

PRIME MINISTER'S SCIENCE, ENGINEERING AND INNOVATION COUNCIL

FIFTH MEETING - 2 JUNE 2000

AGENDA ITEM 5

SCIENCE, CRIME PREVENTION

AND

LAW ENFORCEMENT

Prepared by:
PMSEIC Working Group on Science, Crime Prevention & Law Enforcement

2 June 2000

EXECUTIVE SUMMARY

Technology is rapidly changing the speed and manner in which Australians interact with each other and with the world, the way in which business is transacted and the means by which partners in commerce, or crime, are connected and identified. Those who hurt and abuse others, or profit from illegal activities, are no less able or interested in gaining advantage from technology than are businesses and the general public in protecting themselves from the former.

Globalisation is breaking down state and national boundaries and the boundaries between public and private sectors. As technology helps criminals to operate more easily and quickly across borders, so law enforcement capability must continuously improve to keep one step ahead.

Crime costs Australia an estimated \$11 - \$13 billion pa. The criminal justice system costs States/Territories and Commonwealth another \$6.4 billion. Overall, crime costs us at least \$18 billion per annum (2.5 % of GDP), or \$1,000 per man, woman and child.

Recent Federal Government policies and funding through programs such as the *National Illicit Drugs Strategy* (NIDS) and *Towards a Safer Australia* have driven a renewed focus on innovation in law enforcement agencies, including innovation in the use of science and technology. For example, work on *CrimTrac* (\$50 million over 3 years) will encourage better information exchange and the application of new investigative capabilities across federal and state jurisdictions. Agencies are on a steep learning curve in regard to gaining efficiencies and success through cooperation. There has been support for the establishment of much needed new capabilities in drug detection, such as the *National Heroin Signature Program*, new detection technologies for Australian Customs, and enhancement of existing forensic infrastructure for the Australian Federal Police.

The PMSEIC Working Group on Science, Crime Prevention and Law Enforcement has reviewed the extent to which the law enforcement community has embraced science and technology in dealing with the challenges it faces. In particular the Working Group has noted that there are two key components of effective crime prevention and law enforcement which will require development to deal with the emerging criminal environment. These are proof of identity and rapid availability of information and intelligence. It is clear that to develop these two components the law enforcement community must embrace science and technology at every available opportunity. The Working Group has found both good and bad news.

Some world-class tools and consultancy services in niche areas of forensic technique, instrumentation, systems security, data mining and analysis have been developed for Australian needs and exported through partnerships between Australian scientists, firms and law enforcement agencies. Due to the diversity of such products and services and of sectors from which they originate, more research would be needed to estimate their value, or to assess the potential size of what could, aided by appropriate policies, grow into a forensic industry.

Examples include *Poli-Light*, an instrument for revealing difficult to detect fingerprints, developed in collaboration between the Australian National University and the former Science Directorate of the Australian Federal Police (AFP). Now manufactured under licence by *Rofin Australia*, over 600 *Poli-Light* units are operating in over 49 countries, with an approximate total export value of \$12 million.

Our law enforcement agencies have acquired and adapted some best practice overseas and locally developed systems to good effect. The Working Group has not found a cost-benefit analysis specific to investment in new equipment and systems by law enforcement agencies.

But internal estimates suggest, that alone in the area of tax fraud, hundreds of millions of dollars have been saved just through deterrence or detection facilitated through the application of advanced financial tracking systems.

The bad news is, that to a large extent, successes in developing or commercialising Australian crime fighting technologies (or in acquiring overseas technologies) are relatively few compared to the number of technologies that could become success stories. These need to be identified, matched to potential applications, assessed and promoted in a timely manner.

There is no comprehensive system to ensure that Australia develops, or can acquire the cost effective mix of new technologies and expertise needed to keep ahead of drug pushers and fraudsters. Further investments are not only warranted, but critical in some areas, eg, infrastructure to enable large scale processing of more routine DNA testing requirements. But these must be guided by a strategic vision linking public policy, science, business and law enforcement for mutual benefit.

With the right mechanism to identify, assess and promote the adoption of appropriate new technologies, Australian firms and the community could recoup some of the costs of crime through new business opportunities. There could be greater economic benefit from innovation in crime prevention technologies, than has often been the case with previous technical procurement arrangements.

Australia must extract more value and leverage from crime prevention and law enforcement expenditure. Organised crime can often out-spend and out-manoeuvre 'soft targets', or the law. One Mexican drug trafficker for example, is reported as earning US\$10 billion per annum and cases are cited of criminal 'buy outs' of security technology, to safe-guard criminal activities!

Applying Australia's expert knowledge, with better planning and cooperation, is the innovative way to multiply the impact of our more modest resources.

In regard to the technical infrastructure of crime prevention and law enforcement, a higher degree of coordination than currently exists will be essential if Australia is to strengthen its security and enforcement systems for a high speed, high growth, but higher-risk future.

There are some useful models of cooperation (such as the National Institute of Forensic Sciences) and strategic planning that could be readily adapted to help Federal and State law enforcement agencies engage more wholeheartedly with Australia's strong scientific base and niche industrial capabilities in relevant fields. Some models are outlined in Chapter 3.

There are also legislative frame works, eg. those governing the admissibility of evidence and interception of communications, which must be reviewed in order that new technologies and techniques can be acceptable to the criminal justice system. Community concerns must be addressed about the application of new technologies, for example, the protection from misuse or tampering, of information held in databases of DNA tests. Some of this work appears to be under way, for example in regard to privacy of personal data on public and private databases.

This paper does not deal with legislative or privacy issues, which are being dealt with through various processes, some at the State Government level, by policy makers and specialists in other fields and should also involve community consultation. The Working Group believes there is an urgent need for such processes to move in step with the technical improvements underpinning crime prevention and law enforcement, which are the subject of this paper.

Recommendation 1

Improve law enforcement capacity to fully engage with the scientific community.

There is a need to change the dominant culture in law enforcement agencies, which views scientists and ‘techos’ as a curious, if albeit frequently necessary, adjunct to the main game of crime fighting. A more wholehearted engagement with the science community must be actively promoted, from the top, and possibly aided by the mechanisms recommended below. This engagement in turn, should inform strategic planning by law enforcement agencies that is conducive to the growth and exports of Australian firms that can supply agency requirements.

Recommendation 2

Appoint a high level S&T policy group, underpinned by a science and technology clearing house.

There is an urgent need for a mechanism to receive and consider timely and detailed expert advice on, as well as cooperation in:

- ⇒ Strategic planning to identify and foster solutions from science and technology for crime prevention, security and law enforcement needs.

This paper identifies a number of possible models that could be further explored (see sections 3.1-3.3). There should be little delay, as urgent tasks include to: consider future policy needs and the technological requirements; avoid duplication in procurement efforts; achieve cost savings through larger contract sizes; achieve greater inter-operability of systems; and speed up the exchange and use of real-time intelligence by agencies.

The policy group and cooperative mechanism to be developed as recommended above, should be able to call on expert technical advice and specific research from a new center or network for diffusion of crime prevention and law enforcement technologies. Such a center or network should have the capability to become the preferred and prime source of advice for:

1. identifying existing or emerging Australian or overseas technologies and systems that may potentially offer a cost effective solution for a given purpose;
2. assessing in detail, the extent to which those technologies or systems can, cost-effectively deliver what is required; and
3. assist in the transfer and/or dissemination of such technologies and systems once they have been selected for adoption by one or more jurisdictions.

Recommendation 3

Identify mechanisms to encourage Australian industry and research agencies to participate in the development and production of new, affordable technologies for law enforcement

A mechanism and source of funds needs to be provided to ensure that there is cross fertilisation between forensic science, and user groups with potential applications. As an emerging industry, forensic business would need to rapidly respond to new discoveries globally in fundamental science. This should be underpinned by a clear business plan (predicated on investment funds) to create a forensic industry, which could grow to support itself.

CONTENTS

CHAPTER ONE	CRIME PREVENTION - WE ARE ALL STAKEHOLDERS	1
1.1	NEW TECHNOLOGY, NEW CRIME, NEW ROLES FOR GOVERNMENT?.....	2
1.2	'COST EFFECTIVE SOLUTIONS NEEDED FOR'	3
1.3	THE LAW ENFORCEMENT COMMUNITY AND ITS STAKEHOLDERS	5
CHAPTER TWO	KEY TECHNOLOGIES & EXPERT SERVICES	7
2.1	PHYSICAL SCIENCES.....	7
2.1.1	<i>Finger Printing</i>	7
2.1.2	<i>Drug Profiling & Drug Detection</i>	8
2.1.3	<i>Surveillance, Communications & Monitoring</i>	9
2.1.4	<i>Sub-Surface Radar</i>	10
2.1.5	<i>Forensic Techniques for Materials</i>	10
2.2	BIOLOGICAL SCIENCES, BIOTECHNOLOGY & BIOMETRICS.....	11
2.2.1	<i>DNA Analysis</i>	11
2.2.2	<i>Biometrics</i>	12
2.3	INFORMATION & MATHEMATICAL SCIENCES	13
2.3.1	<i>Financial Intelligence - tracking 'dirty money'</i>	13
2.3.2	<i>Detection of Suspect Payment Claims</i>	15
2.3.3	<i>Securing Electronic Commerce</i>	16
2.3.4	<i>Facial Imaging</i>	17
2.3.5	<i>Networks for criminal intelligence analysis</i>	18
CHAPTER THREE	FRAME WORKS FOR PARTNERSHIP	19
3.1	LINKAGES	19
3.2	AUSTRALIAN MODELS OF COOPERATION AND COORDINATION.....	21
3.3	OVERSEAS MODELS OF COORDINATION.....	22
3.4	CONCLUSIONS.....	23
APPENDIX 1	PMSEIC WORKING GROUP ON SCIENCE & CRIME FIGHTING.....	25
APPENDIX 2	FORENSIC SCIENCE COURSES AVAILABLE IN AUSTRALIA.....	26
APPENDIX 3	PRODUCTS & SERVICES FOR CRIME PREVENTION.....	28
APPENDIX 4	THE NATIONAL CRIME AUTHORITY.....	30
APPENDIX 5	CASE STUDY FROM THE NATIONAL ILLICIT DRUGS STRATEGY (NIDS).....	31

This paper was prepared by an independent working group for PMSEIC. It's views are those of the working group, not necessarily those of the Commonwealth.

CHAPTER ONE

CRIME PREVENTION - WE ARE ALL STAKEHOLDERS

Technology is rapidly changing the speed and manner in which Australians interact with each other and with the world, the way in which business is transacted and the means by which partners in commerce, or crime, are connected and identified. Those who hurt and abuse others, or profit from illegal activities, are no less able or interested in gaining advantage from technology than are businesses and the general public in protecting themselves from the former.

Expert commentators have pointed out regularly over the last few years, that technology is outpacing the law and criminal justice system. Various analyses indicate that the relatively modest investments required to address this problem would be well justified.

The annual costs of crime in Australia are conservatively estimated at between \$11 - \$13 billion¹. In addition, the criminal justice system (States/Territories and Commonwealth) costs some \$6.4 billion (1996 values), of which the States / Territories bear around 63%. At least a further \$1.3 billion may be spent by private businesses and individuals on goods and services provided by the security industry, to prevent future crimes or lessen the severity of their impact.

In total, crime costs Australia a minimum of 2.5 % of GDP (largely the result of white collar crime) plus 1.9% of GDP expended by the public and private sectors to prevent and counter crime. Overall, crime costs at least \$18 billion per annum, or \$1,000 per man, woman and child.

Neither do these numbers capture the hidden costs to individuals and society, eg. reduced opportunities and participation in life and economic activity, because of the fear of crime and the cost to our younger generations through drug abuse.

Commonwealth and State Governments have recognised the concern of ordinary Australians to obtain increased levels of safety from personal and economic injury resulting from crime. There have been new programs and investments in infrastructure to improve preventative measures, speed the identification, investigation and prosecution of criminals and to deal with the after-effects, eg. compensation for victims, justice and rehabilitation for offenders.

In its first term, the Commonwealth Government provided \$13 million to National Crime Prevention, in May 1999 a further \$21.4 million over four years (*Towards a Safer Australia*) including a component for early intervention work with families and young people. From the budget of 1999, \$50 million over 3 years will be provided to establish *CrimTrac*, encouraging better integration of investigative capabilities across federal and state jurisdictions. As part of the Government's *Tough on Drugs* strategy, additional resources were provided to *Australian Customs* amounting to \$35.4 million over four years for new technology, the creation of specialist search teams and an additional marine crew to improve surveillance in the Torres Strait. AUSTRAC, Australia's anti-money laundering regulator and financial intelligence agency was funded to improve its profiling and data mining techniques.

But Australia must extract yet more leverage from crime prevention and law enforcement expenditure. Organised crime can often out-spend and out-manoeuvre 'soft targets', or the law. One Mexican drug trafficker for example, is reported as earning US\$10 billion per annum and cases are cited of criminal 'buy outs' of security technology, to safe-guard criminal activities!

Applying Australia's expert knowledge, with better planning and cooperation, is the innovative way to multiply the impact of our more modest resources.

¹ Walker, J., 1997, *Trends & Issues in Crime and Criminal Justice No.72*. Australian Institute of Criminology

The focus of this paper is the technical innovation urgently needed by the law enforcement community over the next few years, to underpin Australia's crime prevention strategies for a high speed, high growth, but seemingly higher-risk future.

The risk is particularly high in regard to electronic fraud. Recent figures from the United Kingdom for example suggest, that while crime levels for other categories have declined in recent years, the incidence of electronic crime has been increasing by 14% per annum.

1.1 New Technology, New Crime, New Roles for Government?

Criminals are opportunistic. In the 1920s, cheaper private automobiles became available and affordable to many. In addition, cars offered: speed; distance; carrying capacity; relative anonymity (compared to the rider on a horse!). There was a corresponding explosive growth in certain crimes, including: bank robberies and housebreaking; abduction; smuggling; and theft of cars themselves. Countermeasures included: introduction of number plates, chassis/engine serial numbers; motorcycle police and patrol/pursuit cars; special regulation of goods vehicles; improved premises security; and improved cross-jurisdictional arrangements.

In whatever technological environment, crime prevention and law enforcement centres on:

- Reducing the supply of motivated offenders (includes social policies); and
- Making the crime harder to commit and less rewarding (security, detection etc).

In our era, more than ever, new technologies can help with 'target hardening' – to increase the effort and risks of committing crime and reduce the potential rewards.

In a recent expert technical report to the Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA)², the age of IT, advanced communications and e-commerce is said to be characterised by: global reach; openness and accessibility of business and government computing systems to a public network; automation of operations; immediacy –(business systems operate at computer speeds with reduced human intervention and supervision); loss of collateral information (traditional ways of identifying transaction counterparts); cryptography – (secret transfer of data securely over an open network); and new business models to take advantages of new technologies and their characteristics.

The report by the Research Group into the Law Enforcement Implications of Electronic Commerce (RGEC) urges governments to develop a strategy (akin to risk management in a company's business plan), to ensure that criminals and tax evaders do not exploit those characteristics. RGEC proposed a complementary set of measures to:

- foster a more secure, yet flexible environment for the new economy (one which is conducive to the rule of law and, conversely, hostile to crime); and
- provide a set of tools and powers to enable law enforcement to do what will be expected of it in the new environment.

An example of the latter was RGEC's recommendation for a national computer forensics capability to allow on-line investigations, giving agencies a consolidated investigative tool.³

² AUSTRAC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do*. Research Group into the Law Enforcement Implications of Electronic Commerce (RGEC), Sydney, 1999

³ Further work to progress this, as well as other RGEC recommendations, is currently being undertaken by HOCOLEA, in consultation with the National Office for the Information Economy (NOIE).

At the same time it was acknowledged that careful consideration of an appropriate system of controls would be needed to ensure that investigations respect privacy when appropriate and are validated as admissible evidence.

Excessive preoccupation with specific countermeasures, (themselves susceptible to avoidance by criminals), should not be at the expense of ‘target hardening’ of the business environment. It is usually the unexpected, which causes most harm.

An example of ‘target hardening’, *Gatekeeper*, the Commonwealth strategy for the use of Public Key Infrastructure (PKI) is a key enabler for the delivery of Government online. It also leads by example to encourage the uptake of e-commerce in the private sector. *Gatekeeper* provides a structure through which government can ensure integrity, security and authenticity in the transmission of information and transaction of business.

RGEC concluded that: “Australia is positioned to benefit enormously from its embrace of electronic commerce and the wider information economy.” One of the reasons is “the robustness and credibility of its traditional legal system – both civil and criminal.”

In the words of Prime Minister Howard, opening the 15th Asian Regional Conference of Interpol:

“The desirability of a country like Australia as an economic destination depends not solely upon the strength of its economic foundations, but also upon the security of those foundations. (law enforcement agencies), protect the integrity of data flows, banking infrastructure, financial and other telecommunication links. When this is added to transparency in political decision making, law enforcement agencies can contribute to strong business confidence.”

The general approach advocated by RGEC for electronic commerce was ‘light-touch’ regulation and strategic alliances between governments, industry and consumers. Government can give leadership, which “identifies and encourages the conditions needed to ensure the information economy flourishes but which does not dictate how those conditions should be achieved.”

To safeguard the public from crimes of violence, burglary, drug pushing etc, technological changes may cut across current community expectations, as well as the existing processes of the criminal justice system. Some areas of current concern to policy makers are summarised below.

1.2 ‘Cost effective solutions needed for’

A forthcoming book on controlling electronic theft by the *Australian Institute of Criminology*⁴ states: “The information revolution has given rise to many new ways to commit theft, and many new things to steal. This has occurred against a background of increasing recognition that the state is limited in its capacity to control human behaviour, and that security and prosperity in cyberspace will depend upon the proper functioning of, not just agencies of government, but a constellation of institutions and conventions in civil society.”

Some of the types of new electronic crime include: denial of service attacks (“I Love You Bug” and “Melissa” virus), theft of services; encrypted communications in furtherance of criminal conspiracies; information piracy; the dissemination of offensive materials (including paedophilia and extortion threats); electronic money laundering; electronic vandalism and terrorism; telemarketing fraud; illegal interception; and electronic funds transfer fraud.⁵

⁴ Grabosky, P., Smith, R. and Depmsey, G. (forthcoming) *Electronic Theft: Crimes of Acquisition in the Digital Age*. Australian Institute of Criminology, Canberra.

⁵ Grabosky, P., Presentation to the 70th Conference of Commissioners of Police of Australasia and the Southwest Pacific Region, Canberra, 13 March 2000

There are limits of the law, and of law enforcement agencies, in controlling electronic crime, and a growing impetus to share the burden between law enforcement agencies, prospective victims, and other institutions of society. Financial liability for losses incurred through internet fraud for example, is shifting from financial institutions to the merchant.

1.2.1 Money laundering

Money laundering in and through Australia is estimated run to about \$3.5 billion each year⁶. This money comes mainly from drug trafficking, tax evasion and fraud, with smaller amounts from the cash economy, an element of tax evasion, and crimes of a lesser nature. Globally, global money laundering from drug trafficking alone amounts to \$1,100 billion each year. Total money laundering is estimated at between 2-5 % of world GDP⁷.

People involved in large-scale crimes such as drug trafficking and large-scale tax evasion usually set up elaborate systems to hide the nature and financial aspects of their crimes. Australia's technologically advanced system of tracking such transactions is described in section 2.3.1.

1.2.2 Identification for financial institutions

Federal government legislation demands that financial institutions sight documentation that meets minimum standards of identification before a person can open an account⁸. However, many of the documents required for identification can be forged. While appropriate legislation over the past decade or so has made it more difficult for a person to open an account in a false name, the quantity of money involved in money laundering, and in tax evasion, clearly indicates that criminals have opportunities that cannot be removed merely by legislation. Many of these opportunities exist because there is not as yet a positive and completely reliable means of identification. Biometrics (see 2.2.2) is an emerging area that may help solve this problem.

1.2.3 Identity over the Internet

All communication over the Internet can be considered to be anonymous. Traditionally, all such messages lack any positive identifying mark of the sender or the inquirer. A purchaser can use any computer to buy goods over the Internet. Any marker that can provide some identification of the user is easy to forge, rendering it ineffective as a means of proving the identity of the user.

While it may be possible to trace and locate the particular computer used to transmit many messages or data, the identifying codes can be falsified. Messages can have the route through which they were sent falsified or disguised. Re-mailing services can remove all traces of the true source of the messages and send it out again with a new header. Such elaborate disguises could indicate a suspect criminal action. Techniques are also available, which support anonymous access to web sites so the user is not giving out any personal information.

Modern computers using chips such as the Pentium III, can be traced through an identifying serial number built into the chip. Nevertheless, identifying a particular computer does not identify the particular operator who made a transaction or sent a message (such as an authorisation to transfer money overseas) from that computer at a particular time. Forged information, such as computer details and Internet service provider addresses, is useful to criminals because it can be used to mask their true identity.

The identity of e-commerce partners and internet sites must be verifiable so that doubts about their authenticity do not grow into a crisis of confidence, which could greatly limit the tremendous potential of e-commerce.

⁶ Walker, J., *Estimates of Money Laundering in and through Australia*. AUSTRAC, Sydney 1995

⁷ Camdessus, M., President of the International Monetary Fund, quoted February 1998

⁸ Financial Transaction Reports Act 1988

Already there is some misinformation about the security of the Internet and shortcomings will continue to be exaggerated if solutions for proof of identify and verification are not provided and accepted as robust. See sections 2.3.3 and 2.3.4.

1.2.4 People smuggling

People smuggling has increased from 157 illegal immigrants in 1997–98 to over 3500 from July 1999 to April 2000. The majority of illegal immigrants to Australia were from the Middle East. The Department of Immigration and Multicultural Affairs (DIMA) has implemented a number of new technologies to detect and identify those involved in people smuggling, including for rapid communication with other relevant agencies in Australia and abroad.

A mobile communications suite will be supplied, including laptop computers with mobile access to the Internet, and the supply of digital cameras capable of recording high quality images and short continuous video footage. This will provide for the transmission of all types of text, data, voice, still and video images through a continually available medium of communications.

DIMA uses 'Borderguard', a machine reader that captures passport details, and performs basic forensic checks. Amongst other capabilities, this technology performs facial matches of the passport photograph against stored photographs. DIMA is also considering introducing mandatory fingerprinting with scanning technology to enter fingerprint data, and automated data matching to identify individuals, and the latest biometric identification technologies such as DNA testing, and face, palm or retinal recognition and voice testing.

Early detection of vessels suspected of carrying illegal immigrants is important. To aid in this, satellite links are being fitted to surveillance aircraft to enable more reliable long-range communications. Digital cameras are replacing conventional film cameras on surveillance aircraft with satellite communications. This will facilitate rapid dissemination of images, allowing agencies to make quicker assessments of the situation. With future low cost, high data rate transmission through low earth orbiting satellites, real time transmission of digital video will be possible.

Other technologies being investigated include wide area detection/identification from satellites and unmanned aerial vehicles using synthetic aperture radar, and multi- or hyper-spectral imaging systems. High frequency surface wave radar may detect larger surface vessels out to 300 kilometres. Inverse synthetic aperture radar mode for current search radars may facilitate long-range classification of targets, reducing the need for aircraft to deviate from planned search patterns. See section 2.13.

1.3 The Law Enforcement Community and its Stakeholders

The law enforcement community, for the purposes of this paper, are those individuals and organisations in the public and private sectors whose services the people of Australia engage to safeguard their person and property from injury caused by the illegal actions of others, as well as to bring to justice those that have committed such actions.

The Commonwealth Government funds the following key agencies with criminal justice (including law enforcement) responsibilities: the Attorney-General's Department, the Australian Federal Police (AFP); Australian Customs Service (ACS); Australian Bureau of Criminal Intelligence; the Australasian Centre for Policing Research; Australian Institute of Criminology (AIC); Australian Transaction Reports & Analysis Centre (AUSTRAC); Australian Government Analytical Laboratories, including Australian Drug Forensic Laboratory (AGAL/ADFL); the

Australian Security Intelligence Organisation (ASIO); National Crime Authority (NCA)⁹; and the Commonwealth Director of Public Prosecutions (CDPP).

Over 60% of the resources for the criminal justice system in Australia are managed by State and Territory Governments. In common with their Federal counterparts, State agencies such as Attorney-Generals' Departments or equivalent; Directors of Public Prosecutions and police services, make increasing use of sophisticated technical infrastructures and new technologies.

The potential role of the Commonwealth's Defence Science & Technology Organisation (DSTO) in supporting the application of technologies to the criminal justice system and to crime prevention is worthy of further exploration. In the US, the Office of Science & Technology of the National Institute of Justice has an MOU with the US Department of Defence (see 3.3.3).

Another example of how a defence-law enforcement linkage might be developed, is suggested by Australia's Defence Signals Directorate (DSD). DSD's Information Security Group plays a key role in the protection of Australian official communications and information systems. It is the national authority for communications and computer security. As such, it provides material, advice and assistance to Commonwealth Government Departments, authorities and the Defence Force. It also works with industry towards the development of new cryptographic products. In order to deal with the increasing requirement to evaluate information security products, DSD established the Australasian Information Security Evaluation Program (AISEP) in 1995.

In regard to the technology that supports the law enforcement community, the stakeholders of this community that are of particular relevance include:

- users of specific law enforcement services and intelligence, such as Government agencies and commercial organisations, eg. the Australian Tax Office, Health Insurance Commission, banks, insurance companies;
- public and private sector developers and suppliers of technology, equipment, systems and expert consultancy services to law enforcement organizations and their personnel;
- scientific, social and economic researchers in universities, Government research institutes and private think tanks, providing knowledge to solve specific problems, suggesting new applications, prioritising problems, targeting solutions to optimise policy objectives; and
- providers of education and training to law enforcement community personnel and to researchers, technologists and other specialists, in the above stakeholder groups.

Stakeholders of the Australian law enforcement community are not only within Australia, or necessarily Australian entities. Numerous overseas Government organisations have cooperated with Australian partners in law enforcement and have been able to learn and benefit from Australia's technical and methodological expertise in certain areas.

Also of importance, are the overseas suppliers of key technologies and knowledge. As in most areas, Australia's future success in crime prevention and law enforcement will depend as much on the cost effective assimilation of suitable overseas technologies, as it will on the development and commercialisation of our own.

The role of, and opportunities for the Australian security industry sector, needs more detailed consideration than is given in this report. For example, how much further can firms that provide general security services and products assist the commercialisation of new Australian technologies? Some of these firms are already partners with research and law enforcement agencies in developing some of the new technologies highlighted in this paper. Appendix 3 indicates some relevant industry capability.

⁹ A description of some of NCA's work in relation to money laundering is at Appendix 4.

CHAPTER TWO

KEY TECHNOLOGIES & EXPERT SERVICES

From a wide range of security and law enforcement technologies, the focus of this paper has been narrowed to a (still large) group of technologies and services that help to:

- prove the identity of the person or entity of interest; and/or
- deliver and analyse criminal intelligence to law enforcement personnel in ‘real-time’, or at least, much more quickly than has been possible in the past.

Proof of identity and ‘real time’ availability of intelligence are two of the most critical elements to improving crime prevention, including through a stronger deterrence effect, as well as detection and apprehension of crime suspects.

PHYSICAL SCIENCES

FINGER PRINTING

Now

Polilight illuminates and reveals finger prints on surfaces where they are usually difficult to detect. Developed in the 1980s by the ANU and AFP’s former Science Directorate, *Polilight* is manufactured by Rofin Australia. The patented innovation, a frequency-tuning device, enables *Polilight* to deliver a highly selective light over a broader spectrum.

New

AFP and others continue to research better methods and protocols for fingerprint detection. A new method reveals prints on polymer bank notes using metal deposition under vacuum. Together with an Australian firm, *Dynavac*, a large vacuum-metal deposition unit has been developed.

Next Step / Impediment?

Development of field devices to enhance latent fingerprints and for recording on-site. This need funds for basic research and venture capital to develop products.

Three fields of science have provided most of Australia’s new technologies and specialist knowledge applied to these two purposes: **physical sciences** (eg. analytical chemistry, materials science, optics, electronics, physical analytical techniques); **biological/medical sciences** (eg., forensic pathology, dentistry, DNA analysis); and **information & mathematical sciences** (eg. software for risk assessment, profiling, modelling and data mining).

Australia enjoys the services of world-leading-edge expertise in a few niche areas, eg. forensic dentistry, and applications of data mining, where a small number of scientists and specialists are highly sought after by overseas as well as local agencies.

The following profiles of some key technologies and areas of application are not exhaustive, but those the Working Group believes should be regarded as priorities for inclusion in more detailed short-medium term strategic assessments and planning that are needed to maintain and enhance Australia’s crime prevention capability.

2.1 Physical Sciences

2.1.1 *Finger Printing*

If fingerprints had only been discovered in the last few years, the excitement generated in law enforcement, and for the broader justice system, would have far exceeded even DNA, because fingerprints are still the only characteristics that can uniquely identify a person. The fact that forensic application of fingerprints has been with us for over a century should not diminish the excitement.

Australia has a good record on fingerprinting research. Development of the vacuum metal deposition (VDM) technique illustrates the importance of user-researcher links. The original idea came from an AFP technician, and a PhD student was employed for 6 months to research and refine the details for full development.

Commercialisation of VDM is the next challenge, for which Australia's niche instrument making capability needs to be further promoted. The Australian company *Dynavac* has currently produced the VDM deposition cylinder and associated control equipment on a one-off basis. Another is being produced for New Zealand.

New fingerprinting technologies must be made more accessible to law enforcement officers in the field. The new national automated fingerprint identification system (NAFIS), being implemented under CrimTrac will enable the taking of fingerprints by 'live scan' and improve matching through digitisation of existing of fingerprints and improved matching algorithms.

2.1.2 Drug Profiling & Detection

Analysis of drugs' chemical signatures or packaging can identify the seized drugs as identical with those seized in previous operations, showing continual importation, or identifying their source. Drug signatures can be used to show: the level of an individual's involvement in trafficking; supplier-dealer-user networks (by pointing to possible new links between seized drugs), leading to more successful prosecutions; and trends in illicit production and imports. Such operations can seriously disrupt an international drug distribution ring.

Current technology depends on the availability of extremely sensitive gas chromatograph mass spectrometers that can detect these small amounts of substances. Similarly with packaging, tracing various individual substances in the materials of manufacture and their concentrations can be useful. A wide range of techniques are used for these analyses.

Australian initiatives have been through the Australian Government Analytical Laboratories (see Appendix 5), the Australian Federal Police Laboratories, regional laboratories in Victoria and South Australia, and at Deakin University and the University of Technology, Sydney. Drugs targeted by these laboratories are heroin, cocaine and amphetamines.

New instrumentation, such as the isotope-ratio gas chromatograph mass spectrometer, identifies the isotopic ratio of carbon within, rather than the identifiable impurities of a substance, to detect whether two batches are the same. It is necessary to develop this technique for forensic research.

Isotope ratios of other elements such as hydrogen, are now available to greatly increase the potential of the technique. It is expected that isotope-ratio mass spectrometry of more elements may be obtained directly. This will mean the origin of the illicit compound can be identified, since the isotope ratio depends on the location of the original biological source, methods of processing and manufacture in the clandestine laboratory. This ratio is specific to the laboratory and will link the production point and the distribution of illicit substances.

The current forensic technology has been in use only four to five years. Isotope ratio gas chromatography mass spectrometry has been fully developed for about the same time, but has not been applied extensively to forensic science. It is just one more example of an emerging technology for which the forensic application has yet to be explored.

It is necessary for Australia to develop and enhance contacts between those firms capable of developing new technologies and the people using them for forensic purposes. Most of the technology in mass spectrometry is developed overseas, although Shimadzu Pty Ltd manufactures such equipment in Australia. Australian researchers must be encouraged to work in this area where results of research are primarily to the benefit of the public.

Before illicit drugs can be analysed, they must be detected and seized. Particle analysers now in use can detect traces of up to 45 narcotic substances simultaneously in concentrations of less than one billionth of a gram.

This paper was prepared by an independent working group for PMSEIC. It's views are those of the working group, not necessarily those of the Commonwealth.

This apparatus is of Canadian origin, but innovative use by *Australian Customs* is widely recognised. The equipment can detect drugs mixed with less harmful substances as a means of trying to avoid detection of the main drugs.

This capability is timely, since a flood of new drugs is entering Australia from South-East Asia. In particular, new variants of amphetamines with stronger and different properties are being distributed to youth for use as recreational drugs. If the technology is not in place to trace networks of distribution in this area, Australia will remain a target for the distribution of new and existing illicit drugs.

Identification of anabolic steroids and other substances abused by sports people will be an emerging law enforcement issue. By making Australia a difficult area in which to work, the providers of these illicit substances will choose other markets for the distribution of their drugs.

2.1.3 Surveillance, Communications & Monitoring

Satellite technologies have application to surveillance, communications, and monitoring. The *CRC for Satellite Systems* is pioneering **micro-satellite** technologies for affordable access to space. This CRC is introducing new communication frequency bands, advanced on-board signal processing, and accurate positioning techniques for Low Earth Orbit (LEO) micro-satellites capable of object identification, location, and tracking. Applications include:

A. Surveillance

At present sensors can provide wide-area covert visibility of maritime targets, covert detection of remote illegal operations, change detection at land-based targets, and high resolution imaging. **Within five years**, small and low-cost LEO micro-satellites will provide resolution better than 5 metres, for object detection and characterisation, eg. of maritime targets, illegal crops, and chemical signatures around illegal processing sites.

B. Communications

Costly geostationary satellites currently provide satellite communication services. **Within five years**, LEO micro-satellites will provide enhanced personal real-time voice, data and motion video, and **highly secure personal communication** services. Internet service provision to remote areas will also be supported by micro-satellites.

C. Monitoring

Within five years, requirements for **covert tracking** of matchbox sized targets, covert unattended monitoring of remote sites, asset tracking and status (eg. container ingress, infrastructure status) will be supported by LEO micro-satellites. In addition, **covert unattended monitoring** of remote site real-time voice and video, mobile targets, prisoner home detention systems in both suburban and rural areas, and monitoring of vehicle speeds, mechanical condition and other parameters will also be achievable.

Within the CRC for Satellite Systems, there is the combined capability of industrial and technological know-how to deliver affordable micro-satellite services in support of law enforcement. The CRC proposes a *requirements analysis*, to investigate technical solutions, identify costs, and draft an implementation strategy.

PHYSICAL SCIENCES

Illegal Substance Detection

The Australian Sports Drug Agency will receive \$1 million in the 2000 Budget to test blood for the banned substance erythropoietin (EPO), should a test become available.

The Commonwealth previously allocated \$1.5 million for the development of a validated test for EPO which it hopes to have by the Sydney 2000 Games.

Artificial EPO, which until now has been undetectable, increases the number of red blood cells, lifting oxygen levels to boost performance.

A decision for **no action** would deprive Australian agencies of the ability to design and control satellite information services tailored to support national requirements for law enforcement.

2.1.4 Sub-Surface Radar (SSR)

CSIRO Telecommunications & Industrial Physics (CSIRO TIP) has developed SSR, an electromagnetic sensing technology commonly used to locate buried or hidden objects, eg. pipes; reinforcing rods and voids; in mining exploration; ore-body delineation; and machine guidance.

When a high frequency transmitted pulse encounters a change in dielectric properties, energy is reflected back to a receiving antenna on the surface. The time between transmit and receive gives a measure of the depth of the object. The technology works well in most common construction materials such as concrete, masonry, brick and wood, including cavity walls and is equally capable of detecting non-metallic or metallic objects.

CSIRO TIP has used SSR for over a decade in coal mining and land mine detection and has developed a world-leading capability related to high-resolution, close-range applications. This has been successfully employed in the detection of objects hidden in walls or floors of buildings (for example, fine wires, microphones and cavities).

SSR technology has wider application in search and rescue. For example, locating buried objects or people is within the capabilities of existing technologies. Worthy of future investigation is the speculative possibility of detecting living persons (buried or hidden) by using a modified SSR to 'listen' for heartbeats or respiratory function. This could be applied to earthquake rescue or for locating hidden fugitives.

2.1.5 Forensic Techniques for Materials

The fundamental principle underpinning all forensic investigation is that 'every contact leaves a trace'. The challenge for forensic scientists is to locate, identify, compare and interpret trace materials in the context of an investigation and in court proceedings. Trace materials can be particles of soil, fibres, hairs, explosives, glass, paint, plastics and other particulates. Their study is often called criminalistics and can involve the application of biological, chemical and physical technologies. Often these trace materials are the *only* physical evidence in a case linking suspects to a victim and/or a scene, and visa versa.

Australia has a high quality capability but limited capacity in forensic criminalistics. For some trace material there is a critical shortage both of capability and capacity. The Australian Federal Police (AFP), and others, have begun to address these shortfalls through strategic partnerships and initiatives with academic institutions. In particular, an emerging research effort has been established with the University of Technology, Sydney with a number of successful grant applications and postgraduate research students. This work is aimed at developing better techniques for the analysis of trace materials. Most importantly, it is also aimed at providing information to help interpret its meaning and hence value for both investigations and court use.

Criminals are well aware of the potential to leave behind fingerprints and DNA and of the power of these techniques to uniquely identify. There is already evidence of criminals taking measures to avoid detection. Forensic science urgently needs to develop strategic linkages such as those between the AFP and UTS to enhance its capability and capacity to deal with other forms of trace evidence, as these may be the only evidence for many crimes. Failure to do so will result in ineffective investigations and offenders not being successfully prosecuted.

2.2 Biological Sciences, Biotechnology & Biometrics

2.2.1 DNA Analysis

Forensic biology involves the application of criminalistics in cases where biological materials may be present. Developments since the mid 1980's in nucleic DNA analysis have provided a very powerful tool to forensic biologists and for the justice system. In Australia, managers of forensic laboratories, with the help of the National Institute of Forensic Science (NIFS), have introduced a uniform analytical platform using Perkin-Elmer Applied Biosystems *Profiler Plus*. This is an essential foundation for the development of a national DNA database, which will enable the exchange of DNA data throughout Australia.

The DNA database being developed through CrimTrac will come on line progressively through 2001. It is expected to revolutionise the way in which crime is investigated and a large increase in case submissions is anticipated. In NSW for example, authorities now hold more than 15,000 samples of DNA related to all types of crime, helping to identify suspects. State laboratories are responsible for purchasing and validating DNA profiling technology. AFP and ANU are currently working on developing DNA testing for plant samples using Cannabis as a test species. The private forensic services sector can also be expected to seek an active role.

It is essential that there are no significant backlogs in the analysis of biological samples for case analysis and for DNA database purposes. In a recent case in Canada involving a serial rapist, samples were not analysed for some months during which the rapist committed a number of further rapes and abducted and murdered two teenage girls.

Although forensic laboratories are gearing up to meet the anticipated increases in sample submissions the potential for analytical backlogs remains and a range of solutions are required. In the mid to long term this is likely to involve developing more powerful field testing devices based on application of nano-technology in the biomedical field. In turn, this will open up the possibility of conducting database searches of samples tested in the field, providing police with intelligence and investigative leads in real time. The focus in the laboratory will be on more complex and difficult samples requiring more sophisticated handling and analysis.

In addition to nucleic DNA humans have a second form of DNA called mitochondrial DNA (MDNA). In some samples there is insufficient nucleic DNA for analysis by current methods. Sample types such as human hairs are suitable for MDNA testing. Several laboratories including the AFP, are working towards the introduction of MDNA testing.

Recently the AFP completed a \$6M upgrade of its forensic facilities and equipment through funding provided by Federal Government's reform program for the AFP. But further private or public investments must soon be made for the next generation of DNA analysis facilities, to cope with the expected demand.

In general, although Australia can 'match it' with the best in the world in regard to facilities and standards, there are weaknesses. These include a lack of capacity (although all jurisdictions and laboratories are attempting to address this issue) and a lack of research on DNA, and more broadly, biotechnology, for forensic applications. The expertise of the Australian Genome Research Facility at the University of Queensland should be explored.

Desirable 'next steps' must include acquisition, possibly from the UK, of mitochondrial DNA techniques for early implementation in some Australian forensic laboratories. AFP could have a purpose-designed laboratory in its new forensic facilities in the ACT. Then, some DNA testing could move to the field, with the potential for real time identification of suspects. Further development of non-human DNA testing for forensic applications should also be implemented.

This paper was prepared by an independent working group for PMSEIC. It's views are those of the working group, not necessarily those of the Commonwealth.

Impediments to achieving these improvements include the need for successful transfer of nano technology from biomedical fields to forensic application and funding for applied research to develop forensic applications.

With improved coordination and strategic linkages for planning future scientific and technological needs, there may be a medium term opportunity for Australian technologists, instrumentation and biotechnology firms to supply equipment and systems for large-scale analysis of DNA samples. Existing Government programs could facilitate the development and diffusion of appropriate technologies and infrastructure for this purpose.

2.2.2 Biometrics

In addition to fingerprints and DNA, there are other means of authentication based on an individual's unique physical characteristics, which may now be measured with unprecedented precision using digital technology.

Examples include, voice patterns, retinal images (iris scanning), facial or hand geometry, and even the identification of a person's subcutaneous vein structures. For example, each human eye has about 260 discriminators, and hand geometry analysis is based on about 90 variables. Some of these technologies require the knowledge and cooperation of the subject, while others can be applied passively and unobtrusively.

Biometrics can provide the missing link between 'credentials' such as credit cards, smart cards, access cards and PIN numbers and their authorised users. They can also be used to identify unknown individuals. DNA analysis, fingerprint and iris scanning are the most accurate biometrics, but are too intrusive for many applications and are not applicable for surveillance.

One company, *Fingerscan*, has supplied fingerprint identification systems to *Woolworths*. Two Canberra hospitals are conducting trials of systems that enable doctors to gain access to patient records by having their fingerprints scanned electronically.

The latest keyboards and 'mice' may contain in-built biometric access devices such as a fingerprint scanner. Though such systems achieve much higher levels of security than those relying upon passwords, they are expensive. As is the case with most applications of digital technology, the cost of biometric authentication devices may be expected to decrease over time.

Digital authentication technologies do, however, raise potential problems in terms of privacy and confidentiality of the stored personal data. Biometric data may be vulnerable to theft and misuse. Moreover, the systems may be subject to error. If the prescribed margin between the stored and the current measurement is too wide, imposters may obtain access. If it is too narrow, legitimate users may be rejected. System failure can also occur.

Despite these vulnerabilities, it appears that fraud control will largely become an electronically focused activity. This will entail a combination of biometric authentication and automatic anomaly detection. Australia's current use of biometric technologies appears largely derivative.

BIOLOGICAL SCIENCES

DNA ANALYSIS

Now

CrimTrac will use standardised DNA analysis machines and Profiler Plus kits from the US firm Perkin Elmer Applied Biosystems.

New

A new generation of DNA micro-chip arrays may permit real-time data collection and matching with DNA databases.

Next Step?

Incorporate Australian biological expertise into developing a Profiler kit that best suits Australian conditions while providing adequate overlap with international DNA data bases.

2.3 Information & Mathematical Sciences

Australian IT firms are working with research and law enforcement agencies as well as commercial clients, to supply operational technologies for 'proof of identity', 'real time intelligence' and security systems. Highlights, described below, include: facial imaging; data mining; mobile data systems and encryption. International links underpin the development and commercialisation strategies of local research-industry partnerships in a couple of these examples.

2.3.1 Financial Intelligence - tracking 'dirty money'

Financial intelligence is a relatively new tool in the investigator's armoury. It is a tool of great versatility being able to identify and trace money trails in a wide range of criminal investigations, and to provide an understanding as to the way in which criminals use the financial system either to fund their criminal activities or to disguise and remove their proceeds of crime.

Like most intelligence sources, to be of most use financial intelligence must be timely and easily accessible. The use of IT is vital in ensuring that these characteristics are present.

Thanks to Australia's *Financial Transaction Reports Act 1988* and the innovative work of the Australian Transaction Reports and Analysis Centre (AUSTRAC), our country is well respected in the international money-laundering control community. AUSTRAC's expertise in data collection, analysis and dissemination is used as a model by countries in our region and listened to in major international fora in combating organised crime's management of the proceeds of fraud, illicit drugs and contraband.

To the credit of the local IT sector, most of the computing power of AUSTRAC's money tracking is home grown. Its current systems, developed in-house by contracted software experts cope well with 30,000 reports per day, received from 700 financial institutions and others, loaded within 4-5 hours, analysed and 'warehoused' for follow-up action if indicated.

Whilst there are off the shelf products available which can be used in analytical processes, such as name matching software, for the most part, the applications must be custom made. Australia is a world leader in the production and use of information technology for financial intelligence purposes because of the way in which AUSTRAC integrates collection, analysis and dissemination applications.

AUSTRAC analyses its data holdings of some 50 million reports through profiling, rules based systems and data mining techniques. Some 26 Federal, State and Territory agencies have access to and use AUSTRAC analysis information within hours of transactions being reported. Around 700 officers from these agencies have on-line access eg. some 35 in the NSW Police, with 1,250 authorised users in total, making up to 0.5 million searches on the data each year.

INFORMATION SCIENCES

AUSTRAC

Now

Near 'real time' monitoring of reports allows AUSTRAC and its user agencies to 'watch the money come and go', within hours of a suspect transaction, leading to quicker identification of suspects.

New

Looking to move to full electronic delivery service. Related system enhancements would cost \$2 million.

Next Steps?

1. Improve the number of reports covering different types of 'value transfers';
2. Reassess 'choke points' for transaction data, ie. where criminals may be able to bypass financial institutions which have Australian reporting obligations;
3. Provide capability to follow e-commerce value movements to same extent as traditional value movements; and
4. This requires further applications development, eg. automatic reporting and validation of 'signatories'.

All data transfers are encrypted and access to the database is logged and permanently recorded. The Commonwealth's *Secure Gateway Entry* project is an important frame work for maintaining security, along with ongoing enhancements in AUSTRAC's own systems.

AUSTRAC costs about \$10 million per year, but the savings to tax revenue alone, achieved by identification of avoidance activities, is many times this annual cost. The ATO estimated that in the last financial year, AUSTRAC's efforts were principally responsible for the identification and collection of over \$47 million in revenue. This is in addition to further indirect assistance from AUSTRAC intelligence applied in the ATO's activities on international tax haven work, price transfers, cash economy, debt collection, strategic planning and risk management. This contribution facilitates the collection of hundreds of millions of dollars of tax payments.

AUSTRAC has also been instrumental in the successful conclusion of many major law enforcement cases and has been the originator of a significant number of them. But the legislation supporting this work and AUSTRAC systems are ageing. A recent internal report identified a number of vulnerable areas, which can result in certain types of transactions being 'invisible' to law enforcement and revenue authorities, eg. criminals may move value in new ways which are not reportable to AUSTRAC.

Assessments are urgently needed of new IT that can help meet these challenges, including matching the changing computer systems of the major financial institutions that report to AUSTRAC. Questions include: what roles can computer artificial neural networks (ANN) or artificial intelligence (AI) play? How much extra system functionality would allow Tax File Numbers, Australian Business Numbers or other identification indicators to be incorporated in profiling analyses? New techniques with greater analytical powers and precision in data mining and other tools, would allow financial intelligence analysis to constantly improve to keep up with the inventiveness of money launderers and tax evaders.

As in many areas of law enforcement, the resources available for financial intelligence R&D (both in IT and criminal methodologies) are scarce and only available spasmodically. Current funding is regarded as barely sufficient for 'maintenance and core activity' but not enough to keep up with growing IT costs or to pro-actively develop the 'next steps', needed soon.

Australia can be said to have one of the most sophisticated anti-money laundering systems in the world. This is through a combination of world's best practice financial intelligence, collaborative investigative techniques and a comprehensive legislative framework. Enhancements to existing legislation are needed to ensure the reporting of new kinds of transactions and ways in which value is moved between jurisdictions. Some overseas experience is instructive in this aspect. New analytical techniques could identify increasingly complex money laundering and tax evasion activity. Meaningful improvements to current capability are essential to sustaining the detection, investigation and prosecution of crimes and tax evasion.

Funding from the National Illicit Drugs Strategy (NIDS) is enabling AUSTRAC to place more of its staff into partner agencies to assist with improving their intensity of analysis of AUSTRAC data. This is an important example of innovation: investments in human capital achieving greater productivity from the use of existing infrastructure and data inputs.

Another challenge for AUSTRAC, as for other law enforcement agencies, is to retain expert staff to direct and manage external contractors in the development of new systems. AUSTRAC's contractors and analytical experts are motivated by the technical and intellectual challenges of building leading-edge systems. If strategic planning and assessment to maintain this edge is under resourced, there is a risk that corporate expertise will leave, due to lack of new professional opportunities.

2.3.2 Artificial intelligence to combat inappropriate behaviour, non-compliance and fraud

Health: Leakage on the Medicare and PBS schemes through both Medifraud and inappropriate medical practice is estimated to lie between 0.7% and 1.6% per year of total health expenditure (ANAO, 1996). One of the pattern analysis technologies developed by the Health Insurance Commission (HIC) to distinguish inappropriate from appropriate medical practice are artificial neural networks (ANNs). These are leading edge computerised systems which simulate the way the brain is believed to function. ANNs have been developed and deployed by the HIC since 1993 to assess the likelihood of inappropriate practice by medical practitioners. They are currently being used to develop a system for detecting Medifraud by the public, medical practitioners and pharmacists.

As the HIC moves toward electronic claiming, the challenge is to develop systems capable of analysing all transactions as they occur to avoid the 'quick hits' that can result in significant losses. The huge volume of transactions involved, and the requirement to pay genuine claims promptly, demand intelligent systems that can deal quickly with large volumes of data. The HIC, in collaboration with HNC Software Inc in San Diego, USA, is developing risk assessment systems that can assess electronic claims in real-time (under ¼ second). If this type of system is deployed in the future, it may be used in conjunction with existing ANN systems to accrue information over time about repeated suspicious claims coming from particular sources.

Financial institutions: Fraud losses through electronic credit card transactions are estimated to be in the order of tens, if not hundreds of millions of dollars each year in Australia. The major Australian financial institutions are following the lead of their North American counterparts and installing proprietary neural network systems developed in North America to detect credit card fraud by both card-holders and merchants soon after its occurrence. Nonlinear statistical models, such as decision trees and neural networks, are being developed in-house to risk-rate the likelihood of fraud on applications for personal and housing loans.

The financial institutions are particularly keen to curb the growth in identity fraud. They seek collaboration with government to develop a national electronic system capable of verifying in real-time the authenticity of state-issued documentation, such as driver's licences that are used to prove a person's identity when opening an account or applying for a loan.

Compliance agencies: The Australian Taxation Office has been working with CSIRO and the Advanced Computational Systems CRC (ACSys) to develop AI techniques to assist their focus on taxpayers who are likely to be non-compliant. These new techniques provide insight into the characteristics of taxpayer behaviour and provide the means for more sophisticated evidence-based initiatives to improve overall taxpayer compliance. CSIRO/ACSys researchers are keen to deploy their very fast and scalable solutions to the large historical data held by other agencies in the search for 'unusual or suspicious behaviour'. The former ACSys partners are very keen to develop joint research and deployment projects, whereby local knowledge in fraud detection could be combined with local state-of-the-art computer science. Without the next step, of jointly developing a research agenda, Australia will soon buy future technology of this kind from the US and Europe. This would be a lost opportunity to profit from local knowledge.

Australian Customs is working with CSIRO to design AI systems that will improve their ability to identify incoming and outgoing cargo that represents the greatest risk. Customs has also deployed an Australian-developed intelligence system, InterQuest (see section 3.1), to link its separate information repositories into a single, unified intelligence tool. The Australian Bureau of Criminal Intelligence is using the same intelligence software to capture information about the behavioural patterns of repeat serial crimes. The system, which is operated by all Commonwealth and State police, has resulted in the prosecution of numerous serial sex offenders.

This paper was prepared by an independent working group for PMSEIC. It's views are those of the working group, not necessarily those of the Commonwealth.

2.3.3. *Securing Electronic Commerce*

Australia has some solid achievements in preparing for electronic commerce and the 'information society'. For example, on the OECD's Science & Technology Indicators Scoreboard¹⁰, in 1997, Australia was second only to the US in the number of secure (encrypted) websites for e-commerce per head of population.

The majority of Australians shopping 'online', pay online. In the 12 months to November 1999, 594,220 adult net shoppers (74% of all adult net shoppers) paid for their Internet purchases online, while 237,830 (83%) did so in the corresponding period a year earlier.¹¹ Australians appear to be less concerned about security issues than their American counterparts who in a 1999 Internet Shopping Study by Ernst and Young, identified a fear of giving credit card information over the Internet as the primary barrier to net shopping.

However, anecdotal evidence suggests there is no room for complacency. Some purchases of overseas IT security systems by large Australian organisations seem to indicate a lack of faith in locally available security technology and service.

Just as secure e-mail relies on digital signatures to verify the sender, computer applications also need to be sure of the identity of their users. Usually, asking users to log-on via their user identity and a password does this. Techniques, such as 'challenge-response' and single-use passwords, support secure logons over potentially insecure connections. They use encryption to stop eavesdroppers discovering the password, and randomise parts of the process to stop replay attacks.

Highly secure encryption technology is readily available and could also be used by criminals to communicate securely. Law enforcement agencies could intercept these messages in transit but would be unlikely to decrypt them without access to the keys. This may not be a major problem in practice, as the end points are vulnerable to attack. Users of secure encryption must constantly maintain security. Messages and documents may be secure in transit but they have to be kept equally secure on the computers at each end as well. A seized computer may well have decrypted copies of secure documents and the encryption keys also have to be kept somewhere as well.

Australia is well placed, through its IT sector, including research expertise, to be a leading-edge user of encryption technologies provided by several major overseas suppliers. In addition, some pioneering work by CSIRO Mathematical & Information Sciences may lead within 12 months to new 3-way digital verification technologies for e-commerce. This would present a significant business opportunity if an Australian company could be set up to commercialise the technology.

INFORMATION SCIENCES

E-COMMERCE SECURITY

Sensitive data is often sent over secure encrypted connections, normally using Secure Socket Layer (SSL) technology. SSL uses asymmetric encryption to send a symmetric 'secret' session encryption key from the client to the server. SSL, and its successors such as TLS, are commonly used for transferring data such as credit card details.

US company RSA, is a major vendor of Public Key Infrastructure (PKI) and SSL technology. RSA have a development centre in Brisbane, partially to avoid US export curbs on encryption technology. The US government regards such technology as 'munitions', that could be used to prevent US security agencies from intercepting communications, but is relaxing some controls on its export of this technology.

¹⁰ OECD STI Scoreboard 1999 - Benchmarking knowledge based economies

¹¹ *The Current State of Play: Australia and the Information Economy*, National Office for the Information Economy: http://www.noie.gov.au/projects/information_economy/ecommerce_analysis/ie_stats/state_of_play.htm

2.3.4. Facial Imaging

INFORMATION SCIENCES

FACIAL IMAGING

Now

Vision Control International sells a series of related facial image processing software to major private and government clients in over 20 countries, eg. FACEwin for face identikits, FACEalbumn for image databasing.

Banque-Tec, a smart card company specialising in building access control have a START grant to complete the incorporation of CSIRO face recognition technology into their product and conduct trials in Australia, the UK and USA.

New

CSIRO's 'Face in a Crowd' uses low cost PC-based technology and video camera for image capture at up to 25 frames per second. Images are analysed in terms of motion, colour and shape, with accuracy of face matching up to 95%.

Vision Control International are incorporating CSIRO face recognition technology in their core products, allowing a database search for near-matches to sample photographs or composite images.

Next Step ?

Integrating Australian facial imaging technologies with *CrimTrac*, which requires ongoing attention to system inter-operability across all jurisdictions.

As discussed previously, the most accurate biometrics such as finger prints and DNA analysis are a powerful tool, but too intrusive for many applications and not applicable for surveillance. Face recognition is widely applicable (cameras are increasingly used), and most people accept the use of a photograph to identify them.

Verification applications for face recognition include access control, bank teller machines, point of sale for smart card transactions and at computer terminals to control access to sensitive data or to verify the operator's identity in high value transactions.

Identification applications include database searching and surveillance at airports, casinos, sporting venues and prisons. Other proposed applications are the identification of welfare cheats and illegal immigrants, who may present under multiple identities. Some of these applications raise questions of privacy that need to be dealt with openly and frankly.

New technologies being developed by CSIRO *Telecommunications & Industrial Physics* involve imaging, image compression, image transmission, face recognition and video tracking and have a variety of security access applications. Current research on facial recognition began with work undertaken in the *CRC for Robust and Adaptive Systems*.

CSIRO has licensed such technologies to two Australian SMEs (*Banque-Tec* and *Vision Control International*) and this is also under consideration by a number of others. A demonstration at the Hanover Fair in March 2000 was highly successful. The newer CSIRO technology still under development is the 'Face in a Crowd' image capture system, capable of rapidly matching a face captured on video to an image stored either on a portable credential, such as a smart card, or a database.

Government programs can encourage the development of this promising technology, eg. funding under the START program to CSIRO's commercial partners, to help speed their product development and marketing. State, Territory or Commonwealth law enforcement agencies could partner with CSIRO and one or more commercial partners to undertake trials and demonstrations in specific applications.

2.3.5 Networks for criminal intelligence analysis

The Australian Bureau of Criminal Intelligence (ABCI) was established in 1981 as a Commonwealth, State and Territory initiative to facilitate and coordinate the sharing of law enforcement information and criminal intelligence throughout Australia. To achieve its purpose the ABCI has been active in technological development in the areas of information management, intelligence analysis and knowledge based systems. It developed, in-house, the Australian Criminal Intelligence Database (ACID), a relational database provided by, and available to, all police jurisdictions and the Australian law enforcement community.

With such features as electronic data up-load from a multiplicity of systems and single screen search facility, ACID is a most advanced and user friendly system. The ABCI is regularly visited by overseas law enforcement officials who are impressed with this example of advanced technological development in the Australian law enforcement arena. In 2000 alone, presentations have been given to the US Drug Enforcement Administration, US Director of Central Intelligence Crime and Narcotics Center, Hong Kong Police, Indonesian Police, representatives of the People's Republic of China and the Royal Canadian Mounted Police.

The ABCI also uses technology through the Violent Crime Linkage Analysis System (ViCLAS) to compare the idiosyncrasies, behavioural traits and modus operandi of serial criminals across Australia, to reduce the incidence of offenders able to commit seemingly unconnected crimes in different States. ABCI has complemented its databases by developing the Australian Law Enforcement Intelligence Net (ALEIN) to provide a highly protected communications network for rapid and secure transfer of information between State police networks throughout Australia.

CHAPTER THREE

FRAME WORKS FOR PARTNERSHIP

A common theme underlying the Australian technologies featured in this paper, is the ad hoc manner in which technologies are identified, assessed, developed and applied by the law enforcement community, with the danger that they will remain undiscovered and lost. There are indeed success stories in the press of private firms or researchers (particularly in the IT sector) claiming new and effective products and services for enhancing or securing business and government technology-based systems.

Yet there is no comprehensive system to ensure that Australia develops, or can acquire the cost effective mix of new technologies and expertise needed to keep ahead of drug pushers and fraudsters. We have no measure of the extent to which Australia is dependent on purchasing such tools and systems from overseas or the potential loss to our economy of not commercialising home grown technologies that could do the job as well or better.

In this section the Working Group briefly describes some relevant linkages and models, elements of which could be adapted in developing options for such a comprehensive system.

3.1 Linkages

CrimTrac

While there are still issues to be resolved, implementation of CrimTrac is already promoting strategic alliances between jurisdictions and a business plan approach to planning and integrating technological requirements. While States are largely responsible for purchase and validation of the 'sharp end' of CrimTrac, eg. DNA profiling and electronic fingerprint scanning facilities, the Commonwealth is funding the overarching systems and IT framework to link the databases which enable police information and criminal intelligence to be shared and analysed rapidly.

Once the core CrimTrac system is established, there should be a greater opportunity for Australian researchers and firms commercialising new technologies with forensic or other law enforcement applications to tender for the additional components that may be progressively added to extend CrimTrac's capabilities. With the first state DNA laboratories to come on line early 2001, other public and private sector organisations are already providing expertise to complement the core capability, eg. AFP and ANU are jointly developing DNA testing for plant samples using Cannabis as a test species.

While some of the core and subsidiary technology of large new systems such as CrimTrac may be most cost-effectively supplied by specialised overseas corporations, Australia's strategic planning capability should be improved to identify those components where technology based on specific local knowledge may best meet the need. For example, it should be determined whether some elements of the standard 10-piece DNA analysis kits developed for use overseas will be equally effective in capturing the different genetic profiles of certain Australian communities.

Government Support for Research

Government programs for R&D have been accessed on occasion to assist in forming links between university researchers, law enforcement agencies and industry. For example, the AFP and the University of Technology, Sydney, have an active joint research program and have been awarded grants under the Australian Research Council's SPIRT¹², RIEF¹³ and other schemes.

¹² Strategic Partnerships with Industry - Research and Training (SPIRT) program

¹³ Research Infrastructure Equipment and Facilities (RIEF) program

UTS itself contributed over \$1 million to establish its forensic labs. AFP is also a partner with the Australian National University in a SPIRT grant and the University of Western Australia has a SPIRT grant for forensic entomology.

Whilst a number of forensic organisations have active and developing arrangements and collaborations with academia, the scale is still small. Generally, it is hard for universities to get the Australian Research Council's large grants for applied work for law enforcement clients because the funding is primarily directed to conceptual studies in science, while forensic science builds on these discoveries rather than being responsible for their evolution. The end result is that forensic science has to compete against all other science in a selection process which does not generally involve scientists with forensic background.

Education and Training

Forensic science is popular with university undergraduates, as shown by the list of available courses at Appendix 2. However, it is also necessary to regularly upgrade the skills of the specialists in agencies, who are typically so overwhelmed by routine demands on their expertise, that little or no time is available for keeping abreast of the latest developments.

Partnerships for Commercialisation

Canberra IT company *The Distillery P/L* provides an example of successful commercialisation with its product InterQuest. ASIO purchased InterQuest for development as in-house intelligence system. Once deployed successfully by ASIO, other agencies have been willing to adopt the InterQuest solution.

Since InterQuest has gained local acceptance, marketing to overseas law enforcement agencies in South Africa, India and Canada is proving more straightforward. Where individual law enforcement agencies have taken the lead with a particular technology, and found the best solution, they should encourage deployment to other agencies.

One of the reasons for InterQuest's success is that many of *The Distillery's* employees are ex-IT applications developers from law enforcement agencies. They came to understand why certain systems failed, and what the precise business needs of agencies were.

The Criminology Research Council

Comprising a representative of the Commonwealth and of each State and the Northern Territory, the Council was established under the Criminology Research Act (1971). It controls and administers the Criminology Research Fund, comprising Federal and State Government contributions from which grants are made to researchers for criminological research projects.

In the 27 years to 1999 that the Council has been in operation it has made grants from the Fund for 271 separate research projects totalling approximately \$4.3 million. Research projects funded by the Council have been conducted in all Australian jurisdictions and have focused on a broad spectrum of issues related to crime and criminal justice, including a few technical projects such as NetMAP and forensic technologies.

Links with Defence Science & Technology

Funding for R&D in Australia's defence agencies is much greater than that for law enforcement, but some of this may be transferable to the law enforcement community. Discussions should be held to explore strategies for transferring and adapting applicable technologies, which could represent a multiplication of the benefit from the public investment. For example, defence planners in other countries are investing substantially in information warfare - disrupting the IT

infrastructure of defence systems¹⁴. Could counter measures for e-commerce be accessed?

¹⁴ See Institute for the Advanced Study of Information Warfare: <http://www.pyscom.net/iwar.1.html>

3.2 Australian models of cooperation and coordination

Technological planning by the law enforcement community must first be informed by knowledge of what community and Government's priorities are. It is difficult for any one agency, no matter how well funded or expert, to be able to provide adequate advice on the full range of technologies that may be applicable for all forms of crime.

National Institute of Forensic Science

The National Institute of Forensic Science (NIFS) was established as a National Common Police Service, under an Agreement signed by the Australasian Police Ministers' Council in 1991. NIFS commenced operations in February 1992.

NIFS acts to promote forensic science and collaboration between the key practitioners in forensic science, comprising the functions of: collection (scene investigation); examination (scientific/medical); and presentation (advocates/courts). Key activities include training and R&D programs, information exchange and quality management. One of NIFS aims is to give legal practitioners a greater insight into the principles and practices of the collection and examination phases of the forensic case and forensic practitioners a better knowledge and understanding of the principles of evidence and of court procedures. The general public from whom juries are drawn must also be given a balanced view of the strengths and limitations of forensic science.

Cooperative Research Centres

Governments have recognised the difficulties in bringing academia and industry into productive collaborations, eg. through the Cooperative Research Centres (CRC) program and SPIRT. A number of existing CRCs have been cited in this paper as developing technologies applicable to crime prevention and law enforcement. One approach may be for the law enforcement community to make a coordinated approach to several existing CRCs to discuss potential applications of their technologies across a broad range of fields. An expression of interest has been lodged in the current round of CRC applications, for a new CRC for Forensic Sciences. The proposal is indicative of a potential emerging forensic industry.

Industry Networks

Under the Commonwealth's Technology Diffusion Program (TDP), a range of manufacturing and service industries have been assisted to form national networks or international research alliances that facilitate access to the best available technologies for meeting sectoral and company-specific objectives. An example is the Collaborative Health Informatics Network¹⁵ (CHIC), a national, independent, not-for-profit organisation whose focus is to facilitate improvements in business processes and patient care in the health sector through the application of appropriate information technology.

Both the health care and IT&T industries expressed the need for such an independent, national body and TDP assisted the formation of CHIC with \$2.4 million in seed funding over three years. CHIC acts as a matchmaker between the health and IT & Telecommunications industries by facilitating collaboration to bring about better health outcomes through the use of IT. One of CHIC's services is the Health IT Information Service (HITS), a highly specialised subscription-based service which acts as a clearinghouse for the collection, storage and dissemination of information about the health informatics industry. CHIC services help the industry players to make better informed business decisions about the acquisition and application of technology.

¹⁵ See CHIC website: www.chic.org.au

3.3 Overseas models of coordination

The Working Group has noted the efforts made in overseas criminal justice jurisdictions to facilitate access by the law enforcement community to science, engineering and technology (SET) and to coordinate strategic planning and assessment of technological options. Two examples are summarised below, but Australia would do well to develop its own model based on relevant features of these and other examples.

USA: National Institute of Justice's Office of Science & Technology (NIJ / OST)

The National Institute of Justice (NIJ) is the research agency of the US Department of Justice. NIJ supports research, evaluation, and demonstration programs, development of technology, and both national and international information dissemination. NIJ has an Office of Science & Technology (NIJ / OST), which is significantly funded and tasked to:

- Provide state and local law enforcement and corrections agencies access to the best technologies available and help them develop capabilities essential to the improvement of efficiency and effectiveness in every aspect of the criminal justice system; and
- Support the development of new technologies to support national needs served by Federal law enforcement and corrections agencies, while avoiding unnecessary and expensive overlap and duplication.

For example, as a conduit for federal funding, NIJ/OST has been a strong supporter of new technologies and tools in the area of DNA testing. Previously funded and on-going projects in this area can be viewed on the website: www.ojp.usdoj.gov/nij. The NIJ/OST is overseen by a Council, which is responsible for ascertaining the real needs of its client groups, which extend through all States down to municipal police authorities.

While NIJ/OST has a budget of some US\$120 million, it is important to recognise that it is not the only, nor primary agency serving these needs in the US. Other federal agencies such as the Federal Bureau of Investigation and state counterparts also support their own science and technology services. There is a fair degree of cooperation between such agencies, eg. the NIJ/OST has an MOU with the US Department of Defence. The plurality of the system, akin in some respect to Australia's, means that overlap and competition can and does occur.

UK

Within the Policing and Crime Reduction Group of the UK Home Office is a more centralised model of planning and provision for agencies' needs for technology. With a staff of around 130, the Group's Police Science Development Branch (PSDB) provides technical advice to the Police Policy Directorate, the police and Ministers. It also works to improve the operational effectiveness and efficiency of the police service (and other customers) and to support the Home Secretary's responsibilities for counter-terrorism. Also in the same Group, the Police Science and Technology Unit (PSTU) is responsible for developing the Home Secretary's policies on the provision of information technology, communications, scientific and technical support to the police service and on the maintenance and disclosure of criminal record information and the regulation of the private security industry. It also sponsors and evaluates research development on policing for the police service and the Home Office.

A complementary capability to these two units is provided by UK Forensic Science Service, an agency of the Home Office separate from the policing services in England and Wales. The forensic services have grown from 600 to nearly 2,000 staff in the last several years.

3.4 Conclusions

Finding 1 The law enforcement community and science

While law enforcement agency personnel value the advantages of technology, they have, perhaps justifiably tended to regard it as something limited to the specialist laboratory and unsuited to daily field work. The Working Group believes that when technology providers and law enforcement users can understand and better meet each other's needs, investments in technology in economic gains will follow and society expectations can be fulfilled.

There is a need to change the dominant culture in law enforcement agencies, which views scientists and 'techos' as a curious, if albeit frequently necessary, adjunct to the main game of crime fighting.

Recommendation 1

Improve law enforcement capacity to fully engage with the scientific community.

A more wholehearted engagement with the science community must be actively promoted, from the top, and possibly aided by the mechanisms recommended below. This engagement in turn, should inform strategic planning by law enforcement agencies that is conducive to the growth and exports of Australian firms that can supply agency requirements (see Recommendation 3).

Finding 2 Planning, coordination and technology advice

Strategic and scenario planning for crime prevention and law enforcement technology needs should be occurring more systematically across, rather than within agencies. There are a variety of committees and a peak body for law enforcement agencies, such the Heads of Commonwealth Operational and Law Enforcement Agencies (HOCOLEA) and subject matter working groups, but these tend to have operational or short to medium term considerations, or can support or encourage but not substantially undertake or fund the planning activities.

The Working Group's view is that there is considerable room for improvement in coordination across State/Federal jurisdictions of technical advice and procurement, leading to enhanced identification, assessment, development or acquisition of local or imported technologies.

Recommendation 2

Appoint a high level S&T policy group, underpinned by a science and technology clearing house.

There is an urgent need for a mechanism to receive and consider timely and detailed expert advice on, as well as cooperation in:

- ⇒ Strategic planning to identify and foster solutions from science and technology for crime prevention, security and law enforcement needs.

This paper has identified a number of possible models that could be further explored.

There should be little delay, as urgent tasks include to: consider future policy needs and the technological requirements; avoid duplication in procurement efforts; achieve cost savings through larger contract sizes; achieve greater inter-operability of systems; and speed up the exchange and use of real-time intelligence by agencies.

The policy group and cooperative mechanism to be developed as recommended above, should be able to call on expert technical advice and specific research from a new center or network for diffusion of crime prevention and law enforcement technologies. Such a center or network should have the capability to become the preferred and prime source of advice for:

1. identifying existing or emerging Australian or overseas technologies and systems that may potentially offer a cost effective solution for a given purpose;
2. assessing in detail, the extent to which those technologies or systems can, cost-effectively deliver what is required; and
3. assist in the transfer and/or dissemination of such technologies and systems once they have been selected for adoption by one or more jurisdictions.

A ‘technology assessment network’ (or centre) for crime prevention and law enforcement, as suggested under Recommendation 2, should also be able to offer its services to the private sector, subject to competition policy principles (depending on the extent to which the ‘network’ is funded by the public sector). There are a number of existing funding and organisational models which could be explored to develop such a network, eg. from the Cooperative Research Centres program, or from the Technology Diffusion Program (Networks element).

Finding 3 Stimulating opportunities for Australian industry

Forensic science develops from fundamental science. There is currently no mechanism for transferring information from basic science so that forensic science applications can proceed. A forensic industry will not be large globally, but may be significant for a small country, such as Australia. We could create in Australia, a desirable and clean niche industry.

A mechanism and source of funds needs to be provided to ensure that there is cross fertilisation between forensic science, and user groups with potential applications. As an emerging industry, forensic business would need to rapidly respond to new discoveries globally in fundamental science. This should be underpinned by a clear business plan (predicated on investment funds) to create a forensic industry, which could grow to support itself.

In regard to procurement actions, there seems to have been a tendency for law enforcement agencies to individually buy ‘off the shelf’ technologies from the most convincing ‘salesman’ on the day. While the procurement might be effective at one level, a more integrated and strategic approach could expect to deliver further efficiencies and stimulate the growth of those agencies’ Australian research, development and business partners.

Recommendation 3

Identify mechanisms to encourage Australian industry and research agencies to participate in the development and production of new, affordable technologies for law enforcement

PMSEIC Working Group on Science & Crime Fighting

(Chair)

Professor Sue Serjeantson (PMSEIC member)
President, Federation of Australian Scientific & Technological Societies

Ms Sandra Ellims Assistant Secretary, Law Enforcement Coordination Division
Attorney-General's Department

Dr Peter Grabosky Director of Research
Australian Institute of Criminology

Dr Simon Hawkins Program Manager, Data Mining
Advanced Computational Systems CRC
CSIRO Division of Mathematical and Information Sciences

Mr Andrew Kirk Principal Adviser
Office of the Minister for Justice & Customs

Ms Elizabeth Montano Director
Australian Transaction Reports & Analysis Centre (AUSTRAC)

Dr James Robertson Director, Forensic Services
Australian Federal Police

Professor Michael Wilson Head, Dept. of Chemistry, Materials & Forensic Science
University of Technology, Sydney (**representing Professor Ian Chubb, AV-CC**)

Additional inputs from the following organisations are gratefully acknowledged:

Advanced Computational Systems CRC
Australian Customs
Australian Government Analytical Laboratories / Australian Forensic Drug Laboratory
CRC for Satellite Systems
CrimTrac Project Office
CSIRO Mathematical and Information Sciences
CSIRO Telecommunications & Industrial Physics
National Institute of Forensic Science
New South Wales Police Service
Vision Control International Ltd
The Distillery Pty Ltd - business systems consultancy

Secretariat support to the Working Group was provided by the Attorney-General's Department and the standing PMSEIC secretariat within the Department of Industry, Science & Resources.

This paper was prepared by an independent working group for PMSEIC. It's views are those of the working group, not necessarily those of the Commonwealth.

Forensic Science Courses Available In Australia

CANBERRA INSTITUTE OF TECHNOLOGY, ACT

Degree programs:

Bachelor of Applied Science (Forensic Investigation).

Diploma programs:

Diploma of Forensic Investigation (Crime Scene Investigation);

Diploma of Forensic Investigation (Fingerprint Identification);

Diploma of Applied Science with a forensic stream.

Short courses:

Introduction to Forensic and Crime Scene Investigation;

Forensic Photography;

Fire Investigation.

GRIFFITH UNIVERSITY, QLD

Graduate Diploma in Forensic Science;

Master of Science in Forensic Science; and

Master of Science in Forensic Science with Honours.

QUEENSLAND UNIVERSITY OF TECHNOLOGY, QLD

Evidence and Investigation for Forensic Scientists.

LA TROBE UNIVERSITY, VIC

Postgraduate Diploma in Forensic Science.

MONASH UNIVERSITY, VIC

Graduate Diploma in Forensic Medicine.

SWINBURNE UNIVERSITY, VIC

Certificate for Forensic Science;

Diploma in Forensic Science.

DEAKIN UNIVERSITY, VIC

Bachelor of Forensic Science;

THE FLINDERS UNIVERSITY OF SOUTH AUSTRALIA, SA

Bachelor of Technology Degree in Forensic and Analytical Chemistry.

Graduate Diploma in Forensic Science (DNA Technology)

THE UNIVERSITY OF WESTERN AUSTRALIA, WA

Graduate Diploma in Forensic Science;
Master of Forensic Science.

UNIVERSITY OF TECHNOLOGY SYDNEY, NSW

Bachelor of Science (Honours) in Applied Chemistry - Forensic Science;
Master of Science (Physical Sciences); and
PhD (Physical Sciences).

Compiled by:

Professor Mick Wilson

(with the National Institute of Forensic Science Education group)

Head, Department of Chemistry Materials and Forensic Science

Faculty of Science

University of Technology, Sydney

Ph 61 2 9514 1787

Fax 61 2 9514 1628

mobile 0409 913590

<http://www.science.uts.edu.au/depts/cmfc/Staff/people/MickWilson.html>

Products & Services For Crime Prevention

Scientific Instruments & Supplies

Scientific Suppliers Association of Australia (SSAA):
<http://www.ssaa.asn.au/>

The Scientific Suppliers Association of Australia Inc (SSAA) is Australia's leading industry association representing the interests of approximately 100 suppliers, manufacturers, distributors, importers and exporters of scientific products. SSAA members have a combined domestic turnover approximating \$700 million. Their export revenues assist Australia's balance of payments to the extent of in excess of \$250 million per annum, with this figure estimated to be growing at more than 10% per year. In conjunction with others, SSAA has taken leading policy positions involved in crime prevention, most notably the Code of Conduct to Protect Against the Diversion of Chemicals into the Illicit Production of Drugs.

Biotechnology and Forensic Science

The Australian Biotechnology Association Ltd (ABA):
 Tel: (03) 9596 8879; Fax: (03) 9596 8874; E-mail : admin@aba.asn.au
 Website: <http://www.aba.asn.au>

The ABA has over 600 members, including: 40 Corporate Company Members and over 40 student members. Since 1986 ABA has published newsletters, a journal, educational leaflets, directories of biotechnology organisations, and a website. ABA members can provide support to the law enforcement community in the development of pattern recognition systems, the provision of advanced instrumentation such as GC-MS and FTIR for chemical analysis and the adaptation of commercially useful DNA markers for forensic use.

With regard to DNA markers for example, experience in vine identification might be useful in designing methods to identify cannabis cultivars. Systems designed to identify disease markers in humans may be adapted to the identification of individuals from food and biological matter collected from crime scenes. ABA members include experts in molecular biology and could develop and provide this technology and support, including the security of exhibits, validation of methodologies, proficiency testing of analyses and the ability to provide court evidence.

The Australian Biotechnology Directory: **<http://biotech.isr.gov.au/index.html>**

The Directory provides a comprehensive listing of Australian biotechnology companies, research institutions and service providers which will be updated regularly. It will help Australian and international companies and researchers to identify the particular skills, products and potential partners for biotechnology business and collaboration.

Security of Information Technologies and Telecommunications

Australian Information Technology & Telecommunications Security Forum
(of the Australian Electrical and Electronic Manufacturers Association)
<http://ittsecurity.aeema.asn.au/index.htm>

With over 100 member companies, Australia's IT&T Security Forum members specialise in:

This paper was prepared by an independent working group for PMSEIC. It's views are those of the working group, not necessarily those of the Commonwealth.

- Designing, developing and delivering advanced security systems and services that are effective, affordable, fully integrated with information and communication systems, and designed to grow with them;
- Fully satisfying the most exacting international quality and performance criteria;
- Collaborating with other industry members to create complete security packages customised for IT&T systems;
- Ensuring that information is protected so that it satisfies security and privacy requirements;
- Helping you manage interfaces with the Internet, Intranets and electronic funds transfer technology in a way that reduces risk exposure;
- Authenticating and validating data, and the people who provide and access it;
- The evaluation and certification of Trusted Systems;
- Preventing external (and internal) computer crime, espionage, privacy breaches, and the denial of service caused by sabotage and browsing;

The Australian Computer Emergency Response Team (AusCERT)

<http://www.auscert.org.au/>

This Queensland-based team tackles computer security emergencies in the Australian and New Zealand Internet domains. AusCERT's aims to reduce the probability of successful attack, to reduce the direct costs of security to organisations and lower the risk of consequential damage.

National Electronic Authentication Council

<http://www.noie.gov.au/projects/consult/neac/index.htm>

The National Electronic Authentication Council (NEAC) has been established by the Commonwealth Government to enhance business and consumer confidence in e-commerce through overseeing the development of a national framework for electronic authentication of online communications. In particular, NEAC will provide a national focal point on authentication matters, encourage interoperability between different systems and the development of relevant technical standards and provide information and advice to industry, government and consumers.

General Security Products & Services

Australian Security Industry Association Ltd (ASIAL)

Tel: (02) 9906 4780 Email: security@asial.com.au **<http://www.asial.com.au/index.html>**

ASIAL, formed 30 years ago, in 1969, comprises in excess of 3000 members and is the only **national** association servicing the private (non government) security sector. It is a self-regulatory body with a mandatory Code of Practice and fosters the highest standards of efficiency, service, equipment and ethical behaviour amongst persons, firms and corporations engaged in the Australian Security Industry.

ASIAL promotes strong links with government, especially police and other security arms of government. The Association collaborates with relevant authorities to develop Standards and mutual policies which facilitate and improve levels of safety and security within Australia.

The Association publishes *Insider*, the leading security magazine, and *CrimeWatch*, the official publication for Crime Stoppers Australia. In addition, it organises the premier security industry exhibition and showcase annually.

The National Crime Authority (NCA)

The NCA was established in 1984 in response to concerns about increasing organised criminal activity in Australia. The NCA has jurisdiction to investigate against Commonwealth, State and Territory laws—including offences perpetrated across state and territory borders. The NCA's main function is to investigate 'relevant criminal activity' involving two or more offenders, substantial planning and organisation, and the use of sophisticated methods and techniques. The most commonly investigated offences include drug importation, cultivation, manufacture and trafficking, money laundering, theft, fraud, tax evasion, bribery, extortion and violence. The NCA works in partnership with other law enforcement agencies.

ENCRYPTION ISSUES

Cryptography on the Internet is a complex issue for law enforcement. On the one hand it is required in order to protect e-commerce and other legitimate Internet activity from cybercrime, but on the other it is a problem when criminals use it to encrypt communication and information relevant to their criminal activity. There are two major issues for law enforcement agencies arising from their use of encryption software:

- Interception of their communications.
- Evidence collection from seized computers.

The NCA has observed an increase in the use of the Internet as a communications device used by organised criminal networks. Further, the NCA is concerned about the increasing availability of encryption technology on mobile phones and other devices capable of Internet connection.

SWORDFISH FUNDING FOR E-COMMERCE/CYBERCRIME INITIATIVES

In the recent Federal Budget (2000-01), the NCA received an additional \$23.3 million to investigate money laundering and fraud against the Commonwealth. Of this total, \$3.3 million has been earmarked to develop some new strategies to deal with e-commerce and emerging technologies. This is in response to the fact that over the next four years the face of money laundering and revenue fraud will change dramatically:

- Proceeds of crime are being transferred overseas more rapidly; there is an increasing absence of traditional physical evidence; individual transactions are likely to become more difficult to trace amongst the multitude of complex legitimate transactions; and there may be an increased potential for fraud from remote locations.
- The expansion of new technologies and electronic commerce, globalisation of economies and reform of taxation systems have created significant opportunities for opportunistic organised crime.

The evolving skills and technologies need to be fostered to provide a computer forensics capability, including decryption capabilities, to keep pace with the developments in technology and communications.

Case Study from the Commonwealth's National Illicit Drugs Strategy (NIDS)

The *Australian Forensic Drug Laboratory* (ADFL) is a functional unit within the Australian Government Analytical Laboratories' (AGAL) facility located at Pymble NSW. ADFL's forensic science-based activities underpin the Government's tough on drugs and tough on sports drugs initiatives, including heroin and amphetamine-type stimulants signatures.

In particular, the **National Heroin Signature Program** (NHSP), a joint initiative by the Australian Federal Police (AFP) and AGAL/AFDL, is developing and refining advanced trace chemical 'fingerprinting' techniques and associated databases.

Once fully developed the database should enable cross-matching of individual drug seizures. NHSP is funded for three years through the National Illicit Drug Strategy (NIDS) announced by the Prime Minister in October 1997 and started in July 1998. ADFL's expertise in heroin profiling is internationally recognised, as evidenced by the recent hosting in Sydney of the United Nations International Drug Control workshop on this topic.

NHSP is a drug intelligence gathering and dissemination program, **the result of 6 years research** in drugs profiling at AGAL. Another offspring of that research is profiling of seized drugs for prosecution purposes. A number of law enforcement agencies (AFP, NCA, NSW Police, ACT police, NT police etc.) use ADFL's profiling service. The technique has been used successfully in Australia in more than 30 court cases to convict suspected drug traffickers, members of significant drug importation syndicates.

In order to extract all potential benefits of the NHSP, it is necessary to secure funding for the program beyond June 2001, when the current three year funding expires.

A profiling program is also needed for **amphetamines**, but current funding is insufficient to stretch to develop an adequate capability. ADFL has developed the basis of a potential supplementary program for profiling Amphetamine Type Stimulants (ATS).

Having in mind increased illicit supply of amphetamine, meth-amphetamine and ecstasy, it would be beneficial to establish and fund a **national** ATS signature program (NATSSP).

Following the visit of a Swedish expert in October 1999, who described a positive experience with such a program in Europe, a number of law enforcement agencies (NCA, AFP, NSW Police, NSW Crime Commission etc) expressed interest and support for the concept of NATSSP.

In cooperation with AGAL's Australian Sports Drug Testing Laboratory, ADFL has also developed methodology to identify and analyse all of the compounds (performance enhancing drugs) that are banned by the International Olympic Committee (IOC).

This capability has enabled AGAL/AFDL to positively respond to highly controversial *Australian Customs* seizures of such banned drugs during international competitions hosted by Australia. ADFL provides advice to *Australian Customs* on performance enhancing substances and their precursor chemicals. Publicising this capability could serve as a deterrent to smuggling of various performance enhancing substances.