the major Commonwealth agencies involved in the collection and analysis of criminal information and intelligence relating to Cybercrime including ID fraud and card skimming. The AHTCC, hosted by the Australian Federal Police, and the Australian Crime Commission both have increasingly significant operational roles to play in countering Cybercrime.

Australian Crime Commission (ACC)

The ACC, as part of its functions, is responsible for the collection, correlation, analysis and dissemination of criminal information and intelligence and for providing advice on national criminal intelligence priorities. The Board of the ACC may determine that an intelligence operation or investigation be conducted with access to the extensive coercive powers available unde the *Australian Crime Commission Act 2002*. In addition, the ACC continues the role of the former Australian Bureau of Criminal Intelligence, facilitating the exchange of criminal intelligence between police jurisdictions.

The NCA (now part of the ACC) established a National Cybercrime Unit on 25 March 2002, with its initial focus on intelligence collection and investigation. The Board of the ACC has recently authorised the ACC to conduct intelligence operations into card skimming and ID fraud. In carrying out its functions, the ACC works in cooperation with other Commonwealth, State and Territory agencies, including the AFP and the AHTCC, providing a national response to complex and organised crime.

The ACC has also been running a pilot Register of Identity Fraud, the outputs of which have been used by the Commonwealth-NSW Task Force on ID Fraud to investigate ID fraud offences. The ACC also runs the National Fraud Desk which provides intelligence on fraud, including Cybercrime offences, to Commonwealth, State and Territory law enforcement agencies. In addition, the ACC is developing improved links with financial institutions for the exchange of information and intelligence.

Australian Hi-Tech Crime Centre (hosted by the AFP)

The AHTCC, hosted by the AFP, is situated within the AFP's existing Transnational Crime Coordination Centre (TCCC). Its placement within the TCCC reflects the significant overlaps between the goals of the AHTCC and the AFP's existing responsibilities in relation to hi-tech and transnational crime, and protection of the National Information Infrastructure. The AHTCC is the national vehicle to progress serious or complex multi-jurisdictional Hi-Tech investigations. The Centre is a national conduit for investigations, intelligence, forensics, and research and development relating to complex Hi-Tech crime issues. Situated as it is within the AFP, it has access to the computer forensic capabilities of the AFP and to the AFP's international liaison arrangements.

AFP Computer Forensics

The AFP has an internationally recognised forensic science capacity, including computer forensics. The AFP provides high level forensic support for complex Commonwealth and State investigations.

The training and retention of police computer forensic experts has been highlighted as an area of priority for all jurisdictions. Although the AFP has experienced migration of some forensic staff to the private sector in the past, the varied and interesting nature of police work, access to state of the art equipment, and increased remuneration of forensic specialists have combined to make the AFP an attractive employer for specialists in this area.

The AFP is developing a three tiered system of forensic training which aims to keep police roles clearly delineated, rather than requiring all officers to become virtual computer experts. The tiers are as follows:

> Level 1 - Basic understanding of how to operate all common electronic devices (computers; mobile phones, personal organisers etc). Knowledge of what to secure at a crime site. All officers will be trained to this level.
>
> Level 2 - More highly trained senior officers who can collect certain evidence from a crime site eg copy the hard drive of a computer.
>
> Level 3 - Computer forensic specialists who examine evidence in a lab.

Computer forensics remains a relatively immature field in Australia with few specialists operating outside of police forces. Both Murdoch University and UTS are looking at developing academic programs in this area.

Cybercrime Stakeholders

Regulatory Authorities

Australian Securities and Investments Commission (ASIC)

ASIC formed its Electronic Enforcement Unit in 1999. The aim of the unit is to raise consumer awareness of e-crime issues in the area of financial matters. ASIC runs internet surveillance campaigns to identify sites that may breach the Corporations Act by promoting investments schemes and offering financial advice without a license. ASIC also runs a range of education and deterrence programs for industry and consumers. In particular ASIC:

- operates a consumer awareness site called Fido
- runs an online e-crime training program called Enforce.Net, which teaches officers how to handle electronic evidence (Enforce.Net has been used to train officers from a range of law enforcement agencies around Australia)
- runs the Gull Awards, a program which allows consumers to win prizes for reporting financial scams they have encountered to ASIC, and
- has worked with the Internet Industry Association (IIA) to develop a draft Cybercrime Code of Practice.

Australian Transactions Reporting and Analysis Centre (AUSTRAC)

AUSTRAC is Australia's anti-money laundering regulator and specialist financial intelligence unit. AUSTRAC's Cybercrime concerns focus on ensuring that current systems pick-up all significant transaction activity, as well as keeping abreast of technological developments which may allow financial institutions and other reporting entities to circumvent their reporting obligations.

AUSTRAC has a strong interest in proof of identity issues. It is crucial to any transaction reporting regime to be able to correctly verify the identity of parties involved in an online transaction. AUSTRAC chairs the Proof of Identity Steering Committee, with representatives from Commonwealth and State government departments, law enforcement agencies and financial institutions with an interest in proof of identity issues.

Other Stakeholders

Action Group into the Law Enforcement Implications of Electronic Commerce (AGEC)

AGEC was formed in 1997 by the Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA) to investigate the impact of electronic commerce on criminal law enforcement, regulatory and revenue agencies' capacity to function in an environment increasingly influenced by emerging information and communications technology.

The objective of AGEC is to contribute to the Commonwealth's E-Security strategic objective - creating a secure and trusted electronic operating environment - by creating a forum for the identification and discussion of key issues and the development of proactive policy solutions.

AGEC consists of representatives of all HOCOLEA agencies, is chaired by AUSTRAC and reports to HOCOLEA.

In recent times, AGEC has agreed to focus on a small number of high priority issues. Focus groups have being formed to keep a watching brief on four areas: the financial sector, legal and procedural issues, technological developments, and investigative methodology (forensics).

Electronic Security Coordination Group (ESCG)

The role of the Electronic Security Coordination Group is to develop and coordinate Australia's e-security policy. The group consists of representatives from:

Attorney-General's Department
National Office for the Information Economy
Defence Signals Directorate
Australian Security Intelligence Organisation
Australian Federal Police
Department of Prime Minister & Cabinet
Department of Foreign Affairs and Trade
Department of Transport and Regional Services
Department of Industry, Science and Resources
Australian Transactions Reports and Analysis Centre
Australian Investment and Securities Commission
Department of Treasury
Centrelink, and
Australian Bureau of Statistics.

ESCG is chaired by the National Office for the Information Economy. ESCG's main work areas are:

- advancing work on raising e-security awareness in both the public and private sectors
- developing information sharing arrangements with industry, service providers to industry and Commonwealth and State and Territory Government agencies
- ensuring that international activities in e-security are properly coordinated across the Commonwealth, and
- addressing e-security skills, and research and development issues.

Information Infrastructure Protection Group (IIPG)

The role of the Information Infrastructure Protection Group IIPG (formerly the Critical Infrastructure Protection Group) is to provide advice to Government on NII issues of a critical nature. In particular, CIPG will undertake studies as required to identify those elements of the information environment exhibiting critical vulnerabilities, and potential incidents that would have a critical impact on national security, the economy or the general functioning of society.

A critical incident may be defined as an attack or system failure on some part of the NII, which supports or underlies systems or the delivery of services whose loss for more than a short period would:

- be nationally significant, ie. the loss would be felt nationally;
- damage the economic well-being of the nation;
- seriously damage public confidence in the information infrastructure;
- threaten life or public health;
- threaten public order;
- impair national defence; or
- impair national security.

The work of the IIPG supports the activities of the E-Security Coordination Group (ESCG) as they relate to the critical infrastructure aspects E-Security.

The IIPG is responsible to the Secretaries Committee on National Security and is chaired by the Attorney-General's Department. The Australian Crime Commission is a member of the IIPG.

Australasian Centre for Policing Research (ACPR)

The ACPR is a research body established in 1983 by a joint agreement of Police Ministers, and funded by State and Territory police agencies and the Commonwealth. It is based in Adelaide and has a permanent staff of fourteen, bolstered by occasional secondees.

The ACPR has taken a lead role for the Police Commissioners' Conference in the area of e-crime and has done substantial policy development work in this area. In particular it has produced the following documents:

- *The Virtual Horizon: Meeting the Law Enforcement Challenges*
- *Electronic Crime Strategy of the Police Commissioner's Conference Electronic Crime Steering Committee 2001 – 2003*
- *ACPR E-Crime Strategy: 2002-2003 Workplan*, and
- *Critical Issues in Hi-Tech Crime.*

The major outcome of the ACPR's work has been the decision by the Commonwealth, States and Territories to establish the AHTCC. The responsibility for e-crime issues has been transferred to the AHTCC.

Australian Computer Emergency Response Team (AusCERT)

The Australian Computer Emergency Response Team is Australia's foremost Computer Security Incident Response Team (CSIRT) covering the private sector, and was founded in 1992. AusCERT acts as a coordination centre, in an advisory capacity, as a centre of expertise and as a portal to its contacts throughout the world, for issues of computer security. AusCERT is part of the University of Queensland, and is a member of the Forum of Incident Reponses and Security Teams, a global organisation made up of over 70 CSIRTS.

AusCERT's primary service is a subscription based twenty four hour computer security incident response service, which aims to detect, interpret and respond to attacks on their clients' computer systems. AusCERT coordinates information between the affected parties of an attack and other organisations such as foreign incident response teams, vendors, and law enforcement agencies. In addition, AusCERT conducts research into the computer security environment, and also provides advisories, alerts and updates regarding software and network vulnerabilities.

AusCERT has recently launched a national incident reporting scheme and a public alerts service which is supported by funding from a range of Commonwealth agencies, including the Australian Crime Commission. The Commonwealth's relationship with AusCERT on these matters is coordinated by the Attorney-General's Department.

Securities and E-Business Assurance Research Group (SEAR)

SEAR was established in March 2001, and is part of the School of Information Systems, Technology and Management, at the University of New South Wales. It researches a broad range of topics in the field of information system security and e-business. SEAR has also joined with the Australian Computer Crime Manager's Group (ACCMG) to form the Computer Forensic Research Group (CFRG) to guide research in the area of computer forensics, with particular emphasis on:

- the identification of research issues for forensic computing research
- investigating methodologies for computer forensics investigation
- identification of legal issues involved in computer forensics
- investigating intrusion forensics – primarily tracing and tracking activity over the internet, and
- investigating tools and methods for carrying out computer forensics.

The CFRG is in the process of publishing a complete computer forensic methodology.

Business/Government Partnership

Cybercrime Code of Practice

ASIC has worked in conjunction with the Information Industry Association (IIA) to develop a Cybercrime Code of Practice. The IIA is Australia's national internet industry organisation, representing a diverse range of internet stakeholders including telecommunication carriers, ISPs, content creators, e-commerce solution architects, and hardware and software vendors. The Cybercrime Code outlines procedures for interaction between internet stakeholders, particularly ISPs and law enforcement with regard to e-crime. It also sets base criteria for the retention of records

Trusted Information Sharing Network for Critical Infrastructure Protection

In November 2001, the Prime Minister announced the formation of the Business–Government Task Force on Critical Infrastructure. The task force meeting in March 2002 brought together high-level representatives from business, State and Territory governments and Commonwealth agencies, to discuss the national security aspects of Australia's critical infrastructure. The Task Force recommendations included the establishment of a trusted information-sharing network and advisory council.
On 29 November 2002, the Commonwealth Government announced its intention to form the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN). TISN is intended to allow the owners and operators of critical infrastructure to share information on important issues such as business continuity, consequence management, information system attacks and vulnerabilities, e-crime, protection of key sites from attack or sabotage, chemical, biological and radiological threats to water and food supplies, and the identification and protection of offshore and maritime assets.

TISN will involve a number of advisory groups for different business sectors, utilising existing groups where possible. It may be necessary to have multiple groups within a single sector so as to create an atmosphere of trust, based around shared threats and vulnerabilities (e.g. aviation within the transport sector). The Commonwealth agency with portfolio responsibility for a particular industry sector will coordinate the creation and conduct of the advisory groups for that sector. It is anticipated that the advisory group will develop strong links to the equivalent US forums-the Information Sharing and Analysis Centers (ISACs).

Negotiations are underway with regulating agencies to have TISN recognised as an appropriate forum for owners and operators of critical infrastructure to work together to protect critical infrastructure.

Conclusion

Cybercrime will remain a challenge for both governments and the private sector but one that is within our capabilities to prevent, detect, investigate and prosecute. While new technology provides opportunities for criminal enterprises, it can also provide new tools to counter criminal enterprises if that new technology is taken up and adopted by law enforcement and the private sector agencies.. National cooperation and the establishment of national investigative and service agencies such as the Australian Crime Commission, the Australian Hi-Tech Crime Centre and CrimTrac have placed Australian law enforcement in a position to combat Cybercrime.

The Commonwealth will continue to develop partnerships with the private sector in the areas of information and intelligence, forensic capabilities, specialist investigation services, and prevention and detection procedures.