ORGANISED CRIME IN AUSTRALIA 2013

ACC
AUSTRALIAN CRIME COMMISSION

10 YEARS
2003–2013

Correspondence should be addressed to:
Chief Executive Officer
Australian Crime Commission
PO Box 1936 Canberra City
ACT 2601

Telephone:
02 6243 6666 (from within Australia)
61 2 6243 6666 (international)

Facsimile:
02 6243 6687 (from within Australia)
61 2 6243 6687 (international)

Published July 2013

ISSN 2202-3925

CONTENTS

INTRODUCTION

THE CONTEMPORARY FACE OF ORGANISED CRIME

In the two years since the publication of the last Organised Crime in Australia assessment, organised crime has become more pervasive, more powerful and more complex. Such is the risk posed by organised crime that governments around the world, including the Australian Government, have recognised for some time that organised crime has implications for national security. Australia's National Security Strategy, released in January 2013, lists serious and organised crime as one of the seven key national security risks.

Globalisation has been embraced and exploited by organised crime, which capitalises on the way in which globalisation has greatly facilitated international communication, cross-border links, commerce and trade. Although organised crime now seems to have no borders or geographical constraints, combating organised crime and illicit trade has remained in many ways constrained by jurisdictional, legislative and state borders – a fact that is not lost on sophisticated criminals.

The rapid development of technology, and the increasing availability of that technology to users throughout the world, have significantly increased the dynamics, profile and reach of organised crime. The Internet enables global virtual networking and social interaction between criminals, and has enabled the establishment of 'virtual marketplaces' for illegal and illicit goods such as drugs, firearms, identification documents and child exploitation material.

Although traditional purchases through face-to-face contact will continue to be a key form of illicit transactions for the foreseeable future, these virtual marketplaces have created alternative sources of supply, bringing access to illicit goods to the keyboard of Internet subscribers all over the world, and have meant that those dealing or trafficking in illicit goods can be based in any geographical location and still connect directly with customers in any number of international jurisdictions. In this way, the Internet has cut out the traditional

physical 'middle man' or intermediary in these transactions, who has been replaced by a 'virtual intermediary'. For example, users of illicit drugs no longer necessarily have to seek out dealers in person; instead, they can order the drugs of their choice on the Internet, expecting to have their purchase delivered to their door.

This new avenue of drug supply has the potential to grow exponentially, and brings with it new challenges for law enforcement in disrupting the supply of illicit goods.

The combination of globalisation and rapid technological development has had a profound effect on the new and emerging drug markets (the drug analogues and other novel substances markets) and on sophisticated organised fraud. The Internet is the key driver of the new and emerging drug markets, enabling entrepreneurial individuals, rather than traditional organised crime groups, to become significant players within these markets. Organised fraud can now target victims around the world from any location, with the delivery of scams via the Internet or via voice-over-Internet protocols, meaning that those behind these schemes can easily and cheaply reach increasingly large pools of possible victims.

The emergence of entrepreneurial individuals in some key illicit markets is challenging the traditional paradigms of organised crime dominance or control. With serious harms now being wrought by actors outside the traditional organised crime structures, these individuals can, in some instances, be as worthy targets for law enforcement attention as organised crime groups.

Importantly, while the Internet has brought buyers and sellers of illicit commodities together, it has also made it possible for organised crime to introduce itself into the homes or lives of all Australian Internet users. Organised criminals increasingly exploit the online environment to perpetrate crimes such as stealing sensitive personal identification information exchanged over the Internet to commit frauds or identity crime, or delivering mass marketed fraudulent schemes such as advance fee fraud and fake investments to unsuspecting victims.

Organised crime is big business, with profits from transnational organised crime for 2009 estimated in a 2011 report to have been around US$870 billion – an amount equal to 1.5 per cent of global GDP at that time.[1] This figure has almost certainly grown since then. Those engaged in organised crime energetically, aggressively and innovatively compete for their share of illicit markets, are profit driven, and employ increasingly complex network structures and ways of concealing their activities and their identities – increasingly with the help of professional advisers and facilitators.

Organised crime as it affects Australia is inextricably linked to international organised crime. Serious and organised criminals operating in Australia necessarily have international links to facilitate their activities – particularly the movement of illicit goods into Australia – and overseas-based organised criminals actively target Australia. This means that strong and trusted partnerships with overseas law enforcement agencies are now more fundamental to combating organised crime than they have ever been.

1 United Nations Office on Drugs and Crime 2011, *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*, UNODC, Vienna.

THE IMPACT OF ORGANISED CRIME IN AUSTRALIA

Organised crime is now a part of the everyday lives of Australians in ways that are unprecedented. The Australian Crime Commission (ACC) conservatively estimates organised crime to currently cost Australia A$15 billion annually.

Once, encounters with organised crime were largely restricted to those who sought out illicit commodities or illegal activities. Today, any Australian on any day can be affected by organised crime. Some of the more obvious examples of this are:

- the increasing incidence of Australian investors being defrauded in investment scams – sometimes referred by complicit or compromised 'legitimate' brokers – and being targeted for sophisticated 'boiler-room' frauds run by offshore organised crime groups
- theft of credit card and bank account data through online attacks, or by means of skimming machines installed on ATMs or point-of-sale devices
- the discovery of dangerous and volatile clandestine laboratories used to produce drugs in suburban areas, requiring the temporary evacuation of residents in surrounding houses or streets
- violence between organised crime groups that takes place in public.

There are also less obvious impacts of organised crime on Australians. ACC research and investigations have identified the following as examples of some of the more subtle ways in which organised crime can have an impact on Australia:

- increased public expenditure to support health services to treat illness related to illicit drugs – including the increasing number of users who need long-term medical support
- small businesses struggling to remain competitive with businesses used as vehicles to launder money for organised crime, for whom 'profitability' is not an issue
- a distorted share market, in which organised crime has manipulated share prices and asset values for criminal gain.

Organised crime not only has a direct impact on individuals, but also affects our communities, our economy, our government and our way of life. As stated in Australia's National Security Strategy:

> ***Serious and organised crime can undermine our border integrity and security. It can erode confidence in institutions and law enforcement agencies, and damage our economic prosperity and regional stability.***

Organised criminals who may once have been involved in traditional illicit markets, such as drugs, are now expanding their interests – often across a range of illicit activities or sectors – in order to maximise their profits. Although most organised crime activities in Australia are focused on illicit drug markets, organised crime is increasingly diversifying its activities, with convergences being observed between legitimate or licit markets and illicit markets.

Of concern is the diversification of organised crime into legitimate business to conceal its illicit activities. In Australia, criminal entities buy legitimate businesses (cash businesses in particular) to launder money, and use complex business structures to conceal the real ownership or control of diverse business interests. Internationally, powerful organised crime groups have strategically purchased businesses in particular sectors in order to achieve a market share large enough for them to be able to manipulate the prices of certain goods or services. Organised crime has targeted big business that is central to economies in order to infiltrate these businesses with the aim of using their economic power as leverage against governments. Corruption and coercion can then follow. Though this level of organised criminal infiltration of business is not apparent in Australia, these international examples serve to highlight the risk posed by organised criminal involvement in legitimate business sectors.

The infiltration of legitimate business by organised crime can be particularly insidious when that infiltration is used to pursue anti-competitive practices. Internationally, perhaps the most publicised example of this is the involvement of Russian organised crime in big business in critical sectors within Russia and the other countries of the former Soviet Union. This involvement allows criminal monopolies to develop, squeezes legitimate business out of key sectors, and gives significant political influence to organised crime figures as a result of their control of businesses that are fundamental to the economy.

New types of crimes are also having an impact on Australia, such as the phenomenon of 'hacktivism' – compromising computer systems or networks to make a moral or political point. Online politically motivated or issue-motivated groups such as 'Anonymous' have demonstrated both intent and capability to successfully attack the online services of governments, private industry and personal users around the world. These attacks cause financial and reputational damage to their targets, maximise inconvenience and damage, and expose individuals to the risk of fraud.

The anonymity offered by cyber-based criminal methodologies can also mask the underlying motivations for attacks on individuals, organisations and governments. In this respect, it is often difficult to distinguish cybercriminals from 'State-based' actors. Alleged State-based cyber activity around the world between 2008 and 2011 reportedly targeted everything from nuclear reactors and International Monetary Fund (IMF) data holdings to defence contractors and the Google and Hotmail email accounts of individuals.[2]

2 Offensive cyber activity conducted as part of state-on-state conflict or competition represents a criminal offence, potentially resulting in significant damage to the economy and critical national infrastructure. However, state-on-state cyber conflict is not considered to be part of the organised crime environment and is covered in assessments promulgated by the Commonwealth's Cyber Security Operations Centre (CSOC).

The diversity and complexity of the organised criminal environment necessitate agile and adaptable approaches to combating threats and risks, with law enforcement required to develop new skills and capabilities to be effective. The scope and nature of contemporary organised crime mean that, domestically, the relationships between law enforcement, national security, government, regulatory and compliance agencies, private industry and community groups will be more important than they have ever been in identifying and dealing with threats. Internationally, Australia's diplomatic and law enforcement partnerships will be fundamental to containing organised crime.

THE NEXUS BETWEEN ORGANISED CRIME, NATIONAL SECURITY AND THE ECONOMY

In the same way that organised crime is now recognised as a global threat, there is a general acceptance of the threat that organised crime poses to national security. National security incorporates, but is not limited to, concepts of sovereignty, border integrity, political and economic strength, strong institutions of State, the safety and wellbeing of citizens, and the strength and depth of relationships and alliances with other nations.

Economic strength and stability are fundamental contributors to national security. In July 2011, United States President Barack Obama signed an Executive Order and released a strategy to combat transnational organised crime, in recognition of the threat that transnational organised crime now poses to the security of the United States and the international community. The strategy noted that organised crime threatens United States economic interests and can damage the world financial system through the subversion of legitimate markets. This follows the United Nations Security Council, in 2010, noting concerns about the serious threat posed by drug trafficking and transnational organised crime to international security.[3]

In Australia, the National Security Strategy, released in January 2013,[4] listed serious and organised crime as one of the seven key national security risks, and noted that contemporary criminal syndicates 'have the capacity to inflict serious harm on our economy, businesses and institutions'. The syndicates impacting on Australia are not just those based in Australia, but also those located offshore who are targeting Australia for criminal gain.

There is evidence that organised crime groups, including highly professional international organised fraud networks, are targeting the Australian securities and investment sector. The Trio Capital superannuation and investment fraud case[5] in 2011 is an example of the sophisticated methodologies that these organised fraud networks employ.

Fraud or other criminal behaviour that affects the securities and share market in Australia, or in any other country, can have very significant consequences. Behaviour within the market, or having an effect on the market, that undermines investor confidence in its integrity can result in investors – overseas investors in particular – ceasing to invest in Australian shares and securities, with obvious implications for the economy.

3 United Nations Security Council Presidential Statement S/PRST/2010/4, United Nations, Geneva.

4 Department of the Prime Minister and Cabinet 2013, *Strong and secure: a strategy for Australia's national security*, public launch, Canberra, 23 January 2013.

5 A full account of the case can be found in the report of the Parliamentary Joint Committee on Corporations and Financial Services Inquiry into the collapse of Trio Capital, May 2012, <https://fraud.govspace.gov.au/files/2011/03/Inquiry-into-the-collapse-of-Trio-Capital.pdf>.

HOW THE GLOBAL FINANCIAL CRISIS IMPACTED ON ORGANISED CRIME IN AUSTRALIA

The global financial crisis had a particular impact on organised crime overseas, which was quick to identify and capitalise on the business opportunities that the crisis afforded. Internationally, organised crime is reputed to have variously provided sufficient liquid investment capital derived from drug profits to save some banks from collapse, to have stepped in to provide financing (albeit at extortionate rates) to new and struggling businesses across a range of sectors when banks tightened their lending criteria, to have bought or taken over failing companies for well below market value – gaining interests in sectors crucial to economies – and to have amassed substantial real estate at bargain prices. In Italy, it has been claimed that the Mafia is now 'Italy's number one bank', with €65 billion in liquidity and with an estimated 200,000 businesses tied to extortionate lenders, giving the Mafia a 'stranglehold' on the economy.[6]

The financial crisis, dating from 2008, has given transnational organised crime groups the opportunity to use their existing illicit funds to buy power and influence – economic influence, in particular – and to transfer significant sums of money into the legitimate economy, thereby effectively laundering it. In an article published in 2012, Moisés Naím[7] outlined some other ways in which organised crime has benefited from the global economic crisis:

> ***Fiscal austerity is forcing governments everywhere to cut the budget of law enforcement agencies ... Large numbers of unemployed experts in finance, accounting, information technology, law and logistics have boosted the supply of world-class talent available to criminal cartels. Meanwhile, philanthropists all over the world have curtailed their giving, creating funding shortfalls in the arts, education, health care and other areas, which criminals are too happy to fill in exchange for political access, social legitimacy and popular support. International criminals could hardly ask for a more favourable business environment.****
>
> * Naím, M 2012, 'Mafia states', accessed 18 March 2012, available at <http://www.moisesnaim.com/es/node/949>.

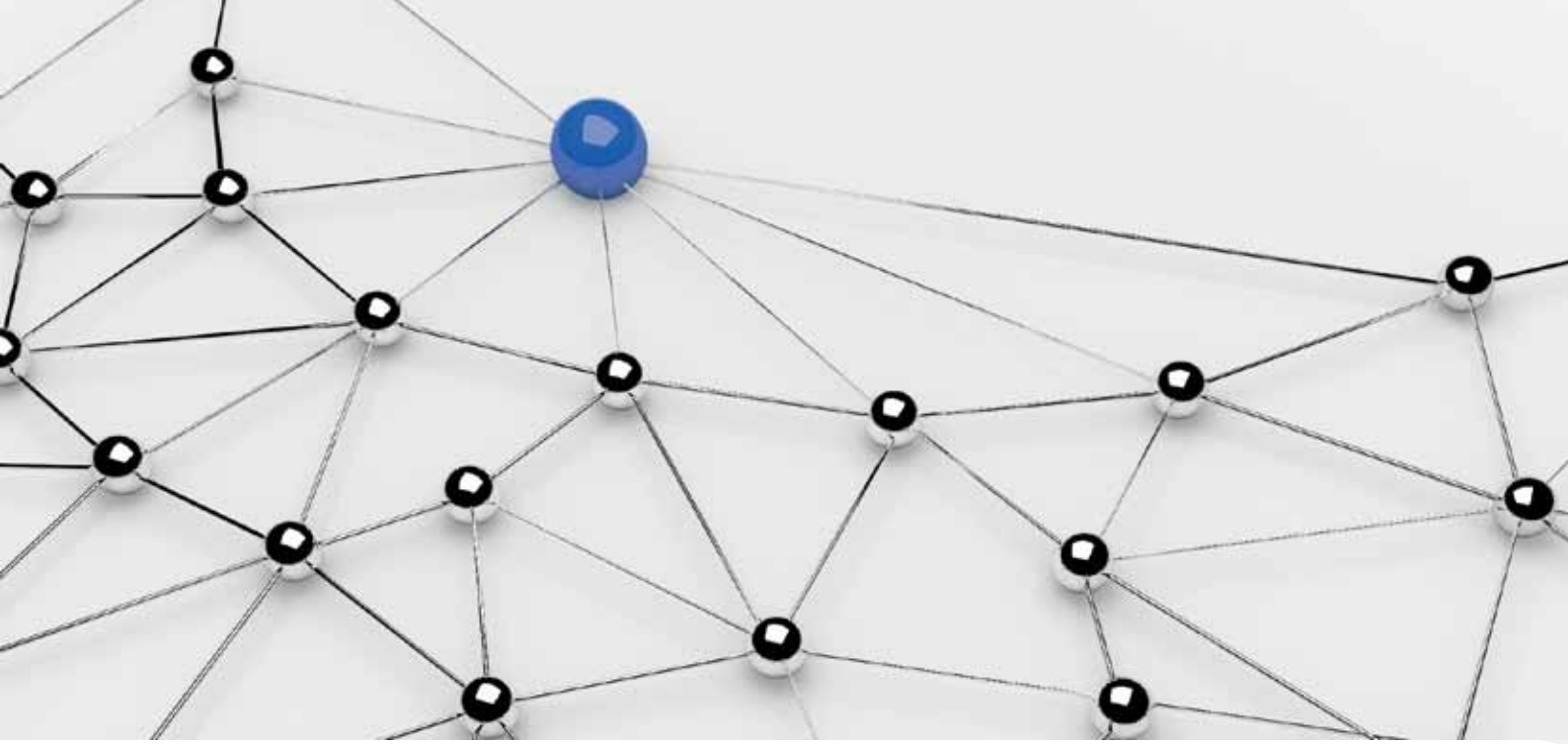
In relation to the impact of the global financial crisis on organised crime in Australia, the relative strength of the Australian economy is likely to be attractive to organised criminals seeking to place their assets in an environment that is perceived as stable and safe. This may mean that organised crime will be seeking to deposit laundered funds into Australian banks, to invest in Australian business or the Australian stock market, or to put money into tangible assets such as real estate.

6 From a report by Italian anti-crime group SOS Impresa, titled 'Mafia Spa is the first bank in Italy' (not available in full English translation), quoted by Mackenzie, J 2012, 'Mafia now "Italy's No.1 bank" as crisis bites: report', *Reuters*, 10 January.

7 Moisés Naím is an academic, journalist, author and commentator on international politics and economics.

The high prices paid for illicit drugs by Australian drug users will continue to make Australia an attractive target for organised crime groups involved in international drug trafficking. Not only will their product be sold at higher wholesale prices than almost anywhere else in the world, but the profits from the sale of the drugs, earned in Australian dollars (which remain strong in international financial markets), will have a high value when moved offshore. The potential for significant profits is likely to motivate international organised crime groups to pursue aggressive tactics in order to capture a part of the lucrative Australian market, including bribing, corrupting or coercing public officers holding positions that enable them to facilitate criminal activities.

As discussed later in this report, the relative strength of the Australian economy, and the comparatively affluent population, have also made Australia an attractive target for organised crime groups involved in fraud. With a compulsory superannuation regime, and superannuation assets in Australia currently estimated at A$1.3 trillion, highly sophisticated offshore organised fraud networks have established, and will continue to establish, complex fraudulent schemes to steal superannuation savings. Individual Australians are being targeted for mass marketed fraud, including 'boiler-room' or cold-call investment fraud, and Ponzi schemes, with organised crime also seeking to exploit and manipulate the legitimate securities and share market for criminal gain. These financial crimes are emerging as an important threat, and have the potential to do significant harm to the Australian economy and the Australian community.



UNDERSTANDING ORGANISED CRIME THROUGH RISK AND THREAT ASSESSMENTS

MARKET-BASED RISK ASSESSMENT

Illicit markets operate in the same way as markets for legitimate commodities – the primary motivator is financial gain or profit, with the markets governed by demand, supply, price and the perceived quality of the goods or services.

Consequently, the ACC uses a market-based risk assessment approach to evaluating illicit markets that conforms to international risk assessment standards.[8] This approach informs a comprehensive picture of serious and organised crime, the unique activities that enable organised criminal activity, and the impact of each of the illicit markets on Australia. The ACC's risk assessment methodology derives a level of risk by combining an assessment of the threat posed by each specific illicit market with an assessment of the 'harms' wrought by that market on the Australian community. Expressed as an equation, the risk methodology is:

Threat (assessment of market dynamics) x Harm = Risk

8 International Standard AS/NZS/ISO 31000:2009.

THREAT AND HARM ASSESSMENT

The harm – the negative consequences arising from an illicit market – is assessed from a political and social perspective. The threat – the likelihood of those consequences – is assessed by considering market dynamics and the activities of market participants, taking into account the nature and effectiveness of existing controls (such as legislation or regulation) that impact on the market.

This market-based risk assessment underpins the ACC's Organised Crime Threat Assessment (OCTA). The assessment provides contextualised information about the impact of serious and organised crime on the Australian community, market dynamics, vulnerabilities, and areas that would benefit from further intelligence or risk analysis.

This report is an unclassified version of the Organised Crime Threat Assessment that was delivered in June 2012 to the ACC's Board and the ACC's partner law enforcement agencies.

The report outlines trends in the international environment, serious and organised crime[9] activities in Australia, and the resulting harms to the Australian community. It examines factors that affect supply and demand, the risks posed by a range of crime markets, and the way in which enabler activities facilitate organised crime.

The overall risk to Australia from organised crime is assessed as high.[10] Relevant factors are:

- demand for and supply of the illicit commodity
- the nature and extent of the market
- barriers to entry and the level of competition in the market
- general characteristics of significant individuals or groups in the market
- the rationale for and context of the market in relation to other illicit markets and the legitimate economy
- the impact of the existing regulatory framework and controls on the market, and
- the impact of the market on the community generally.

As an unclassified document, this report cannot provide the same level of detail as the classified version. It can, however, give a clear picture of the scope and nature of the activities that make up the organised crime environment in Australia. The report is not intended to cause undue concern about organised crime, but rather to inform Australians about organised crime so that all elements of the Australian community – government, law enforcement, public and private sector agencies, academic institutions, business sectors and the public – can increase their awareness of the problems and risks, and work together to combat the threat.

9 The *Australian Crime Commission Act 2002* (Cwlth) defines 'serious and organised crime' as an offence that involves two or more offenders, substantial planning and organisation and the use of sophisticated methods and techniques, which is committed in conjunction with other serious offences punishable by imprisonment for a period of three years or more. A broad range of serious offences are listed in the legislation, including theft, fraud, tax evasion, money laundering, illegal drug dealing, extortion, bribery or corruption of an officer of the Commonwealth, an officer of a state or an officer of a territory, perverting the course of justice, bankruptcy and company violations, and cybercrime.

10 This assessment is based on the collective risk posed by the illicit markets that affect Australia. The level of risk has not been assessed relative to other national security risks. Risk is assessed on a six-point scale, with the risk levels being very low, low, medium, high, very high and critical.

ENABLER ACTIVITIES

The ACC's Organised Crime Threat Assessment 2012 identified six distinct illicit activities as being 'key enablers'. Those activities are:

- money laundering
- cyber and technology-enabled crime
- identity crime
- exploitation of business structures
- corruption
- violence.

These activities are classified as 'enablers' as they each have unique roles in enabling or facilitating organised crime, but are not an end in themselves – that is, money laundering would not be necessary if the crime from which illicit profit had been made had not been committed, necessitating concealment of the proceeds of that crime. Similarly, the theft of identity documents would pose little threat if those documents were not intended to be used to commit offences.

Activities such as money laundering, identity crime, corruption and violence contribute to the effectiveness of other types of organised crime. Although not all of the enablers are present in every illicit market, enablers can work in unison, with any one organised crime group (OCG) using several enablers at once. Corruption can be used to facilitate, or to hide, the use of other enablers.

Importantly, enablers are also unique in that any impacts of law enforcement, regulatory, legislative or policy activity that are felt within the enabling activities – such as the closing of loopholes in financial reporting systems to prevent money laundering, or regulatory changes in relation to the requirements for registering businesses – have the potential to resonate through all of the illicit markets in which those enabling activities are present. For example, should law enforcement capability to identify, trace and prosecute cyber and technology-enabled crime be enhanced, all of those markets that rely on technology to perpetrate crime would be affected.

MONEY LAUNDERING

INTRODUCTION

Organised crime groups rely on money laundering as a way of legitimising or hiding proceeds or instruments of crime. Money laundering is a pervasive, corrupting process that can blend criminal and legitimate activities. It stretches across areas as diverse as mainstream banking, international funds transfers and foreign exchange services, gambling, shares and stocks, artwork, jewellery and real estate.

THE CURRENT SITUATION

Financial profit is a main driver for organised crime groups. Legitimising the proceeds of crime and the instruments of crime (the means by which crime is committed) is crucial for organised crime groups and this activity poses an ongoing risk to the Australian community. Money laundering involves criminals attempting to hide or disguise the true origin and ownership of the instruments of crime and the proceeds of crime so that they can avoid prosecution, conviction and confiscation of criminal funds. Money laundering offences are defined in Part 10.2 of the Criminal Code Act 1995 (Cwlth). The offences encompass a very wide range of criminal activity.

Money laundering is an extremely diverse activity. It is carried out in Australia at all levels of sophistication by most, if not all, organised crime groups, increasingly with the assistance of professional advisers, and using a constantly evolving variety of techniques. Although the banking system and money transfer and alternative remittance services are major channels for money laundering, organised crime groups consistently seek out new channels for money laundering.[11]

There is no single method of laundering money. Money launderers have shown themselves to be imaginative, creating new schemes to get around the counter-measures designed to identify and stop them. Some examples of strategies that criminals might use to launder money are:

- breaking up large amounts of cash and depositing the smaller sums in different bank accounts, or buying money orders or cheques and depositing them in other accounts, in an effort to place money in the financial system without arousing suspicion

11 Australian Transaction Reports and Analysis Centre (AUSTRAC) 2011, *Money laundering in Australia*, AUSTRAC, Sydney.

- moving money around to create complex money trails, making it difficult to identify its original source – usually through a series of quick transactions, or through businesses in other countries
- using funds 'legitimised' through introduction into the formal financial system to facilitate criminal activity or legitimate business, or to purchase high-value goods or real estate
- using a number of people to carry out small transactions or cash smuggling
- using online gambling platforms, placing illegal proceeds of crime into gaming machines or purchasing casino chips and cashing them out shortly afterwards
- trade-based money laundering – concealing the movement of funds within large volumes of legitimate financial transfers associated with international trade.[12]

The absence of an agreed methodology for estimating the value of money laundering, and gaps in information on the financial dimension of organised criminal activity, hamper efforts to calculate an accurate figure for money laundering in Australia.

Money laundering can harm the Australian community in many ways, including:

- 'crowding out' legitimate businesses in the marketplace when businesses that are fronts for money laundering subsidise products and services so that they can sell them at levels well below market rates
- affecting the reputation and integrity of financial institutions when, usually without knowing, they become involved with the proceeds of illegal activity
- distorting investment patterns
- assisting in the financing of international and domestic terrorism
- financing and providing motivation for further criminal activities.[13]

Three key factors influence the selection of particular money laundering methodologies: efficiency, capacity and cost. On the basis of these criteria, organised crime groups continue to widely use alternative remittance dealers. International funds transfers by some dealers can conceal their clients' illicit money flows among the high volumes of aggregated (mainly legitimate) daily transactions.

Some organised crime identities are suspected of being involved in the financing and construction of internationally based casinos and of using this opportunity to launder funds, as well as continuing to launder illicit funds on completion of the project. Many casinos and gaming facilities offer services similar to those of financial institutions, including accounts, foreign exchange, electronic funds transfers, cheque issuing and safety deposit boxes. These ancillary services, in addition to the variety of gambling services offered and the high cash turnover, make the gaming sector highly attractive and effective for money laundering.

12 ibid.
13 ibid.

In June 2011, the Combating the Financing of People Smuggling and Other Measures Bill was passed, amending the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, the *Financial Transactions Reports Act 1998* and the *Privacy Act 1988*. The amendments were made to reduce the risk of money transfers by remittance dealers being used to finance people smuggling and other organised crime ventures through the introduction of a more comprehensive anti-money laundering and counter-terrorism financing regulatory regime for the remittance sector.[14]

However, new money exchange platforms – in particular, virtual currencies – remain a challenge for law enforcement as they often fall outside the anti-money laundering and counter-terrorism financing regulatory framework. Bitcoin is an example of a digital currency that can be bought and sold anonymously online and does not rely on a central bank or financial institution to facilitate transactions. The unregulated environment and the anonymity of transactions make currencies such as Bitcoin attractive to organised crime for money laundering.

The ability of law enforcement to take illgotten gains from criminals is considered to be a powerful tool in preventing serious and organised criminal activity. Amendments to the Commonwealth *Proceeds of Crime Act 2002* came into force in February 2010. These provisions provide for the making of an unexplained wealth order if the court is satisfied that there is a reasonable suspicion that a person's total wealth exceeds the value of the wealth that they have lawfully acquired, and the person has either committed, or has wealth which was derived from, a relevant offence.

KEY CURRENT AND EMERGING ISSUES

- Although regulated sectors (such as banking, gaming and the alternative remittance sector) continue to be major avenues for money laundering activity, organised crime groups are also using less traceable methods, with new methodologies being constantly employed. This includes international trade, cash smuggling and virtual currencies, such as Bitcoin, which can be bought and sold anonymously.
- Organised crime groups are increasingly using professionals to identify and establish money laundering structures and methods, many of which capitalise on established global financial networks to move money rapidly around the world.
- Licit and illicit financial activity is becoming increasingly intermingled and difficult to differentiate.

14 Parliament of the Commonwealth of Australia 2011, Combating the Financing of People Smuggling and Other Measures Bill – explanatory memorandum, accessed 31 January 2013, <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:legislation/billhome/display.w3p;query=Id%3A%22legislation%2Fems%2Fr4509_ems_134783ce-d183-440c-9e21-082f9df5932a%22;rec=0#_ftn9>.

CYBER AND TECHNOLOGY-ENABLED CRIME

INTRODUCTION

The threat to Australia of cyber and major technology-enabled crime from international and domestic organised crime groups is significant. The use of computers and the Internet has become an integral part of daily life for most Australians, from online banking, shopping and social networking, to using email and browsing the web. Organised crime has identified and seized on the opportunity to exploit for criminal gain the growing use of the Internet by Australians.

Cyber and major technology-enabled crime has a major impact on the world economy, with a 2012 study estimating the global cost of cybercrime at US$110 billion annually.[15] The overall cost of cyber and major technology-enabled crime to the Australian economy is estimated to be US$1.7 billion[16] per year, with major cyber intrusions costing organisations an average of US$2 million per incident.[17]

THE CURRENT SITUATION

Cybercrime takes two forms: crimes where computers or other information communications technologies (ICTs) are an integral part of an offence (such as online fraud, identity theft and the distribution of child exploitation material), and crimes directed at computers or other ICTs (such as hacking or unauthorised access to data).

In relation to the use of the Internet and technology to facilitate traditional criminal activities and offences, Table 1 shows the migration of traditional crime to the online environment. Importantly, computing and information technology enables the commission of crime remotely and relatively anonymously – two characteristics that are particularly attractive to organised crime, as they make the identification and prosecution of the offenders more difficult. The global reach of technology also significantly increases the potential victim base. The principal identified threats to Australia emanate from offshore networks specialising in technology-facilitated traditional offences.

15 Norton 2012, Norton Cybercrime Report 2012, <http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/NCR-Country_Fact_Sheet-Australia.pdf >, viewed 30 May 2013.

16 ibid.

17 Pomenon Institute 2012, 2011 Cost of data breach study: Australia, <http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-australia-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_Australia>, viewed 30 May 2013.

TABLE 1: TRADITIONAL CRIME TYPES AND THEIR CYBERCRIME EQUIVALENTS

Traditional crime	Cybercrime equivalent
Fraud	Online fraud, mass marketed fraud
Child sex offences	Online child grooming, child exploitation material websites, storage and exchange of exploitation material on technical devices
Money laundering	Online money laundering via payment systems, e-cash
Identity crime	Online identity crime, 'phishing'
Extortion	Online extortion through ransomware, distributed denial of service attacks, hacking
Intellectual property crime	Online unauthorised access (hacking) and theft of information for financial advantage

Australia has a large and increasing number of Internet users, any of whom may become the victim of cybercrime. According to the Australian Bureau of Statistics (ABS), at the end of June 2012 there were over 12 million Internet subscribers in Australia (excluding Internet connections through mobile handsets)[18] – an increase of 4 per cent since the end of December 2011. In addition, the ABS reports that there were 16.2 million mobile handset Internet subscribers, an increase of 7 per cent from December 2011, and an increase of 22 per cent since June 2011. Although these mobile devices are just as vulnerable to attack as traditional computing devices such as laptop computers, users often do not give the security of these devices the same consideration, which may increase their vulnerability.

Attacks on Internet users aside, organised crime groups are also making use of 'darknets'. These are protected hidden networks of webpages, forums and auction sites, which often harbour trading in illicit commodities, including child exploitation material, illicit drugs and firearms, stolen credit card and identity data, and hacking techniques.

Attacks against computer services are becoming more sophisticated and common. Organised crime groups without strong technological skills are able to obtain ready-made malicious software packages ('malware') online, to help them commit a range of offences, or there are those who will provide packages to organised crime for a fee.

The malware available is also increasingly difficult to detect – often containing 'rootkit' features. A rootkit (also called 'stealthware') is computer code designed to hide from the operating system and security software of the target computer. Malware incorporating rootkits is more effective in avoiding detection by anti-virus software, allowing cybercriminals to gain unauthorised access to systems for longer periods of time. This can, among other things, provide unauthorised backdoor access to a computer to steal or falsify documents, steal credit card details or passwords, such as online banking passwords, install viruses, or direct the computer to send spam email.

18 Australian Bureau of Statistics 2012, *Internet activity Australia, June 2012*, cat. no. 8153.0, ABS, Canberra.

Organised crime may also use distributed denial of service (DDoS) attacks to attack business or government websites. DDoS attacks attempt to make the website unavailable to its intended users by flooding it with traffic. This causes the server to become overloaded with connections, so that new connections cannot be accepted.The Defence Signals Directorate (DSD) plays a vital role in Australia's cyber and information security. The DSD provides advice and assistance to federal and state authorities on matters relating to the security and integrity of information, on greater understanding of sophisticated cyber threats, and on coordination of and assistance with operational responses to cyber incidents of national importance across government and systems of national importance. As with home Internet users, adequate security practices are paramount to preventing cyber intrusions. At least 85 per cent of the intrusions that the DSD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the top four strategies listed in their *Strategies to mitigate targeted cyber intrusions*.[19]

In late 2012, there was an increase in reports of attacks in which users' computers were 'locked' until a fee was paid to have them 'unlocked'. This type of attack – named 'ransomware' or 'scareware' (see case study on page 20).

Recognising that cyberspace is a strategic asset for Australia, the Australian Government is establishing the Australian Cyber Security Centre to improve partnerships between governments and with industry. The Centre will bring together Defence's Cyber Security Operations Centre, the Attorney-General's Computer Emergency Response Team Australia, the Australian Security Intelligence Organisation (ASIO)'s Cyber Espionage Branch, elements of the Australian Federal Police's High Tech Crime Operations capability and all-source-assessment analysts from the ACC.[20]

KEY CURRENT AND EMERGING ISSUES

- The threat posed by organised crime groups is high and the continued rapid uptake of technology in Australia is increasing the opportunities for cyber and major technology-enabled crime.
- The principal threats to Australia come from criminal networks based offshore that specialise in technology-facilitated crimes, such as online fraud and attacks on computer systems.
- Organised crime groups are making use of Internet 'darknets' – protected hidden networks for trading in illicit products and information.

19 Defence Signals Directorate 2012, *Strategies to mitigate targeted cyber intrusions*, 10 October 2012, accessed 20 May 2013, <http://www.dsd.gov.au/publications/Top_35_Mitigations_2012.pdf>.

20 Department of the Prime Minister and Cabinet 2013, *Strong and secure: a strategy for Australia's national security*, viewed 31 January 2013, <http://www.dpmc.gov.au/national_security/docs/national_security_strategy.pdf>.

RANSOMWARE ATTACKS

In late 2012, there was an increase in media reporting of victims of 'ransomware' in Australia and around the world. Two main types of attacks were reported: one targeting small businesses in particular, and the second distributed en masse to home computer users.[1]

The first type of attack hacked into computers, encrypting the files and rendering them inaccessible without payment of a 'ransom'. Businesses were asked to pay a fee for their files to be unlocked.[2] In some cases, the fee increased each day it remained unpaid.[3]

The second type of attack displayed a pop-up message purporting to be from a law enforcement agency or government department (complete with logo), along with a message claiming the computer had been involved in illegal activity and had been locked until a 'fine' was paid.[4] In most cases, the files were not encrypted, but the screen had simply been locked.[5] In some instances, the webcam was remotely activated so that it seemed the user was under real-time surveillance.[6]

A variation of this attack was reported in Germany in 2013, whereby the pop-up message also contained images purporting to be child exploitation material, along with the names, dates of birth and locations of the children allegedly depicted in the photos.[7]

1 Tung, L 2012, '2013: a look at four malware predictions', *CSO Magazine* (online), 18 December 2012, viewed 19 December 2012, <http://www.cso.com.au/article/444856/2013_look_four_malware_predictions/>.
2 Department of Broadband, Communications and the Digital Economy 2012, 'Ransomware attacks will increase in 2013', accessed 18 April 2013, <http://www.staysmartonline.gov.au/alert_service/advisories/ransomware_attacks_will_increase_in_2013>.
3 O'Neill M 2012, 'Ransomware targeting businesses, home PCs', *ABC News Online*, 25 October 2012, accessed 18 April 2013, <http://www.abc.net.au/news/2012-10-25/ransomware-targeting-aussie-businesses2c-pcs/4332526>.
4 Australian Competition and Consumer Commission 2013, 'Police scareware scam continues to target Australians', accessed 18 April 2013, <http://www.scamwatch.gov.au/content/index.phtml/itemId/1026168>.
5 Tung, L 2012, '2013: a look at four malware predictions', *CSO Magazine* (online), 18 December 2012, viewed 19 December 2012, <http://www.cso.com.au/article/444856/2013_look_four_malware_predictions/>.
6 O'Neill M 2012, 'Ransomware targeting businesses, home PCs', *ABC News Online*, 25 October 2012, accessed 18 April 2013, <http://www.abc.net.au/news/2012-10-25/ransomware-targeting-aussie-businesses2c-pcs/4332526>.
7 Cluley, G 2013, 'Ransomware scares victims with child sex abuse images', accessed 18 April 2013, <http://nakedsecurity.sophos.com/2013/04/05/ransomware-child-buse/>.

IDENTITY CRIME

INTRODUCTION

Identity crime broadly encompasses:

- the theft of personal identity information (PII) and related financial information
- the assumption of another identity for fraudulent purposes
- the production of false identities and financial documents to enable other crimes.

The Australian Government's Organised Crime Response Plan recognises that combating identity crime is a key priority at the national level, because of the possible impact on national security, law enforcement and the community. The National Organised Crime Response Plan 2010–13 listed one of five core strategies as being a national response to key elements of the organised crime environment, including measures to target identity crime. As an enabler for other crime types, identity crime undermines the integrity of the economy, of financial and banking institutions, and of licensing, immigration and welfare systems.

THE CURRENT SITUATION

The rapid growth of identity crime and the misuse of PII affects many areas of society, and has also raised serious concerns internationally from a personal security and safety perspective. Identity crime has considerable social and financial implications for the Australian community. Individuals whose identities are stolen and used to facilitate criminal offences expend considerable time and effort restoring personal profiles, including re-establishing financial arrangements and amending credit profiles.

There are a range of reasons for criminal entities to engage in identity crime. In some instances, PII is stolen in order to create a false or fraudulent identity to use in the commission of an offence. With prosecutions for criminal offences being reliant on establishing the identity of the offender, criminals have historically tried to ensure that their identity has been either obscured or falsified. False identities, often based on personal details stolen from others, have variously been used by criminals to, for example, perpetrate frauds, establish business structures and companies through which to facilitate crimes such as money laundering or the importation of illicit commodities, or undertake national or international travel without those travel movements being able to be identified or traced by law enforcement agencies. Stolen identities have also been used in the commission of terrorism offences.

The size of the identity crime market in Australia is difficult to assess. For example, in some cases the victim of identity crime might, in the first instance, notify their financial institution of the theft of their credit card and other personal details, rather than notifying police. If the institution cancels the card, reimburses the victim and provides them with a new card, the identity crime is unknown to law enforcement agencies and is not recorded.

The manufacture and use of false or counterfeit and fraudulent identity documentation mainly targets banks, lending agencies, financial institutions and large retailers, allowing groups involved in identity crime to obtain fraudulent loans and withdraw funds illegally, or to facilitate organised shopping groups using false credit cards and skimmed card data. Government agencies, however, are also increasingly being targeted, particularly those that provide some form of benefit or refund, such as Centrelink and the Australian Taxation Office (ATO). For example, between 1 July and 30 November 2011, the ATO identified over 7,300 income tax returns, with claimed refunds of around $36 million, as being suspected cases of identity crime.

Identity and identity-related crime is increasingly facilitated by technology, with a growing requirement for individuals to divulge PII online in order to access goods and services, and with a greater willingness, particularly among younger people, to share PII and data with other parties online. In particular, social networking sites, on which individuals often post details such as dates of birth, addresses and places of work, can provide organised crime with sufficiently detailed personal information to allow them to commit identity crime. These details can be easily harvested and can be 'warehoused' for years before being used. This makes it difficult to identify where and when the information has been compromised.

An emerging technology-related problem is the growing availability of portable devices capable of reading bank card details from a distance – for example, 'tap and go' cards. This technology is likely to be adapted by traditional 'card skimming' groups.

Notwithstanding the increasing threat of identity crime that Internet users face, there are indications that users have a relatively low awareness of the risks associated with using information and communication technologies from an identity crime perspective. User awareness of identity crime is particularly important in the contemporary environment, in which online 'phishing' attempts are increasingly targeting specific groups such as professionals (for example, in the medical, accounting and legal professions), organisations or employment sites, with the aim of eliciting PII or other valuable data (see case study on page 23).

Capitalising on the current need for individuals to have multiple forms of electronic PII, such as personal identification numbers and computer system passwords, some organised crime groups specialise in the theft of identity data, and in particular financial data, for the purpose of on-selling it to other criminal groups. In this way, identity data has become another commodity that organised crime can trade in.

As security features on identity documents continue to improve, and more electronic PII is held in centralised repositories, organised crime is increasingly likely to target 'trusted insiders' who can facilitate the theft or compromising of sensitive data. This might involve attempts to infiltrate agencies responsible for the production of personal identification documents, or to corrupt employees within those agencies who have access to identity information and documents.

CHILDS PLAY

AN UNSOPHISTICATED ATTEMPT TO GET PERSONAL INFORMATION

In April 2013, media reporting highlighted a scam attempting to solicit personal information from Australian Government employees working in sensitive areas. The scam involved targeted emails advising that a childcare centre was soon to open that would only accept children whose parents worked in the Russell complex in Canberra. Russell is where the Defence Signals Directorate, ASIO, Defence Intelligence Organisation and other Defence Force and Department of Defence areas are located.

As part of the invitation to apply for a childcare place, the related website included an application form that asked for information not normally requested. This included employee numbers, tax file numbers and official business cards.

Although the attempt to solicit personal information from a large number of people was unsophisticated, if successful it could have garnered enough information to steal multiple identities. These could then have been used to obtain other identification documents and also to commit offences such as fraud.

KEY CURRENT AND EMERGING ISSUES

- The threat from identity crime is likely to increase over the next two years.
- Warehousing of data by organised crime groups for later use, making it difficult to detect when and how data breaches have occurred, has increased.
- In the future, organised crime groups are more likely to target trusted insiders or to attempt to corrupt officials to access information and documents. As security features on identity documents continue to improve, there may be a move to offenders applying for fraudulently obtained genuine documents.

EXPLOITATION OF BUSINESS STRUCTURES

INTRODUCTION

The criminal exploitation of business structures involves the use of unlawful business practices, and both simple and complex business structures, to conceal the criminal infiltration of an industry, to enable businesses to maintain or expand market share, and to generate and/or conceal profits. This form of exploitation, in which professional facilitators continue to have a significant role, is becoming increasingly common in Australia.

THE CURRENT SITUATION

Simple business structures – Simple business structures such as restaurants, hotels, pubs and clubs, entertainment venues and other cash-intensive businesses are typically used by organised crime in support of money laundering. This is primarily because cash profits from criminal activity can be mixed with cash flowing legitimately into these businesses, making it difficult for law enforcement to be able to identify which funds are 'clean' and which funds are 'dirty'. Transfers of cash can also be made leaving no audit trail – unlike, for example, the electronic transfer of funds, or the formal transfer of assets.

Illicit funds can also be invested in a business in an effort to maintain or expand market share, creating an unfair advantage for organised crime competing with legitimate business owners. In some instances, organised crime groups may also use violence (threatened or actual) to intimidate business competitors.

Complex business structures – Complex business structures (for example, those composed of multiple layers, with multiple controllers and international connections) are currently used by organised crime in relation to large-scale revenue and taxation fraud and money laundering. These structures may be used to hide beneficial ownership behind layers of companies and trusts in multiple offshore jurisdictions, to move and obscure the ultimate destination of funds, and to hinder regulatory and law enforcement efforts to identify assets and illicit money flows.[21]

21 Australian Transaction Reports and Analysis Centre 2011, *Money laundering in Australia 2011*, AUSTRAC, Canberra.

The exploitation of trust structures by organised crime is an ongoing problem that impairs the ability of law enforcement to identify and successfully disrupt money laundering, and the ability to identify assets obtained through criminal activity. Although trusts play an important and legitimate role in protecting assets and providing for beneficiaries, organised crime continues to use trust structures for the purpose of money laundering. Trust structures often form part of a larger, sophisticated network of business structures and proprietary companies. Unravelling complex business structures can be resource intensive, often requiring specialist skills and knowledge, protracted investigations and strong cooperation between law enforcement and regulatory agencies.

Professional facilitators – The use of professional facilitators (those with the specific skills, knowledge, expertise and resources sought by organised crime to allow them to operate seamlessly across both legitimate and illicit markets) remains a key element in the exploitation of business structures. Some facilitators – also referred to as 'promoters' – help organised crime to evade tax by registering companies (often in tax havens with strict secrecy provisions), establishing bank accounts, and providing asset management and trust services that are designed to circumvent taxation laws and obscure the owner of the funds.

Sophisticated organised criminals typically seek the services of several professional facilitators at once, enlisting each one to assist with different elements of their 'business' arrangements. This compartmentalisation of their business allows the architect of a fraudulent arrangement to create separate parts of the scheme, with each part able to be viewed in its own right as having a plausible rationale, and with each part constructed in such a way that each professional facilitator is unable to view or have knowledge of the true purpose of the entire arrangement. Typically it is only when such schemes are viewed in their entirety that their fraudulent nature is apparent.

KEY CURRENT AND EMERGING ISSUES

- Organised crime groups operating in Australia are currently using sophisticated networks of businesses, proprietary companies and trusts to enable a range of organised criminal and regulatory offences.
- Professional facilitators and 'promoters' have a significant role in helping organised criminals to exploit business structures, drawing on their specialist skills, knowledge, expertise and resources.

PUBLIC SECTOR CORRUPTION

INTRODUCTION

Public sector corruption refers to the misuse of public power or position with an expectation of undue private gain or advantage (for self or others). It may include instances of bribery, embezzlement, fraud, extortion, trading in influence, or perverting the course of justice. Corrupt conduct can occur directly through the improper or unlawful actions of public sector officials, or through the actions of individuals operating in the private sector who attempt to inappropriately influence the functions of government.

Transparency International's 2011 Corruption Perceptions Index ranked Australia the eighth 'cleanest' country in public perceptions of corruption.[22] Although this is a positive finding, it does not mean that corruption is absent in Australia (given, for example, the recent arrests of border agency officers), and organised crime continually probes for weaknesses in systems and will take advantage of any opportunities to corrupt public officials. Corruption can undermine the best regulatory systems and requires constant monitoring by anti-corruption and other agencies to mitigate the risk that it poses.

THE CURRENT SITUATION

Organised crime seeks to corrupt public sector personnel to gain access to public funds, information, protection and other services that help facilitate criminal activities. This can include targeting public officials who work in areas where they have access to information on the activities of other organised crime groups and law enforcement agencies, or where staff are able to provide identification documents such as drivers licences. Officials with the capability to facilitate organised criminal activities through 'turning a blind eye' to activities, or those who can direct targeting of goods at places such as importation points, are also likely targets.

Corruption of public sector officials has substantial multiplier effects and benefits for organised crime. There may be significant links between corruption in the public sector and organised crime groups that, by their very nature, remain hidden. The key challenge in identifying and investigating corruption is that corrupt conduct occurs in secret, between consenting parties who, frequently, are skilled at deception.

Anti-corruption agencies in Australia have highlighted that the relative strength of the Australian economy significantly increases the potential profitability of importing illicit commodities, such as illicit drugs, into Australia, with the profits from the sale in Australian dollars then being repatriated overseas. This may provide incentives for organised crime to pay large bribes to facilitate their activities and access Australian markets.

It is not just domestically based public sector officials who may be targeted by organised crime groups. Australia is represented overseas by a large number of Australian officials working in a diplomatic capacity, including law enforcement, consular, diplomatic and other officials. Many of them work in countries where there is a higher level of corruption in the public sector than is the case in Australia. Transnational organised crime groups based in those countries are likely to attempt to seek opportunities to corrupt Australian government representatives. This risk has been recognised by the Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity, which, in December 2011, announced that it would conduct an inquiry to consider the corruption risks facing international operations of law enforcement agencies. The inquiry is ongoing.

22 Transparency International's Corruption Perceptions Index measures the perceived level of public sector corruption in nearly 200 countries. It has been published since 1995.

Anti-corruption and law enforcement agencies continue to highlight public sector officials' inappropriate relationships with informants and criminal entities as a threat that can lead to corrupt activities, particularly for law enforcement agency members. Facilitating these relationships is the increasing use of social media sites by organised crime to initiate contact with public sector officials. This has been through sites based on similar interests – particularly relating to bodybuilding and kickboxing – or professional sites such as LinkedIn or Facebook, where public officials have included large amounts of personal details. Organised crime groups have used these details to initiate contact, which at first may appear to be within the context for interaction within these forums, but can be built upon to judge the potential for compromising the person being targeted.

The Australian Government is currently developing a National Anti-Corruption plan, which will position Australia to deliver a coordinated approach to fighting corruption. The plan will include specific measures to identify and manage corruption risks, including those related to organised crime. The plan will also include measures to improve the reporting and analysis of Commonwealth data on corruption.

KEY CURRENT AND EMERGING ISSUES

- The relative strength of the Australian economy significantly increases the potential profitability of importing illicit commodities, such as illicit drugs, into Australia. This may provide incentives for organised crime to pay large bribes to facilitate their activities and access Australian markets.
- Facilitating corrupt relationships is the increasing use of social media sites by organised crime to initiate contact with public sector officials. This has been through sites based on similar interests – particularly relating to bodybuilding and kickboxing – or professional sites such as LinkedIn or Facebook, where public officials have included large amounts of personal details.

VIOLENCE

INTRODUCTION

In Australia, key reasons for the use of violence by organised crime include 'warning off' competitors in criminal markets, retaliation for previous violent acts, retaliation for failure to supply goods, employment of stand-over tactics on behalf of other criminal groups, internal group discipline, maintenance of 'honour' or status, and extortion to gain money or access to other business activities. Some inter- and intra-group violence is not always related to enabling organised crime activity. It has been observed that some violence between and within organised crime groups has been to settle family and other disputes. This particularly relates to matters of honour and status as mentioned above. Examples include violence in response to a perceived slight on an individual's relative.

THE CURRENT SITUATION

The use, or threat, of violence remains an integral part of organised criminal activity in Australia. The frequency of use, and the type of violence used, depends on ethos, the crime market involved and the type of organised crime group.

Organised crime operating in Australia is also likely to use extortion, through threats of violence, as both a primary profit-generating activity – for example, in conjunction with the trafficking of highly profitable illicit commodities such as amphetamine-type stimulants (ATS) or cocaine – and an enabling activity that can assist in the expansion of market control. This can include the infiltration of legitimate business structures for criminal gain.

Violence is a key arbitrator in the competition between those operating in the same criminal markets. This means that it is likely that the levels of violence occurring among organised crime groups will ebb and flow depending on the number, size and 'strength' of the groups in any particular crime market, as well as the size and profitability of any given crime market.

Observations from Canada are that 'more sophisticated groups at times hire subordinate criminal groups or individuals to undertake violent acts on their behalf'.[23] Although the extent to which this might be occurring in Australia is not clear, there is a risk that, should more organised crime groups 'contract out' debt collection and threat functions, there could be an increase in actual violence as less sophisticated, less disciplined lower-level criminal groups accept sub-contracts for these roles. Groups willing to engage in 'stand-over' threats and debt collection are likely to have a propensity towards violence, and to consider it a legitimate tactic.

Some organised crime groups in Australia, such as outlaw motorcycle gangs (OMCGs), have a long-standing association with a culture of violence. In the past this violence has typically been conducted out of the public view. There are, however, some indications that this may be changing. The bludgeoning and stabbing death of an OMCG member at Sydney Airport in 2009 and the shooting death of Giovanni Focarelli in South Australia in January 2012 are examples of cases in which OMCG-related violence is being played out in public. The drive-by shootings that have occurred in a number of Australian states are other examples. If violence between crime groups is increasingly played out in the public space, the risk increases that members of the public will become unintended 'collateral' victims of this violence.

KEY CURRENT AND EMERGING ISSUES

- The use of violence remains an integral part of organised criminal activity in Australia.
- The apparent willingness of organised crime, and OMCGs in particular, to bring their violent disputes into public spaces increases the risk that members of the public will become unintended victims.

23 Criminal Intelligence Service Canada 2010, *Annual report 2010*, CISC, Ottawa, accessed 10 January 2012, <http://www.cisc.gc.ca/annual_reports/annual_report_2010/document/report_oc_2010_e.pdf>.

ILLICIT COMMODITIES

ILLICIT DRUG MARKET OVERVIEW

The use of illicit drugs, and the consistent exploitation of demand for illicit drugs by organised criminal individuals and groups, remain enduring problems for the Australian Government, state and territory governments, law enforcement and health agencies, and the broader community.

Although the traditional illicit drugs such as methylamphetamine, cannabis, cocaine and heroin remain entrenched markets, the broader illicit drug market is becoming increasingly complex, with a vast array of substances now available to motivated users.

In recent years, law enforcement and health agencies in Australia, Western Europe and North America have encountered an increasingly complex environment, with the emergence of drug analogues and other novel substances. According to analysis of the current European Union (EU) drugs markets by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol, there has been a dramatic increase in the number, type and availability of new substances in Europe, with a record 73 new substances detected there for the first time in 2012. Overall, the EU early warning system currently monitors more than 250 substances.[24]

The drug analogue and other novel substances market is unique, and is challenging existing regulatory approaches. This is compounded by the existence of a marketplace within a 'virtual environment' – where interaction between manufacturers, suppliers and users, and the exchange of drugs, product and use knowledge, and payment for product, occurs on the Internet.

24 European Monitoring Centre for Drugs and Drug Addiction & Europol 2013, *EU drug markets report: a strategic analysis*, EMCDDA, Lisbon & Europol, The Hague.

The Internet has also accelerated the evolution of some drug markets and created a rapidly changing market dynamic. Information on new drugs, doses, routes of administration, effects and drug combinations – which was previously communicated through word of mouth – now spreads rapidly through social networking sites and bulletin boards devoted to illicit drug use. Vendors are also exploiting the Internet by openly advertising the development and release of new product lines and offering product reviews and free drug samples to promote their latest products.

Although established drug monitoring systems continue to provide a good insight into the dynamics of established and traditional drug markets, the growing speed with which new markets are developing has made the monitoring of drug markets from a holistic perspective increasingly difficult, and has decreased the effectiveness of established drug monitoring systems. This situation has left both health providers and law enforcement agencies struggling to maintain a contemporary understanding of these markets.

Further, visibility of the drug analogue and novel substance market remains limited, as these drugs emerge so quickly that questions pertaining to their use are typically not included in established drug use monitoring questionnaires, such as the Australian National Household Survey.

To overcome this problem, agencies in the European Union and the United Kingdom have developed innovative data collection strategies[25] designed to provide relevant authorities and decision-makers with ongoing timely insights into these markets. In Australia, the Australian component of the Global Drug Survey and the National Drug and Alcohol Research Centre's National Illicit Drug Indicators project are currently looking at the Australian novel substances market and the use of the Internet.

METHYLAMPHETAMINE

In the past, law enforcement has assessed the market for methylamphetamine under the heading of amphetamine-type stimulants (ATS) – a heading that also covered MDMA or 'ecstasy'. Now, the markets for methylamphetamine and MDMA have evolved so differently that it is no longer useful or appropriate to group them together in undertaking an assessment of the risk that they pose.

National drug use monitoring surveys have identified increasing use and availability of methylamphetamine, and increases in users' perceptions of the purity of the drug, over the past five years.[26] Both anecdotal reports and drug user monitoring surveys suggest increasing use and availability of crystalline methylamphetamine in particular.[27]

The Australian methylamphetamine market continues to combine domestic production with illicit importations. Although organised crime groups maintain a strong presence in the market, market participants are diverse, and include individuals and groups operating at various levels of sophistication and capability. The following case study demonstrates the sophistication of some organised crime groups involved in the methylamphetamine market (see case study on page 31).

25 This includes the collection of samples from urinals at major music festivals and the analysis of waste water.

26 National Drug and Alcohol Research Centre 2012, 'Key findings from the 2012 IDRS', NDARC conference, Sydney; Macgregor, S & Payne, J 2011, *Increase in use of methamphetamine*, Australian Institute of Criminology, Canberra.

27 National Drug and Alcohol Research Centre 2012, 'Key findings from the 2012 IDRS', NDARC conference, Sydney.

SEIZURE OF 365 LITRES OF LIQUID CONTAINING METHYLAMPHETAMINE

A joint investigation by the Australian Federal Police, Australian Crime Commission, Australian Customs and Border Protection Service and Victoria Police identified a shipping container that was believed to contain methylamphetamine being imported into Australia.

The container, holding 46 pallets of liquid carpet stain cleaner, arrived in Melbourne from Hong Kong in April 2013. Examination of the contents revealed that 96 of the 3,332 bottles of liquid cleaner contained methylamphetamine. It is estimated that the 365 litres of liquid methylamphetamine would equate to 280 kilograms of pure methylamphetamine, with a total street value of up to $205 million.

Criminal entities involved in methylamphetamine production have a great degree of flexibility because of the numerous methods by which methylamphetamine can be synthesised, and the variety of precursor chemicals that can be used in methylamphetamine production. This enables those involved in the production of methylamphetamine to quickly adapt to any changes in the availability of precursors, or in regulatory controls.

A recent ACC assessment of precursor chemical controls found that, since the inception of the voluntary Code of Practice for Supply Diversion into Illicit Drug Manufacture in 1994, illicit drug manufacturing methodologies have changed. A trend back towards the classic routes of synthesis for methylamphetamine has been observed. Many of the key chemicals used in these methods are listed in Category II of the Code, which does not require that they be recorded or reported to authorities.

In relation to distribution, the market is also diverse. Distribution occurs through a complex web of networks, ranging from social groups through to organised criminal groups engaged in the large-scale importation and distribution of precursor chemicals and methylamphetamine.

PRECURSOR CHEMICALS

Precursor chemicals are an essential part of the production process for illicit drugs. The chemicals required differ according to the drug being produced and the production process used. Methylamphetamine is the main illicit drug manufactured in Australia requiring precursor chemicals.

Large amounts of precursor chemicals continue to be detected at the border, and to be diverted domestically from a range of sources. The People's Republic of China, Thailand, Cambodia and India are primary source countries for the Australian illicit precursor chemical market.

In 2011–12, the Australian Customs and Border Protection Service (ACBPS) made 1,026 precursor detections, weighing a total of 2,079.22 kilograms.[28] This represented an increase in the number of detections (up from 785), but a decrease in the weight of detections (down from 3,470.47 kilograms) from the previous year.[29] The majority of these detections (in both weight and number) were of precursors used in the production of amphetamine-type stimulants (incorporating precursors to methylamphetamine) such as ContacNT,[30] but precursors for LSD (lysergic acid diethylamide), GHB (gamma-hydroxybutyrate) and MDMA (3,4-methylenedioxymethylamphetamine or 'ecstasy') were also detected.[31] In addition to precursor border detections, there were a number of significant national precursor seizures in 2011–12. This included an 11 tonne seizure of hypophosphorous acid, which is used in the manufacture of methylamphetamine.[32]

28 Australian Customs and Border Protection Service 2012, *Annual report, 2011–12*, ACBPS, Canberra.
29 ibid.
30 ContacNT is a cold and flu medication manufactured legitimately in China for use in the domestic market. It contains a high proportion of pseudoephedrine and is a favoured precursor used in the manufacture of methylamphetamine.
31 Australian Customs and Border Protection Service 2012, *Annual report, 2011–12*, ACBPS, Canberra.
32 Australian Crime Commission 2013, *Illicit Drug Data Report 2011–12*, ACC, Canberra.

COCAINE

The main countries involved in cocaine production are Colombia, Peru and Bolivia. Global coca production has continued to decline because of significant decreases in the cultivation of coca in Colombia. Although coca production increased in 2010 in Peru and Bolivia, these increases were not sufficient to offset decreased Colombian coca production[33] – a decrease largely brought about by enforcement efforts in Colombia.

According to the UNODC's World Drug Report, North America and Western and Central Europe remain the largest cocaine markets. Though reduced Colombian cocaine production has led to a decrease in supply of cocaine to the United States, there has not been a decline in supply of the same magnitude in the European market.[34]

There are mixed indications of the availability and use of cocaine in Australia. On the one hand, the 2010 National Household Survey reported the highest level (by number of users) of recent cocaine use since the survey began in 1993.[35] It also reported that the number of individuals who had been offered, or had the opportunity to use, cocaine increased consistently between 1998 and 2010.[36]

However, while reported cocaine use in Australia is at historically high levels, an examination of patterns of use shows that 60.8 per cent of people who had used cocaine within the last year had used cocaine only once or twice.[37] The proportion of people reporting recent use of cocaine through injection has also been declining.[38] Drug user surveys indicate that cocaine use is relatively stable among injecting drug users and decreased significantly between 2011 and 2012 among regular ecstasy-and-related-drug users.[39]

The international cocaine market continues to be dominated by entrenched criminal groups such as Colombian and Mexican groups, who have consistently demonstrated the capacity to innovate in response to law enforcement actions. In recent years, however, an increasing range of criminal groups have become involved in cocaine trafficking as a result of new trafficking routes and the global footprint of cocaine in terms of user market locations.

Given the increasingly dynamic international cocaine market and the increasing involvement of criminal groups who have not traditionally been involved in cocaine trafficking, Australia is likely to see groups who have not traditionally been involved in cocaine trafficking and distribution develop a presence in the Australian cocaine market. The high price that cocaine commands in Australia makes this country an attractive and lucrative market for criminal groups.

33 United Nations Office on Drugs and Crime 2012, *World drug report 2012*, United Nations, Vienna.
34 ibid.
35 Australian Institute of Health and Welfare 2011, *2010 National Drug Strategy Household Survey*, Drug Statistics Series no. 25, cat. no. PHE 145, AIHW, Canberra.
36 ibid.
37 ibid.
38 Phillips, B & Burns, L 2011, *Eleven years of cocaine trends among people who inject drugs in Sydney: price, purity and availability 2000–2010*, Drug Trends Bulletin, NDARC, Sydney.
39 National Drug and Alcohol Research Centre 2012, 'Key findings from the 2012 IDRS and EDRS', NDARC conference, Sydney.

These high prices, however, may also act as an inhibitor to the large-scale expansion of the cocaine user market in Australia. The price of cocaine in Australia has been stable to increasing over the past two years, and some users are reporting inconsistent purity as a factor discouraging their use.

HEROIN

Global production of opium increased substantially in 2011. In South West Asia, opium production was estimated at 5,800 tonnes – a 61 per cent increase compared with 2010, when opium yields were significantly lower because of a plant disease.[40] This was despite a 65 per cent increase in poppy eradication in 2011.

Opium production in South East Asia has also continued to increase, particularly in Myanmar, which remains the main producer of opium in the region. Based on UNODC crop estimates, opium production in South East Asia has doubled between 2006 and 2011. Sources in Myanmar suggest that opium production is more widespread and substantially higher than official UNODC estimates.[41]

The number and weight of national heroin seizures, which includes both border and domestic seizures, continued to increase in 2011–12. The number of heroin seizures in 2011–12 is the highest reported in the last decade, while the weight of national seizures is the second highest weight reported in the decade.[42] Despite fluctuations in national heroin seizures over the last decade, reported recent heroin use in the general population has remained unchanged since 2001.[43]

Rates of heroin use in Australia are relatively low in comparison with the rates for other illicit drugs. The 2010 National Household Survey identified that 1.4 per cent of Australians aged 14 years or older had ever tried heroin, and just 0.2 per cent of the population had used it in the previous 12 months.[44] Despite reports of heroin becoming increasingly available, and significant increases in border and domestic seizures, user reports suggest that the quality of heroin remains inconsistent.

Although Afghanistan remains the largest producer of illicit opium in the world, South East Asia and South West Asia remain the key source regions for heroin seized at the Australian border.[45]

Should the availability of heroin increase, any expansion in the use of heroin may be limited by the negative reputation that the drug retains within the wider community.[46] The price of heroin has remained relatively stable over many years and is unlikely to decrease in the immediate future. However, a reduction in price is also unlikely to change the negative perception associated with heroin use. It is therefore anticipated that the heroin market will remain stable in Australia over the next two years.

40 United Nations Office on Drugs and Crime 2011, *Afghanistan opium survey 2011 summary findings*, UNODC, Geneva.
41 Palaung Women's Organisation 2011, *Still poisoned*, Palaung Women's Organisation, Burma; Shan Herald News Agency 2011, *Shan drug watch newsletter*, October 2011, Shan Herald News Agency, Burma.
42 Australian Crime Commission 2013, *Illicit Drug Data Report 2011–12*, ACC, Canberra.
43 Australian Institute of Health and Welfare 2011, *2010 National Drug Strategy Household Survey*, Drug Statistics Series no. 25, cat. no. PHE 145, AIHW, Canberra.
44 ibid.
45 Australian Crime Commission 2013, *Illicit Drug Data Report 2011–12*, ACC, Canberra.
46 Australian Institute of Health and Welfare 2011, *2010 National Drug Strategy Household Survey*, Drug Statistics Series no. 25, cat. no. PHE 145, AIHW, Canberra.

DRUG ANALOGUES AND OTHER NOVEL SUBSTANCES

Drug analogues[47] are synthetically created substances that have a similar chemical structure to an illicit drug, or that mimic the effects of illicit drugs. An increasing range of drug analogues continue to be manufactured and released, creating an increasingly complex market. The range of substances includes stimulants, hallucinogens, anaesthetics and cannabimimetics (substances that mimic the effects of cannabis).

Vendors and manufacturers continue to exploit legislative loopholes, with the manufacturers of drug analogues using scientific literature to assist in the identification of potentially psychoactive substances not yet regulated.[48]

The Internet remains a key driver of the drug analogue market both domestically and internationally. One of the most significant features of the drug analogue market is the acceleration of market trends as the result of rapid diffusion through the Internet of information on new drug analogues. This is being facilitated by vendors and through user discussion groups, with information readily available on effect, side-effects and dose.

Distribution of drug analogues through the Internet has also shortened supply chains, with users now making direct contact with wholesale vendors and, in some cases, the manufacturers of these substances. According to the United Kingdom Advisory Council on the Misuse of Drugs (ACMD), the drug analogue market has brought a different type of 'drug dealer', with many of the people importing drug analogues having had no previous involvement in the illicit drug trade. These individuals are in the market to make a quick profit by exploiting the window between the release of novel substances and their subsequent regulation.[49]

The manner in which the market responds to the introduction of regulation varies considerably. Certain drug analogues will disappear from the catalogues of online vendors quite rapidly after legislative amendments, accompanied by a corresponding rapid decline in reported seizures. This may be the result of a combination of reasons, including user dissatisfaction and increased risk associated with supply. Other substances, irrespective of changed legal status, will persist in the market, albeit at reduced volume and at irregular intervals. Examples of these are a number of the cannabimimetics (in particular, several JWH compounds), MDPV, TFMPP and the 2C-phenethylamines. It is interesting to note that, although certain drugs may appear to be absent from markets when assessed on traditional seizure indicators, their continued presence can be identified through forensic toxicology screening and post-mortem analysis.

The number of novel substances entering the global market is steadily growing, with particular substances becoming established independent of controls. Thus the trajectory of the Australian drug analogue and novel substances market is likely to follow the global trend, and the market is anticipated to further diversify.

47 For the purposes of this assessment, the term 'drug analogue' is used to describe drug analogues and other novel substances.
48 Advisory Council on the Misuse of Drugs 2011, *Consideration of the novel psychoactive substances (legal highs)*, ACMD, London.
49 ibid.

As many of the substances entering the market are novel, there is limited research or information on the health consequences of their use. There is also potential for harm as the result of inadequate user information and/or understanding about potentially fatal doses, risk of dependence and possible adverse effects caused by use with other drugs.

MDMA

After a major worldwide shortage in the availability of MDMA (3,4-methylenedioxymethylamphetamine or 'ecstasy'), the domestic market has been in a state of dormancy for the past eighteen months to two years. However, with the recent increased availability of high-quality MDMA, the market now appears to be regenerating. This reflects trends being observed in Western Europe and North America, with reports suggesting a possible resurgence in the global market.[50] Detections of the MDMA direct precursor safrole at the Australian border in 2013 point to the existing criminal interest in re-establishing local manufacture of MDMA in Australia.

Before this recent shift in the market, the consistently poor quality of the tablets that were available, and the acceptance by users of the short supply, resulted in users moving away from the use of MDMA[51] to a range of other drugs, including drug analogues and methylamphetamine. It is likely that this trend will reverse should MDMA availability and quality continue to improve.

Should the increased availability of MDMA continue, groups previously active in the trafficking of MDMA will be capable of quickly re-establishing distribution. It is anticipated that criminal groups with a historical presence in the Australian MDMA market will move quickly back into the market should they be capable of securing adequate supplies.

The presence of tablets marketed as MDMA but containing other substances will remain a feature of the Australian MDMA market, with demand for tablets and MDMA increasing the opportunity for criminal individuals and groups to pass off substances such as piperazines and drug analogues as MDMA.

With the number of MDMA laboratories detected in Australia in 2011-12 decreasing considerably from 16 in 2010-11 to 2 in 2011-12, [52] the Australian MDMA market relies largely on international supplies to satisfy domestic demand. It is anticipated that domestic criminal groups will continue to try to acquire precursor chemicals to produce MDMA, but that these ventures will remain largely opportunistic. Given the established large-scale capacity of overseas production, international suppliers will remain the predominant source of MDMA for the Australian market.

50 See European Monitoring Centre for Drugs and Drug Addiction 2013, *EU drug markets report: a strategic analysis*, EMCDDA, The Hague, p. 95, p. 101 and United Nations Office on Drugs and Crime 2012, *World drug report 2012*, UNODC, Vienna.
51 National Drug and Alcohol Research Centre 2011, 'Key findings from the 2011 IDRS and EDRS', NDARC conference, Sydney.
52 Australian Crime Commission 2013, *Illicit Drug Data Report 2011–12*, ACC, Canberra.

CANNABIS

The Australian cannabis market remains the largest illicit drug market in Australia, with continued high levels of cannabis use. The 2010 National Household Survey identified the first increase since 1998 in the percentage of people reporting recent cannabis use – which increased from 9.1 per cent in 2007 to 10.3 per cent in 2010.

Diversity in the size and sophistication of cultivation remains a feature of the Australian cannabis market. Cultivation ranges from small-scale production for personal use or distribution within social networks through to large, sophisticated hydroponic and outdoor operations. Importations of cannabis are minimal – in 2011–12, there were 2,660 detections, weighing a total of 16.95 kilograms.

The most significant change to the cannabis market over the past two years has been the increasing popularity of synthetically produced smoking blends that provide effects similar to cannabis because of the presence of cannabimimetics – substances that mimic the effects of cannabis. Although cannabimimetics have been available online since at least 2004,[53] they have recently become increasingly popular among Australian users.

Smoking blends containing cannabimimetics are readily available through the Internet, 'legal high' stores, adult sex shops and tobacconists. These products are popular with users, given the legality of some products[54] in some jurisdictions, and the difficulties in identifying these products in standard workplace testing processes. Regulatory authorities have been challenged in effectively regulating cannabimimetics because of the large number currently on the market. As in the drug analogue market, after the introduction of regulations to control a specific type of mimetic, vendors will switch to selling those that have not yet been identified for regulation.

High levels of domestic distribution of cannabimimetics have been identified in Australia. The distributors identified in this country demonstrate a moderate level of sophistication and organisation, but low-level distribution operations have also been identified.[55]

ILLICIT PHARMACEUTICALS

The illicit pharmaceutical market is highly complex and multifaceted. The abuse of genuine pharmaceutical drugs is recognised as an increasing problem both domestically and internationally.[56] The principal classes of prescription drugs misused are opioid analgesics and benzodiazepines. Though a range of antidepressants and antipsychotics are also misused, this is not yet a major problem in Australia.

53 European Monitoring Centre for Drugs and Drug Addiction 2009, *Understanding the 'Spice' phenomenon*, EMCDDA, Lisbon.

54 It should be noted that some samples of 'legal' products seized by police do actually contain banned compounds and are therefore illegal.

55 For example, although wholesalers identified in Australia have professional packaging and high levels of organisation, some distributors in Australia and New Zealand are operating out of residential premises and packaging by using computer printers and stapling the pieces of paper to clip-seal bags.

56 International Narcotics Control Board 2010*, Report of the International Narcotics Control Board 2009*, United Nations, Geneva.

Collectively, the non-medical use of pharmaceuticals is a large market, with 4.2 per cent of people reporting the recent use of any pharmaceutical for non-medical purposes in the 2010 National Household Survey. This is the second-highest category of all illicit drugs examined in the survey and a significant increase from the 3.7 per cent reported in 2007.

The illicit pharmaceutical market is composed of diverse users, ranging from high-dose dependent users, who may also be illicit drug users, through to nondependent users. The population of users is large but hidden, with these people rarely coming to the attention of police or health services. Pharmaceuticals are misused for a variety of reasons, including the management of other drug-related problems and drug substitution.

The ease with which pharmaceutical drugs can be acquired through, and diverted from, legitimate avenues of supply remains a major feature of the illicit pharmaceutical market. Because of the ease with which these drugs can be acquired, the involvement of organised criminal groups and individuals is limited. However, there are organised networks of individuals involved in the acquisition and on-selling of pharmaceuticals, particularly opioids. These networks are typically composed of individuals who are also users of these substances and are engaged in on-selling for profit.

There are significant potential harms from misuse and abuse of illicit pharmaceuticals. In the United States, the Department of Health and Human Services statistics show that, in 2007, medical opioids were involved in more overdose deaths than heroin and cocaine combined.[57] In 2010, a press release from the US Centers for Disease Control and Prevention stated:

> ***In 2010, nearly 60 percent of the drug overdose deaths (22,134) involved pharmaceutical drugs. Opioid analgesics, such as oxycodone, hydrocodone, and methadone, were involved in about 3 of every 4 pharmaceutical overdose deaths (16,651), confirming the predominant role opioid analgesics play in drug overdose deaths.****
>
> * Centers for Disease Control and Prevention, viewed at <http://www.cdc.gov/media/releases/2013/p0220_drug_overdose_deaths.html>.

OPIOID ANALGESICS

Opioid analgesics, also known as narcotic analgesics, are pain relievers that act on the central nervous system. Among the drugs in this category are codeine, fentanyl, morphine and oxycodone. These drugs come in many forms – tablets, syrups, suppositories and injections – and are sold only by prescription. Opioids cause euphoria, which may account for their increasing misuse and abuse. Despite high levels of legitimate prescribing, pharmaceutical opioids are widely and increasingly being misused in Australia.

57 US Department of Health and Human Services 2010, *Unintentional drug poisoning in the United States*, <http://www.cdc.gov/homeandrecreationalsafety/pdf/poison-issue-brief.pdf>.

This is reflected in the 2010 National Household Survey data, where 3 per cent of people reported the recent use of analgesics for non-medical purposes[58] and 0.4 per cent of people reported the non-medical use of other opiates/opioids. This contrasts with 0.2 per cent of people reporting the recent use of heroin.[59] A key driver of the misuse of pharmaceutical opioids is consistency in quality, price and availability.

Pharmaceutical opioids remain readily available, with a variety of sourcing methods used to acquire these drugs. Specific research into the prescription drug market by the Australian Institute of Criminology's Drug Use Monitoring in Australia (DUMA) program found that 43 per cent of recent users of prescription opioids had been given them by a friend or family member, with 21 per cent using a script in their own name.

BENZODIAZEPINES[60]

Benzodiazepines are a group of drugs called minor tranquillisers that are prescribed by doctors to help with anxiety and sleeplessness. Commonly known trade names include Valium®, Serapax®, Zanax® and Mogadon®. The misuse of benzodiazepines is not a new phenomenon, with historical data showing consistently high levels of benzodiazepine use and misuse in Australia. The relatively high level of benzodiazepine misuse is reflected in National Household Survey data, with 1.5 per cent of survey respondents (an estimated 250,000 people) reporting the recent use of tranquillisers/sleeping pills for non-medical purposes in 2010. This compares with 2.1 per cent of survey respondents reporting the recent use of cocaine in the same 2010 survey. Alprazolam – used to treat anxiety and panic disorders - has been identified as one of the most widely used benzodiazepines in Australia, with more than 400,000 prescriptions for alprazolam recorded by the Pharmaceutical Benefits Scheme (PBS) in 2009.[61] High levels of alprazolam abuse have also been reported among injecting drug users who report the injection of benzodiazepines.[62]

PERFORMANCE AND IMAGE ENHANCING DRUGS

Quantifying the size of the performance and image enhancing drugs (PIEDs) market in Australia remains difficult, given the limited amount of formal research that has been conducted on PIEDs use. However, based on law enforcement data it is clear that the Australian PIEDs market has expanded rapidly in recent years:

- There has been an increase in border seizures, with the number of PIEDs detected at the Australian border increasing from 2,695 in 2009–10 to 5,561 in 2010–11, a 106 per cent increase and the highest recorded number of PIEDs detections at the border in the last decade.

58 In the 2010 National Household Survey, analgesics include paracetamol, aspirin, Nurofen Plus®, Panadeine Forte®, morphine, pethidine, fentanyl and Endone®. Of the 3 per cent reporting the recent use of analgesics, 27.9 per cent were for Panadeine Forte®, morphine, pethidine, fentanyl and Endone®.
59 Australian Institute of Health and Welfare 2011, *2010 National Drug Strategy Household Survey report*, AIHW, Canberra.
60 Benzodiazepines are a group of legal psychoactive drugs that act as central nervous system depressants, and have a sedative effect on those taking them.
61 Monheit, B 2010, 'Prescription drug misuse', *Australian Family Physician*, vol. 39, no. 8 (August 2010).
62 ibid.

- There was an increase of 255 per cent between 2009–10 and 2010–11 in the number of hormones detected at the Australian border.
- The number and weight of national steroid seizures in 2011–12 were the highest reported in the last decade, with the number of arrests the highest on record.[63]

Although anabolic steroids remain the most widely recognised PIEDs, an array of drugs that were originally developed for the treatment of medical and hormonal disorders by manipulating the body's hormonal system are now also being used as PIEDs as they promote muscle and bone growth. These can be broadly grouped as:

- growth hormone releasing peptides (commonly known as peptides)
- selective androgen receptor modulators (SARMs)
- insulin-like growth factor (IGF-1) and mechano growth factor (MGF).

Research has found that PIEDs use among young males is substantially higher than in the general population, with body image considerations a major driver of PIED use for this segment of the population.[64]

Motivated individuals are able to readily acquire PIEDs through avenues such as personal networks, individuals within legitimate businesses such as gyms, sporting clubs and fitness centres, compliant doctors, anti-ageing clinics, pharmacists, thefts from medical sources (such as hospitals), the veterinary industry and Internet sales. Coaches and elite athletic support staff have also been identified acquiring PIEDs for elite athletes.

Various methods are used to import PIEDs into Australia, including post, carriage on the person and air cargo. Sophisticated concealments and strategies employed in the importation of other illicit commodities have also been used to import PIEDs. Overseas-based suppliers of PIEDs have been identified facilitating concealments and providing advice on how to reduce the likelihood of importations being detected at the border.

A diverse range of individuals have been identified as users of PIEDs. However, users can be categorised into three main groups – elite and sub-elite athletes, bodybuilders and clients of anti-ageing clinics.

Entrepreneurial individuals and groups also feature prominently in the PIEDs market in Australia, but typically operate at lower levels of sophistication. Profitability remains a key driver of this market, with the distribution of PIEDs being highly profitable and relatively low risk, given the penalties typically handed down for PIED importations and distribution. In many cases, entrepreneurial individuals and groups are also users of PIEDs.

63 Australian Crime Commission 2013, *Australian Illicit Drug Data Report 2011–12*, ACC, Canberra.

64 Dunn, M & White, V 2011, 'The epidemiology of anabolic-androgenic steroid use among Australian secondary school students', *Journal of Science and Medicine in Sport*, vol. 14, pp. 10–14. This survey of secondary school students found that 2.4 per cent of 12–17-year-old males reported that they had used PIEDs.

Internationally organised crime groups are heavily involved in the trafficking of PIEDs, with groups such as the Italian Mafia and Russian organised crime groups trafficking PIEDs across Europe. Organised criminal groups and individuals have been identified as having an increasing presence in the distribution of PIEDs, and have developed an increasing presence in the trafficking of PIEDs in Australia. The majority of the PIEDS currently identified being trafficked to Australia have been ordered online from China, though some have also come from online suppliers in the United States and Canada.

In February 2013, the ACC released its report *Organised crime and drugs in sport*. The report concentrated on new-generation PIEDs and organised criminal involvement in their use in professional sport. It assessed that organised criminal identities and groups will expand their presence in the Australian peptide and hormone market. Furthermore, it identified that the presence of organised criminal identities and groups in the PIEDs market presents a threat to the integrity of Australian professional sport, as a direct consequence of the increased likelihood of criminal identities and groups interacting with professional athletes and the potential exploitation of these relationships for criminal purposes, including match fixing.

ANAESTHETICS

The markets in both ketamine and GHB – the principal anaesthetics used illicitly in Australia – remain stable niche drug markets, with the National Household Survey revealing that only 0.2 per cent of the population reported recent use of ketamine and only 0.1 per cent of the population reported recent use of GHB in both the 2007 and 2010 surveys.

KETAMINE

Ketamine – most commonly used legitimately as a veterinary anaesthetic – continues to be sourced through diversion from legitimate sources, such as veterinary clinics and hospitals, with the postal stream remaining the predominant importation stream (94.9 per cent of border detections).[65] In 2010–11, China and the United Kingdom[66] were the principal embarkation points for ketamine importations into Australia. Although ketamine is distributed alongside other illicit drugs and through traditional user–dealer relationships, organised criminal groups do not have a strong presence in the ketamine market in Australia, with opportunistic diversion and importation sufficient to satisfy market demand.

In November 2010, the European Monitoring Centre for Drugs and Drug Addiction identified the emergence of methoxetamine (3-MeO-2-Oxo-PCE), a substance that provides similar effects to ketamine.[67] This substance started to gain popularity among users in Australia in mid-2011 and, since that time, appears to have become increasingly popular.

65 Australian Crime Commission 2013, *Australian Illicit Drug Data Report 2011–12*, ACC, Canberra.

66 The use of ketamine has increased significantly in the United Kingdom in recent years. According to data compiled through the British Crime Survey, in 2006–07 an estimated 0.8 per cent of 16–24-year-olds had taken ketamine in the last month. In 2010–11, this figure had risen to 2.1 per cent.

67 According to erowid.org, a major drug information site, a normal dose of ketamine (75 mg – 300 mg) will last about 90 minutes, with after-effects lasting 4 to 8 hours. A typical dose of methoxetamine (15 mg – 50 mg) will last 3 to 5 hours, with after-effects lasting 2 to 48 hours.

Methoxetamine is distributed through 'legal high' stores on the Internet alongside other drug analogues, and retails for about A$26 per gram. Should methoxetamine remain available through international 'legal high' websites, the methoxetamine market in Australia is likely to expand.

GHB

Gamma-hydroxybutyrate (GHB) is a powerful central nervous system depressant. Although use of GHB among the general population remains low, it is more prevalent within specific populations, such as the 'rave'/dance scene.[68] Research on GHB and ketamine users found that GHB users are typically male and experienced poly drug users.[69]

Though organised criminal individuals and groups have a presence in the trafficking of GHB, GBL and 1,4-BD in Australia, the level of sophistication required to operate in this market is low, given the ease with which GBL and 1,4-BD can be diverted from legitimate industry to satisfy the demands of a small market.

TRYPTAMINES

Tryptamines are hallucinogenic substances that act on the central nervous system, distorting mood, thought and perception. Common tryptamines used in Australia are LSD, psilocybin-containing mushrooms and dimethyltryptamine (DMT).

A range of tryptamines are used in Australia. The tryptamine market is complex, given the significant diversity in relation to both the sourcing of, and subsequent distribution networks for, the various substances. Although LSD is typically produced overseas, and must therefore be imported, substances such as DMT and psilocybin-containing mushrooms occur naturally in various parts of Australia.

According to national drug user surveys, hallucinogen use has expanded in recent years, with significant increases identified in the use of LSD, DMT, psilocybin-containing mushrooms, mescaline, 5 MeO-DMT and salvia.[70] A significant increase in the number of individuals who had the opportunity to use hallucinogens was also identified in the National Household Survey in 2010.[71]

Although LSD and psilocybin-containing mushrooms remain the most commonly used hallucinogens, a range of other hallucinogenic substances are available in Australia. The majority of individuals use tryptamines irregularly, but a defining feature of the tryptamine market is the strong sub-culture that exists around the use of these substances for personal, spiritual and/or religious reasons. This niche user community who use tryptamines on a regular basis have dedicated websites, Internet forums, conferences and events, and actively promote the use of hallucinogenic substances.[72]

68 Degenhardt, L & Dunn, M 2008, 'The epidemiology of GHB and ketamine use in an Australian household survey', *International Journal of Drug Policy*, vol. 19, pp. 311–16.

69 ibid.

70 National Drug and Alcohol Research Centre 2011, 'Key findings from the 2011 IDRS and EDRS', NDARC conference, Sydney; Australian Institute of Health and Welfare 2011, *2010 National Drug Strategy Household Survey*, Drug Statistics Series no. 25, cat. no. PHE 145, AIHW, Canberra.

71 ibid.

72 One organisation in particular – MAPS – has been instrumental in gaining US Government approval for formal research into the efficacy of hallucinogens for the treatment of addiction, pain, trauma and anxiety.

Though social networks play a primary role in the distribution of tryptamines, these substances are also distributed through traditional user–dealer transactions. However, organised crime involvement in the market remains low. The barriers to entry into the tryptamine market are relatively low, given the ease with which some tryptamines can be sourced, and the large number of substances that provide hallucinogenic experiences.

INTELLECTUAL PROPERTY CRIME

Intellectual property (IP) crime is a generic term that describes three types of crime markets – counterfeit goods, piracy (the illegal copying of or access to content such as films, music, computer games and software for profit), and the theft of trade secrets.

The high profits to be made from the three types of IP crime attract organised crime, and the appeal of this market for international organised crime is likely to increase as the value of IP continues to rise. The increasing value of IP can be seen in the royalties and licensing fee receipts of companies.[73] According to the World Intellectual Property Organization, these increased from US$2.8 billion in 1970 to US$27 billion in 1990, and to about US$180 billion in 2009 – outpacing growth in global gross domestic product.[74] Key drivers of this increase are a global surge in research and development leading to more patentable inventions; globalisation of economies leading to a need to lodge patents in more jurisdictions; increased tradeability of IP and knowledge; and strategic patenting by business to collect IP-related income and protect revenue.

COUNTERFEIT GOODS

Globally there is ongoing growth in the volume and types of goods counterfeited by organised crime. This includes products as diverse as aircraft parts for military, commercial and general aviation, oilfield pipeline couplings,[75] razors, batteries, pesticides and foodstuffs. This is reflected in Australia, where the ACBPS seizes counterfeit goods under 22 different product-type headings.

Assessments of the value of the global counterfeit goods market vary. Recently, Frontier Economics completed an assessment based on 2008 figures, and estimated the cost of the global market to be between US$455 billion and US$S650 billion per year, forecasting that it could reach US$1.7 trillion by 2015. This is higher than previous forecasts, but includes the impacts of lost tax revenue and higher government spending on law enforcement and health care that result from counterfeiting. There are no similar figures for Australia, but the ACBPS does provide a value for counterfeit goods seized. For 2008–09 this value was just over A$11 million, in 2009–10 just over A$37 million, and in 2010–11 just over A$29 million.

73 The World Bank defines royalty and licence fees as payments and receipts for the authorised use of intangible, nonproduced, non-financial assets and proprietary rights (such as patents, copyrights, trademarks, industrial processes and franchises) and for the use, through licensing agreements, of produced originals of prototypes (such as films and manuscripts). For more information, see <http://data.worldbank.org/indicator/BX .GSR .ROYL .CD>.

74 World Intellectual Property Organization 2011, *2011 World intellectual property report: the changing face of innovation*, WIPO, Geneva, p. 9.

75 For more on these, see Federal Bureau of Investigation, *PRO IP Act annual report 2010*, Congressional Report, pp. 5–6.

PIRACY

IP piracy is considered significant in most economies and is facilitated by technological change. Improvements in technology are making it easier and cheaper to pirate products for profit. For example, the expansion of broadband network connections to the Internet and increasing peer-to-peer networks make it quicker and easier to download large files such as films and video games.

Overseas, OCG involvement in IP piracy offences is well documented. Organisations such as Interpol, the World Customs Organisation, the United Kingdom's Intellectual Property Crime Group and Canada's Criminal Intelligence Service have all identified OCG involvement in this crime type. The level of involvement of Australian-based organised crime in this activity is not clear.

IP piracy in the future will most likely be influenced by changes in technology. The two main aspects of this are likely to be increased use of mobile devices and increasing bandwidth and download speeds for Internet users. In the United States, industries have reported growing piracy problems as a result of criminals exploiting mobile phones, palm devices, flash drives and other mobile technology.[76] The continued expansion of new technologies is likely to enhance the ability of criminals to pirate digital products, with a continuation of the trend of digital IP piracy taking a greater share of the overall IP piracy market away from physical media. As technology makes it easier for more people to pirate digital products, it may lessen the attractiveness of this activity to organised crime, as profits would probably decline. There would also be less need for consumers to rely on organised crime to obtain pirated product.

TRADE SECRETS

The true extent of the theft of trade secrets (commercially valuable information not disclosed to the public) and other intangible IP is difficult to ascertain because of the lack of reporting by companies that have suffered losses. However, it is estimated that US$1 trillion of IP is stolen globally each year.[77] Even if the trade secrets and other intangible IP component of this is small, it still represents a substantial figure. Victims face a difficult choice. If they report the theft or unauthorised use of trade secrets and other intangible IP, they risk broader disclosure in the community (and therefore possible financial loss from the 'secret' becoming public knowledge). If victims choose to minimise the risk by not reporting the incident, they allow the offender to go unpunished. Ultimately, ongoing reluctance by owners of trade secrets to report this type of IP crime to a wider audience contributes to the attraction of this activity for organised crime.

There are two main ways these types of IP are compromised: through physical theft and through cybertheft – cybertheft having become the more common methodology.

76 Kirk, Ronald 2011, *2011 special 301 report*, Office of the United States Trade Representative, Washington DC.
77 Twomey, P 2010, 'Cyber security threats', presentation to the Lowy Institute for International Policy, 8 September 2010.

Cyber-espionage and cybertheft targeted at IP and other trade secrets is a growing problem. This method of stealing or accessing trade secrets is likely to increase as the movement of IP between companies and countries becomes more common with ongoing globalisation. It is probable that cyberthieves will move beyond hacking for credit card and other personal details and increasingly target IP such as trade secrets.[78] An example of this could be the theft of simple designs that can then be used with emerging technology such as 3D printers to make the designed product.

Cyber attacks are an increasing threat to a company's capabilities and competitiveness in the marketplace because of the ongoing use of technology to store and transmit information, including trade secrets and other IP. Corporate brands are already under attack and US companies are known to have lost billions of dollars worth of IP to cybercriminals.[79] It is unclear if the situation in Australia is similar. A failure to adequately respond to this threat could diminish industry confidence, and in turn national economies could be damaged.

Law enforcement will face increasing challenges in countering the threat posed by organised crime groups that are targeting trade secrets and other forms of IP. Cybercrime groups are often assessed as being loosely structured and flexible, coalescing for short periods to conduct specific tasks. However, some groups from Eastern Europe are well organised and involved in numerous crime types. Moreover, research is demonstrating the emergence of a mature, service-based economy for computer hacking that can derive profit from online IP theft,[80] including theft of trade secrets.

As economies around the world transition to being knowledge-based, it is likely that there will be an increase in State actors' involvement in accessing IP trade secrets. This is already occurring. For example, in April 2010 it was alleged that three major Australian mining companies were targeted by Chinese hackers soon after four employees of Rio Tinto were arrested in China for alleged offences against Chinese business interests.[81]

FIREARM TRAFFICKING

Australia has a growing pool of firearms that can be accessed by criminals. The durability of firearms ensures that those diverted to the illicit market remain in circulation and available for use by criminals for many decades. They can be traded, sold and moved around over a period of years both within and between jurisdictions. This can complicate the process of 'tracing' a firearm to its original source or owner in the event that it is seized by law enforcement.

78 McAfee, Inc. 2009, *Unsecured economies: protecting vital information*, McAfee, Inc., Santa Clara, p. 18.
79 Twomey, P 2010, 'Cyber security threats', presentation to the Lowy Institute for International Policy, 8 September 2010.
80 Picarelli, JT 2010, *Expert Working Group report on international organized crime*, US Department of Justice Discussion Paper, US Department of Justice, Washington DC, p. 18.
81 ABC Reports, *Rio, BHP, Fortescue hit by Chinese computer hackers*, viewed 18 January 2011, <http://chinadigitaltimes.net/2010/04>.

The illicit firearm market (which incorporates both the black and grey markets) comprises any firearm that has been diverted from the licit market, illegally imported into Australia or illegally manufactured.

- *Black market:* the black market comprises any firearm illicitly obtained by individuals and criminal entities. When obtained by organised crime groups, a black market firearm will almost certainly be intended to assist in the commission of crime.
- *Grey market:* the grey market consists of all long-arms that were not registered, or surrendered as required during the gun buybacks, following the National Firearms Agreement (1996). An unregistered firearm is an illegal firearm. Grey market firearms may end up in the illicit market.[82]

In addition to the demand from organised crime, some demand for illicit firearms comes from lower-level criminal individuals – for example, members of street-level gangs – as well as from firearm enthusiasts. Lower-level criminals use illicit firearms for self-protection, protection of assets and enabling of other crime types, and to enhance their perceived image. Firearm enthusiasts, on the other hand, may turn to the illicit market in search of rare or specialised items not readily available through legitimate channels.

Although there are a disparate range of participants involved, Australia's illicit firearm market is facilitated mostly by trade among criminal groups, along with a small number of corrupt licensed firearm dealers, licensed firearm owners and 'backyard manufacturers'. These entities deal in stolen or lost, illegally diverted, owned or imported, modified and manufactured firearms, as well as grey market firearms.

There are a number of ways in which firearms have been and are diverted to the illicit market, including reactivation of deactivated firearms, historical legislative and regulatory loopholes, and interstate transfers. However, theft remains one of the primary methods of diverting firearms from the licit to the illicit market. An average 1,545 firearms[83] per annum were reported stolen to Australian state and territory police during the period 2004–05 to 2008–09.[84]

Although the majority of illicit long-arms in Australia are sourced from the grey market, there is evidence that other long-arms, and illicit handguns, are sourced from firearms illegally imported from overseas, as well as firearms that are illegally manufactured in Australia. In some cases, these activities are combined and firearm components (for example, trigger mechanisms) are imported and used in domestic manufacture of an illicit firearm. Though the domestic manufacture of illicit firearms has been occurring in Australia for a number of decades, it is a niche segment of the overall market (see case study on page 47).

An emerging trend in the firearm market is the use of online (Internet-based) sites to trade firearms and associated parts, including 'hidden' websites concealed in online networks — sometimes referred to as 'darknets'. Given the increasing popularity of online trading platforms, it is possible that this will soon become a larger-scale activity in Australia.

82 Bricknell, Samantha 2012, *Firearm trafficking and serious and organised crime gangs*, Australian Institute of Criminology, Canberra, p. x.

83 Because of non-reporting, this figure is likely to underestimate the actual number of firearms stolen. Not all stolen firearms are reported to police, particularly if the victim is in unlicensed possession of an unregistered firearm or has not adhered to prescribed storage requirements.

84 Bricknell, Samantha 2011, *Firearm theft in Australia 2008–09*, Australian Institute of Criminology, Canberra, p. iii.

AUSTRALIAN CUSTOMS AND BORDER PROTECTION SERVICE DETECTS AND SEIZES FIREARM PARTS AT THE BORDER

In July 2011, Australian Customs and Border Protection Service officers in Queensland successfully prosecuted two men in separate incidents for attempting to illegally import firearm parts into Australia. In the first incident, a 43-year-old Brisbane man was charged with offences relating to the attempted importation of parts of an Uzi sub-machine gun. After the seizure, a search of the man's home located more firearm parts and dangerous weapons. The man appeared in the Brisbane Magistrates Court on 7 July 2011, where he was convicted of five charges and received an $8,500 fine plus costs.

In the second incident, a 51-year-old Gympie man was charged with offences relating to the attempted importation of four parcels containing handgun parts. The handgun parts were concealed in a number of objects, including scales and an electronic voltage regulator. The man appeared in the Gympie Magistrates Court on 7 July 2011, where he was convicted for importing handgun parts and fined $4,000.

ENVIRONMENTAL CRIME

Australia is identified as a biodiversity hotspot,[85] with many unique species of flora and fauna. Demand for such unique flora and fauna positions Australia as a source country for illegal trafficking.[86]

The environmental crime market in Australia remains a niche illicit market. Individuals and groups from within the wildlife/pet industry, along with private collectors, remain prominent in the trafficking of wildlife into and out of Australia. Legitimate businesses within the wildlife industry can be used to mask illegal activity, with illegally poached wildlife changing hands accompanied by false documents listing them as captive breeds.

The illegal wildlife trade is driven by supply and demand from local and international collectors of native wildlife. Networks within Australia that are involved in illegal wildlife trading appear consistent with international networks, and include opportunistic traders, complex trade chains made up of suppliers, poachers, couriers and collectors, and entrenched criminal syndicates.

The Internet provides the illegal trade in wildlife with an unregulated and anonymous marketplace that connects suppliers and collectors from around the world. As part of a 2008 International Fund for Animal Welfare (IFAW) investigation,[87] exotic birds were found to be the most prevalent wildlife offered for sale on Australian websites, with the majority of animals listed on eBay (43 per cent) and Australian Pet Link[88] (28 per cent). The most common mode of transporting illegal wildlife is through the postal system.[89]

Apart from the illicit trade in wildlife, there is also a large global market in illegally logged timber. It has been estimated that 22 per cent of wooden furniture and 14 per cent of miscellaneous wooden items were made using timber of suspicious origin.[90] In contrast to the illegal wildlife trade, in which Australia is a source country, Australia remains a destination country for illegal timber.[91]

The United Nations Office on Drugs and Crime has identified environmental crime as an emerging international crime problem, with organised criminal groups and individuals attracted by increasing demand and financial incentives. In recognition of the detrimental effect that this crime has on human health, the environment and global biodiversity, five intergovernmental organisations have recently formed the International Consortium to Combat Wildlife Crime (ICCWC).[92]

Increased recognition of criminal activities within the Australian environmental crime market has led to tighter regulations, but difficulties in detecting these activities mean that the market continues as one of low risk – high reward for those involved.

85 Alacs, E & Georges, A 2008, 'Wildlife across our borders: a review of the illegal trade in Australia', *Australian Journal of Forensic Sciences*, vol. 40, no. 2, pp. 147–60.

86 For example, a breeding pair of native geckos can return the supplier up to A$1,200 within Australia and a higher amount if sold to overseas markets.

87 International Fund for Animal Welfare 2008, *Killing with keystrokes: an investigation of the illegal wildlife trade on the World Wide Web*, IFAW, Yarmouth Port, Massachusetts.

88 Australian Pet Link is a website with classified advertisements and information resources on pets in Australia.

89 Bricknell, S 2010, *Environmental crime in Australia*, Research and Public Policy Series no. 109, Australian Institute of Criminology, Canberra; Dore, M 2009, *The illegal trade in wildlife across the Australian border*, ACBPS, Canberra.

90 Bricknell, S 2010, *Environmental crime in Australia*, Research and Public Policy Series no. 109, Australian Institute of Criminology, Canberra. Illegal logging, in its narrowest sense, involves the taking of protected tree species, taking of timber from protected areas or outside authorised concessions, and taking timber in excess of specified quotas.

91 Australian Institute of Criminology n.d., *Environmental crime: illegal logging and timber trade*, <http://www.aic.gov.au/crime_types/environmental/illegal%20logging.aspx>.

92 Organisations include CITES, INTERPOL, the UNODC, the World Bank and the World Customs Organization.

CRIMES IN THE MAINSTREAM ECONOMY

CARD FRAUD

Card fraud is defined as the fraudulent acquisition and/or use of debit and credit cards, or card details, for financial gain. Card fraud may involve acquiring legitimate cards from financial institutions by using false supporting documentation (application fraud), or stealing legitimate credit and debit cards. It may also involve phishing,[93] card-not-present fraud, the creation of counterfeit cards, hacking into company databases to steal customer financial data, and card skimming.

In Australia, as in many other developed nations, there has been an increase in the use of credit and debit cards as a method of payment for goods and services, including over the Internet. Although this increase has provided greater convenience for consumers, it has been accompanied by higher levels of fraud and theft of funds in relation to electronic transactions.

Payment fraud statistics compiled by the Australian Payments Clearing Association (APCA), the payments industry self-regulatory body, indicate that, from July 2010 to June 2012, the total number of card fraud transactions on Australian-issued cards both in Australia and overseas increased by 26 per cent, with the value of these fraudulent transactions increasing by 25 per cent over the same period to A$262 million.[94]

93 Phishing refers to attempts to obtain sensitive personal and banking information (such as bank account numbers, passwords and credit card numbers) to be used for criminal gain. Criminals send emails making false claims in order to trick users into revealing personal details, or establish fake websites, with links sent through electronic communication including email, instant messaging, texts and online advertising.

94 Australian Payments Clearing Association 2012, 'Fraud statistics: 1 July 2011 – 30 June 2012', APCA, Sydney; Australian Payments Clearing Association 2011, 'Payment fraud statistics: 1 July 2010 – 30 June 2011', APCA, Sydney.

Notably, APCA statistics show that card-not-present fraud – the use of account information without the physical card being involved, typically through phone, mail or Internet, and without the authority of the cardholder – has increased significantly, with the number of fraudulent transactions increasing from July 2010 to June 2012 by 26 per cent. Card-not-present fraud currently accounts for 78 per cent of the reported fraudulent transactions on Australian-issued cards.[95] Much of this fraud occurs when criminal groups use stolen credit card data to purchase goods through the Internet from retailers overseas.

The increase in card-not-present fraud is likely to be the result of a confluence of factors such as improved security measures to prevent point-of-sale fraud – including the introduction of personal identification number (PIN) and chip technology – the displacement of organised crime groups previously involved in large-scale card skimming, and a continual increase in online spending by Australians.

The introduction of PIN and chip technology in Australia has reduced the opportunities for organised crime groups to engage in fraudulent credit card transactions at the point of sale where the card being used to make the purchase is physically present. This is because a card's unique chip is used to verify the transaction details, rather than the magnetic stripe. Although the banking sector is moving toward the use of PIN and chip technology for all Australian-issued cards, the replacement of all non-chip cards may take several years to complete.

Overseas-based organised crime groups continue to target Australia for card fraud, with Asian and Romanian card skimming syndicates having recently received coverage in the media. Some of these syndicates are involved in activity in multiple crime markets, with the funds obtained from card fraud being used to support other lines of illicit business (see case study on page 51).

The existence of black market web portals – underground forums set up by criminals to openly trade in a range of illicit commodities, including stolen banking details – allows organised crime groups to purchase credit card numbers for less than A$1 each if bought in bulk. Further details such as cardholder name and expiry date can be purchased for about A$7, and full card details, including identity data, can be bought for between A$70 and A$80.[96] The ability to purchase and trade sensitive card data and customer information through the Internet is almost certain to enable organised criminal involvement in card-not-present fraud, and may also contribute to identity fraud in instances where full identity details are purchased.

The introduction of 'smartphone' applications such as 'Google Wallet' may also create opportunities for criminal groups involved in card fraud, with card data being compromised and used unlawfully in instances where a smartphone is lost or stolen.

95 Australian Payments Clearing Association 2012, 'Fraud statistics: 1 July 2011 – 30 June 2012', APCA, Sydney.

96 Commonwealth of Australia 2010, Official Committee Hansard: House of Representatives – *Standing Committee on Communications*, 17 March 2010, Canberra.

ROMANIAN CRIME SYNDICATE A$30 MILLION CARD FRAUD

In November 2012, 16 members of a Romanian crime syndicate were arrested in a joint Australian Federal Police and Romanian National Police operation in Romania. The syndicate exploited weaknesses in the security systems of 100 Australian small businesses, which were hacked to steal the credit card details of up to 500,000 Australians who had used their cards at the businesses to buy goods or services.

Though investigators have not been able to establish exactly how many card details were stolen from the Australian businesses, 30,000 of them had, at that time, already been used to illegally buy goods worth more than $30 million.

The stolen credit card data was allegedly used to create fake credit cards, enabling thousands of counterfeit transactions to be carried out around the world, including in Europe, Hong Kong, Australia and the United States.

MASS MARKETED FRAUD

Mass marketed fraud refers to fraudulent schemes or 'scams' delivered via mass communication methods, such as the telephone, mail (including email) and the Internet (including social networking sites, chat-rooms and online dating services). The contact is unsolicited or uninvited, and false claims are made to con the victim out of money.

Australia is an attractive target for overseas-based criminals involved in mass marketed fraud as it has a relatively affluent population (offering high profits for organised crime) and a large number of people connected to the Internet (providing a substantial pool of possible victims). In Australia, the two key forms of mass marketed fraud are investment fraud and advance fee fraud.

INVESTMENT FRAUD

Fraudulent investment schemes, such as boiler-room frauds and Ponzi schemes,[97] attract victims based on promises of high financial returns and claims of low risk investment strategies. Investment fraud causes significant harm to victims.

Victims of boiler-room fraud are most often encouraged to buy shares in a fictitious company or product, which is fraudulently represented as legitimate, with the revenue from this activity misappropriated or diverted by the fraud operators. These schemes attract all forms of investors and do not prey solely on those with limited financial knowledge or experience. Recent ACC research indicates that the typical profile of a victim of boiler-room fraud is a self-employed male, aged (on average) 54 years, and educated to tertiary or secondary school level.

Fraud perpetrators targeting Australia have traditionally implemented well-planned and sophisticated schemes that provide criminal individuals and organised crime groups with high-profit returns in a short period of time. They spruik the schemes to potential victims using a range of techniques, including cold-calling, email communications and Internet websites. In some cases, Internet sites promoting these schemes will contain links to fraudulent government and/or regulatory agency websites. This is intended to make the scheme appear legitimate to prospective investors.

Organised crime groups are known to have exploited commercially available 'leads lists' to identify potential victims for sophisticated boiler-room schemes. Leads lists – lists containing the personal details of people who have, for example, filled out retail surveys or signed up to loyalty programs – are sold commercially to legitimate businesses seeking 'leads' for their marketing strategies, but can also be purchased by organised crime groups that are seeking these details to exploit for illegal purposes. This highlights the importance for Australians of being aware of what is done with the details that they provide to businesses from which they purchase goods or services.

97 A type of fraud that uses money from new investors to make interest payments to earlier investors. The schemes typically offer high rates of return and fall apart when no new investors can be found.

Investment fraud is an area of particular concern to law enforcement, as the incidence of this type of fraud appears to be increasing, and the harm that it causes to Australians is significant. There are also indications that organised criminal groups who have formerly been involved in other illicit markets, such as drugs, are being attracted to investment fraud because of the high profits to be made and the perceived low risk of detection and prosecution.

Notably, in addition to boiler-room fraud and Ponzi schemes, there is evidence that some stockbrokers and financial advisers have received substantial commissions from sophisticated organised fraudsters for promoting fraudulent investment schemes to their clients. This problem of trusted financial advisers being paid very large commissions to promote schemes later identified as frauds was identified by the Parliamentary Joint Committee on Corporations and Financial Services Inquiry into the collapse of Trio Capital – the largest superannuation fraud in Australian history. Although the Australian Securities and Investments Commission (ASIC) has taken steps to remedy the problem in the form of very recent reforms to the Corporations Act to deal with 'conflicted remuneration'[98] for financial advisers, organised criminal involvement in investment fraud requires the ongoing attention of law enforcement.

ADVANCE FEE FRAUD

The term 'advance fee fraud' (AFF) refers to any fraud that involves the payment of fees upfront for goods, services or rewards that are never supplied. This includes dating and romance scams (including adult services), lottery and sweepstake fraud and unexpected prize fraud. These are sometimes also referred to as Nigerian or West African scams. Advance fee fraud has been significantly enabled by the reach of modern Internet and telecommunications technology, making it easier and cheaper to reach victims all over the world.

According to the Australian Competition and Consumer Commission (ACCC), in 2011, for the third consecutive year, mass marketed advance fee fraud recorded the highest number of scam reports, contributing more than half (44,233) of the incidents reported to the ACCC,[99] with total reported losses of A$55 million.[100] These figures represent the reported incidence and losses associated with AFF, which are likely to be significantly under-reported.

The ACCC reports a shift in the preferred mode of scam delivery from online methods, including Internet and email, to unsolicited telephone calls, with almost 52 per cent of scams reported in 2011 delivered by phone. The rise in unsolicited telephone calls is likely to be associated with the increasing use of voice over Internet protocol (VoIP) services, which allow users to make low-cost or free domestic and international telephone calls over the Internet.

98 ASIC released Regulatory Guide 246 regarding conflicted remuneration in March 2013, banning 'many benefits given to those persons who provide financial product advice to retail clients that could reasonably be expected to influence the financial product advice they give'.

99 Australian Competition and Consumer Commission 2012, *Targeting scams: report of the ACCC on scam activity 2011*, ACCC, Canberra.

100 This includes losses from advance fee/upfront payment, dating and romance (including adult services), lottery and sweepstakes and unexpected prizes scams.

Almost all AFF activity that affects Australia originates from overseas, emanating mainly from West Africa, Europe and, to a lesser extent, North America. Fraud perpetrators use a variety of techniques to identify possible victims. In some cases they trawl the Internet for personal identity information – such as name, home address and email contact details – recorded on social networking sites such as Facebook and MySpace. In other cases, victims have been identified by fraud perpetrators using information recorded on commercially available leads lists.

Organised crime groups responsible for AFF are innovative and adaptable, with new scams constantly emerging.

REVENUE AND TAX FRAUD

Organised criminal groups and significant criminal individuals based in Australia and overseas are exploiting Australia's tax system, primarily through fraudulent refund activity. However, the information and intelligence currently available indicate that the level of traditional organised crime involvement in revenue and tax fraud is low. Those involved in this crime type display varying levels of expertise and sophistication, often matched to the complexity of the fraud committed, and increasingly rely on technology to support their activities.

Revenue and tax fraud by organised criminals is often enabled by a myriad of complex business and trust structures and professional facilitators, such as tax agents, accountants and legal experts – some of whom may be complicit in the fraud. Identity crime is also used to enable this type of fraud. The creation of 'corporate vehicles' such as companies or trusts in secrecy jurisdictions[101] by professional facilitators allows organised crime to conceal the beneficial ownership of those companies, as well as masking the true purpose behind the establishment of the companies.

In relation to refund fraud, some of the methods identified as being used by organised crime are:

- deliberate falsification or overclaiming of input tax credits, deductions, offsets or expenses
- failure to declare income where there is an obligation to do so – which can lead to the payment of a higher refund
- the use of false information or identity details to claim a refund
- using stolen, purchased or fabricated proof of identity documents to obtain a tax file number (TFN) or GST registration in a real or false name
- theft, purchase or borrowing of another person's TFN and/or Australian business number (ABN) to lodge fraudulent claims using a third-party identity.

The Australian Tax Office uses a range of analytical models and tools to assist in the detection of fraud within the taxation environment. As the ATO's understanding of criminal behaviour and tax evasion methodologies expands, these models and tools are adjusted accordingly. The ATO also works in concert with law enforcement and government under the auspices of Project Wickenby to investigate suspected tax fraud and money laundering activities undertaken by Australian residents, some of whom are criminal individuals.

101 Secrecy jurisdictions are those jurisdictions in which legislation governing the banking and finance sector is intended to protect the privacy of those incorporating companies in that jurisdiction.

ILLEGAL TOBACCO

Involvement in Australia's illegal tobacco market is perceived by organised crime groups as a low risk, high profit activity: they see it as a market in which large profits can be made with minimal risk of detection or significant penalties. Organised crime has sustained access to cheap tobacco product overseas, which can be illegally imported, avoiding tax obligations, to supply the illegal tobacco market in Australia. Many of those involved in illegal tobacco importations are also involved in other illicit markets, such as drugs. Minimal quantities of illegal tobacco are produced domestically.

Traditionally, the illegal tobacco market has been dominated by unbranded tobacco product, more commonly known as 'chop chop'. The product is normally sold in loose-leaf form in half-kilogram and one-kilogram lots, usually in clear plastic bags without the health warnings carried by legitimate tobacco products. In recent years, however, the ACBPS has reported an increase in the seizure of illegal tobacco in the form of cigarettes, and a decrease in the seizure of illegal loose-leaf tobacco.[102] Given the variability in detections of illicit tobacco, future years' statistics will need to be monitored to identify whether this represents a trend.

In the 2011–12 financial year, the ACBPS detected and seized 46 sea cargo importations of illegal tobacco, comprising a combined 175 tonnes of tobacco and 122 million cigarettes. The duty evaded on these importations was A$128 million. A significant recent seizure of illegal tobacco in Australia was that made under Operation Polaris in September 2011. The ACBPS continues to make regular detections of illegal cigarettes and loose-leaf tobacco (see case study on page 56).

As a deterrent to illegal tobacco smuggling, the ACBPS recently pursued legislative changes to increase the penalties available for tobacco smuggling under the *Customs Act 1901*, including the option of jail terms of up to ten years. These changes came into effect in November 2012.

SUPERANNUATION FRAUD

Recent law enforcement activity and intelligence gathering suggests that organised criminal involvement in superannuation fraud in Australia may be more significant than previously thought. Traditionally, the greatest threat to superannuation savings was believed to have come from opportunistic individuals involved in the operation or administration of funds, such as employees and service providers. Now well-resourced and sophisticated international organised fraud networks and groups have been known to actively target the Australian superannuation sector, drawn by the very large pool of compulsory superannuation savings currently amassed.

102 Australian Customs and Border Protection Service 2012, *Annual report 2011–12*, ACBPS, Canberra.

OPERATION POLARIS SEIZURE OF OVER 60 TONNES OF ILLEGAL TOBACCO

In September 2011, members of Operation Polaris – a joint waterfront operation comprising the NSW Police Force, Australian Federal Police, Australian Customs and Border Protection Service, Australian Crime Commission and NSW Crime Commission – arrested and charged three men after the seizure of more than 60 tonnes of illegal tobacco and almost 25 million counterfeit cigarettes that were illegally imported into Sydney. The illegal imports had the potential to defraud the Australian Government of more than A$35 million in revenue.

It is alleged that those importing the tobacco attempted to bribe a Commonwealth official. As a result of this attempted bribe, the official reported the matter to authorities, who launched a multi-agency investigation. After their arrest, the men were charged with offences relating to bribery of a Commonwealth official, dealing in proceeds of crime, and obtaining financial advantage by deception.[1]

1 Australian Federal Police 2011, *Polaris arrests two men and seizes more than 60 tonnes of illegal tobacco*, media release, September 2011, viewed 2 February 2012, <http://www.afp.gov.au/media-centre/news/afp/2011/september/Polaris-arrests-two-men-and-seizes-more-than-60-tonnes-of-illegal-tobacco.aspx>.

In the Australian Government Budget 2012–13, superannuation assets in Australia at the end of 2010–11 were cited as 'around $1.3 trillion, or about 95 per cent of annual GDP'. Notably, the same document stated that 'superannuation assets are projected to rise to almost $7 trillion (130 per cent of GDP) over the next 25 years'.[103] Given the very large amounts of money involved, organised criminal targeting of the superannuation sector can have significant impacts on Australian superannuants, the government and the economy. Consequently, addressing organised criminal exploitation of the superannuation industry is a priority for law enforcement.

The Australian superannuation pool is composed of funds invested in professionally managed superannuation funds (including industry superannuation funds, employer-managed funds, public sector funds and retail funds) and self-managed superannuation funds (SMSFs). The Australian Prudential Regulatory Authority (APRA) has responsibility for supervising regulated professionally managed superannuation funds, while the Australian Tax Office has responsibility for regulating SMSFs. Organised crime has been identified exploiting both professionally managed superannuation funds and SMSFs.

The collapse of Trio Capital – which has been described as the largest superannuation fraud in Australian history – illustrates the way in which highly sophisticated and well-funded organised crime can go about targeting the Australian superannuation sector. Trio Capital was the 'responsible entity' for two managed investment schemes – the Astarra Strategic Fund and the ARP Growth Fund – in which nearly 6,090 Australian investors lost a cumulative A$122 million in superannuation, managed and individual investments. Those who lost superannuation savings had invested in Trio through APRA-regulated funds, and through SMSFs (see case study on page 58).

With regard to SMSFs, organised crime has been identified as being involved in the promotion and facilitation of illegal 'early release schemes', offering often vulnerable members of the community quick and easy access to retirement savings – frequently in exchange for large commissions. Individuals who manage their own SMSFs, and who do not have extensive experience in the investment market, can also be vulnerable to fraudulent investment schemes established and promoted by organised crime.

Recent changes in the regulatory and legislative environment, such as those arising from the 2010 Cooper Review of Australia's superannuation system, and the implementation of the Future of Financial Advice (FOFA) Legislation, have sought to address identified vulnerabilities within the Australian superannuation sector, and to offer better protections to investors. However, organised crime – and, in particular, organised crime involved in frauds such as the Trio Capital fraud – has access to very specialised professional advisers (including legal advisers) who monitor changes in the environment, and develop strategies and schemes aimed at targeting remaining vulnerabilities in the sector.

103 Australian Government Budget 2012–13, Budget Paper, Canberra, viewed 11 March 2013, <http://www.budget.gov.au/2012-13/content/bp1/html/bp1_bst4-03.htm>.

TRIO CAPITAL

According to the Parliamentary Joint Committee on Corporations and Financial Services Inquiry into the collapse of Trio Capital, the fraud commenced in 2003 with the purchase of an existing reputable funds manager, Tolhurst Funds Management, by a group of organised fraudsters. The group are reputed to have paid nearly A$2 million for Tolhurst in two part-payments. The purchase is alleged to have been made 'with a view to defrauding Australian investors (particularly superannuation investors) of substantial sums of money'. The fraudsters changed the name of Tolhurst and, over the following six years, moved significant amounts of Australian investors' money into hedge funds based in overseas jurisdictions, including St Luca and Anguilla, and understood to be controlled by Thailand-based American national Jack Flader. A key part of their strategy was the payment of large commissions to financial advisers to promote their schemes. The fraud was exposed in September 2009 after an ASIC surveillance and after a Sydney-based finance executive had written to the Chairman of ASIC expressing his concerns with regard to the legitimacy of the Trio Capital–operated Astarra Strategic Fund.

FINANCIAL MARKET FRAUD

Financial market fraud, in the context of this report, refers collectively to the following activities as they impact on Australians:

- securities and share market fraud (manipulation or exploitation of the legitimate share market, rather than the 'boiler-room' fraud and Ponzi schemes dealt with in the earlier section 'Mass marketed fraud')
- mortgage and loan fraud.

SECURITIES AND SHARE MARKET FRAUD

As of 2010, approximately 7.26 million Australians – or 45 per cent of the adult population – owned shares,[104] with the trend to share ownership increasing. Although criminal manipulation and exploitation of the share market in Australia may have very significant effects on the economy, the fact that almost half of the Australian adult population own shares serves to highlight the potential for the harm caused by organised criminal activity in this sector to resonate throughout the Australian community.

Organised crime is motivated to manipulate or exploit the securities and share market by the potential for significant financial gain. Notably, organised criminal involvement in this type of fraud is typically sophisticated and high-level, as significant capital is often required to implement the schemes from which profits are derived. This capital is obtained from prior criminal activity, such as previous frauds, or trafficking in illicit commodities. Some methodologies employed by organised crime are:

- *Share ramping schemes* – establishing a 'start-up' company and making fraudulent claims (for example, that the company has discovered rich mineral deposits). Supported by reports produced by complicit geologists, the company is listed on the ASX and heavily promoted. Investors, believing the claims to be true, buy shares at a price commensurate with the projected value of the company. Once the share price has been sufficiently 'ramped', the criminals sell their shares in the company for a significant profit. The company then inevitably collapses, leaving investors with worthless shares.
- *Takeover schemes* – involving taking over an existing legitimate listed company (either by intimidation or through purchasing enough shares to achieve a controlling influence) and then launching aggressive marketing and capital raising campaigns based on fraudulent claims. A network of brokers (sometimes both domestic and international) are paid substantial commissions to promote the shares. The criminals then divert invested money offshore for personal use, or sell their shares at the height of their value, leaving the company to collapse.

104 Australian Stock Exchange 2011, *2010 Australian share ownership study*, ASX, Sydney.

Organised crime also uses the stock market to launder illicit funds, with investment in shares in legitimate Australian listed companies made through a complex web of offshore-based 'front' companies, of which criminal entities are the ultimate beneficiaries. This allows organised crime to hide its interests, and to move any profits from share dividends offshore, avoiding Australian tax.

MORTGAGE AND LOAN FRAUD

There is also evidence of recent organised criminal involvement in mortgage and loan fraud in Australia, with organised crime groups using false documentation, stolen or fraudulent identities and trusted insiders with experience in the banking or real-estate sectors to commit sophisticated and large-scale fraud against Australian victims and lending institutions.

In some instances, the identities of homeowners have been stolen by organised crime groups and used to acquire high-value loans, with the property or other assets as security. Often, victims do not realise what has happened until they are contacted by a financial institution with late payment or final demand notices in respect of the loan. Fraud perpetrators have also previously used the names of recent immigrants and the elderly to obtain fraudulent loans, resulting in millions of dollars worth of costs to the finance sector each year,105 in addition to the stress caused to victims.

105 Keane, A 2010, 'Mortgage fraudsters target recent migrants and the elderly', *Daily Telegraph*, 26 July 2010.

CRIMES AGAINST THE PERSON

Crimes against the person include human trafficking, maritime people smuggling and child sex offences.

HUMAN TRAFFICKING

Human trafficking is the physical movement of people across and within borders through deception, coercion or force for the purpose of exploitation at their destination. It is a different crime from people smuggling, which is the organised unlawful movement of people across borders, usually on a payment-for-service basis.[106]

The clandestine nature of human trafficking, along with probable high levels of under-reporting, means that there is little reliable data about the nature and extent of human trafficking at a global, regional or domestic level. However, there is general consensus that people trafficking affects almost every country in the world, whether as a source, transit or destination country, or any combination of these.[107]

Australia is still a destination country for victims of trafficking, particularly from Thailand, Malaysia, the Philippines and the Republic of Korea. To date, the majority of victims identified by Australian authorities have been women working in the sex industry (in both legal and illegal brothels). However, authorities are increasingly identifying male and female victims trafficked for other forms of labour exploitation, including in the agricultural, construction and hospitality industries.[108]

106 Australian Government 2012, *Trafficking in persons – the Australian Government response, 1 July 2011 – 30 June 2012: the fourth report of the Anti-People Trafficking Interdepartmental Committee*, Australian Government, Canberra.
107 ibid.
108 ibid.

In Australia, the extent of organised crime in the labour hire industry has not been assessed. However, recent research has indicated that labour trafficking exists in a broader context of exploitation of migrant workers, particularly those in low-skilled professions. In 2010, those perceived to be at greatest risk of exploitation were vulnerable migrant workers. These were most commonly encountered on 457 visas relating to semi-skilled occupations,[109] and among migrants working in the agricultural sector or as domestic workers, international students and those working in the maritime/seafaring sector.[110]

MARITIME PEOPLE SMUGGLING

The United Nations High Commissioner for Refugees (UNHCR) reported that, at the end of 2011, there were 42.5 million forcibly displaced people worldwide, including 26.4 million internally displaced people[111] as the result of conflict.[112] These internally displaced people are targets for people smugglers worldwide. Maritime people smuggling is often just one stage of a larger journey also involving land and air movements. Although it is the most dangerous form of smuggling for the migrants concerned, there are some groups of migrants who see it as the best, or possibly only, option available.[113]

Some displaced persons reportedly perceive Australia to be an attractive destination country because of its geographic location and positive economic, political and social environment. This is reflected in the significant increase in detections of people attempting to enter Australia by boat in the past few years. People who arrive by boat and seek asylum are referred to as irregular maritime arrivals (IMAs). In addition to maritime arrivals, some people enter Australia by air on a valid visa (such as a tourist or student visa) and then seek asylum. These people are referred to as non-IMA asylum seekers.

In 2008–09, Australian authorities intercepted 23 suspected illegal entry vessels (SIEVs) with 985 IMAs onboard.[114] In 2011–12, this figure had increased to 111 SIEVs carrying 8,092 IMAs (see Table 2).[115] The only comparable time for this number and tempo of boat arrivals was more than a decade ago, when 12,176 people arrived on 180 vessels between 1999 and 2001.[116]

109 The Subclass 457 visa program enables employers to fill short- to medium-term skill shortages by recruiting (sponsoring) qualified overseas workers where they cannot find appropriately skilled Australians. Sponsors must adhere to a set of legal obligations, which include paying Subclass 457 visa holders market salary rates. Subclass 457 visas are generally valid for four years.

110 David, F 2010, *Labour trafficking*, Research and Public Policy Series no. 108, Australian Institute of Criminology, Canberra.

111 For the purposes of United Nations statistics, internally displaced persons are people or groups of individuals who have been forced to leave their homes or places of habitual residence as a result of armed conflict and who have not crossed an international border.

112 United Nations High Commissioner for Refugees 2012, *UNHCR global trends 2011* (online), viewed 21 December 2012, <http://www.unhcr.org/4fd6f87f9.pdf>.

113 Expert Panel on Asylum Seekers 2012, *Report of the Expert Panel on Asylum Seekers*, Australian Government, Canberra.

114 Australian Customs and Border Protection Service 2011, *Annual report 2010–11*, ACBPS, Canberra.

115 Australian Customs and Border Protection Service 2012, *Annual report 2011–12*, ACBPS, Canberra.

116 Expert Panel on Asylum Seekers 2012, *Report of the Expert Panel on Asylum Seekers*, Australian Government, Canberra.

TABLE 2: DETECTIONS OF SIEVS AND IMAS, 2008–09 TO 2011–12[117]

	2008–09	2009–10	2010–11	2011–12
Number of SIEVs	23	117	89	111
Number of IMAs	985	5,327	4,750	8,092

Irregular maritime arrivals to Australia are dominated by a few key nationalities – Afghani, Iranian, Iraqi, Pakistani and Sri Lankan nationals, or those who are stateless (see Table 3).[118]

TABLE 3: NUMBER OF IMA REFUGEE STATUS DETERMINATION REQUESTS RECEIVED, BY TOP FIVE COUNTRIES OF CITIZENSHIP[119]

	2008–09	2009–10	2010–11	2011–12
Afghanistan	528	2,642	1,621	3,179
Iran	13	198	1,563	1,553
Sri Lanka	33	907	359	825
Pakistan	3	17	70	618
Stateless	25	460	854	576
Other	66	355	707	628
Total	668	4,579	5,174	7,379

People smuggling is both a regional and a global problem. People smugglers use highly organised international networks to make logistical arrangements for the travel of irregular migrants and typically demand exorbitant fees for their services. The impact of people smuggling extends beyond domestic law enforcement and border protection capability and dealing with it requires mutual cooperation and international engagement.

Although some ventures depart from Sri Lanka, as at August 2012 nearly all current irregular maritime arrivals had departed from Indonesia, generally as the final leg of a longer journey from the Middle East or South Asia.[120] The exact route taken may vary, but there are a number of well-established paths that people smugglers use to transport migrants from place to place, before they depart for Australia by boat (see Table 4). Alternatively, some migrants may make their own way to Indonesia and engage the services of people smugglers once there. Indonesia is generally used as a departure point because of its proximity to Australia. Most boats then head towards the Australian territories of Christmas Island or Ashmore Reef, rather than attempting to reach the Australian mainland.[121]

117 Adapted from Australian Customs and Border Protection Service 2012, *Annual report 2011–12*, ACBPS, Canberra; and Australian Customs and Border Protection Service 2011, *Annual report 2010–11*, ACBPS, Canberra.
118 Expert Panel on Asylum Seekers 2012, *Report of the Expert Panel on Asylum Seekers*, Australian Government, Canberra.
119 Top five countries of citizenship are based on 2011–12 data. Department of Immigration and Citizenship 2012, *Asylum trends – Australia: 2011–12 annual publication*, Department of Immigration and Citizenship, Canberra.
120 Expert Panel on Asylum Seekers 2012, *Report of the Expert Panel on Asylum Seekers*, Australian Government, Canberra.
121 United Nations Office on Drugs and Crime 2013, *Transnational organized crime in East Asia and the Pacific – a threat assessment*, UNODC, Vienna.

In an unusual occurrence, a SIEV carrying 66 Sri Lankan asylum seekers arrived undetected in the harbour at Geraldton in Western Australia in April 2013.

TABLE 4: TYPICAL ROUTES USED TO SMUGGLE PEOPLE TO AUSTRALIA[122]

Country of origin	Transit country 1	Transit country 2	Transit country 3
Afghanistan	Travel by bus or foot into Pakistan or Iran	Travel by air from Pakistan or Iran to Malaysia	Travel by bus, train or ferry to Indonesia, before departing by boat to Australia
Iran	Travel by air to Malaysia or Indonesia before departing by boat to Australia		
Iraq	Travel by air to Malaysia (may stop over in transit destinations such as Jordan or Iran)	Travel by air from Malaysia to Indonesia, before departing by boat for Australia	
Myanmar	Travel overland through Thailand to Malaysia.	Travel overland to Indonesia before departing by boat for Australia.	

Irregular maritime voyages are particularly dangerous. The growing frequency of attempted voyages to Australia has resulted in substantial loss of life at sea. Between October 2001 and June 2012, an estimated 964 people died (or are presumed to have died) while attempting to reach Australia by boat, 605 of them since October 2009.[123] For example, in 2001 more than 350 lives were lost in one incident when an unseaworthy vessel headed for Australia sank off the coast of Java, Indonesia, and in 2010 a vessel crashed onto rocks at Christmas Island, with the loss of 50 lives.[124]

People smugglers may use boats that are unseaworthy, sinking without the means for passengers (who may not have been provided with life vests) to signal for help.[125] Under international law, the master of a ship that receives information about persons in distress at sea, and is in a position to render assistance, must do so, regardless of the nationality or status of the persons in distress or the circumstances in which they are found.[126] A frequently reported modus operandi is for smugglers or migrants to force a rescue by sinking or scuttling intercepted boats to ensure that authorities assist the people on board.[127] An example of this happening in Australian waters occurred in 2009, when a boat carrying 47 Afghani asylum seekers and two Indonesian crew exploded off Ashmore Reef after being intercepted by the Royal Australian Navy.

122 ibid.
123 Expert Panel on Asylum Seekers 2012, *Report of the Expert Panel on Asylum Seekers*, Australian Government, Canberra.
124 United Nations Office on Drugs and Crime 2011, *Issue paper: smuggling of migrants by sea*, UNODC, Vienna.
125 ibid.
126 Expert Panel on Asylum Seekers 2012, *Report of the Expert Panel on Asylum Seekers*, Australian Government, Canberra.
127 United Nations Office on Drugs and Crime 2011, *Issue paper: smuggling of migrants by sea*, UNODC, Vienna.

The coroner investigating the incident found that the crew had intended to beach the vessel on the reef before it was intercepted, and that, after interception, the crew had deliberately sabotaged the engine by pouring salt in it and one or more passengers set the boat alight, as they mistakenly feared they were being returned to Indonesia.[128]

Under Australian policy, IMAs are compulsorily detained while health, identity and security checks are undertaken and their reasons for travel are determined.[129] Some IMAs may remain in detention centres, while others may be moved to community detention, or released into the community on bridging visas while their application for protection is assessed.[130] Non-IMA asylum seekers are not detained, provided they abide by the conditions of the visa on which they entered the country.

Between 2002–03 and 2007–08, IMAs comprised less than 5 per cent of applications for protection[131] in Australia. This increased to 11 per cent in 2008–09 and has been steadily increasing to 51 per cent in 2011–12.[132] However, protection visa grant rates are much higher for IMAs (almost 90 per cent[133]) compared with non-IMAs (around 50 per cent).[134]

CHILD SEX OFFENCES

Child sex offences encompass a range of offences such as child sexual assault, child sex tourism, child prostitution, the possession, distribution and production of child exploitation material and online offences. Child sex offences have a significant effect on the victim, including both physical and emotional harm. Victims of child sex offences (or their families) may develop serious social and mental health-related problems, which can have a flow-on effect for health and welfare services throughout the country, sometimes over extended periods of time.

The International Labour Organisation estimates that there are as many as 1.8 million children exploited in the commercial sex industry or pornography worldwide.[135] Since 2005, 850 offenders have been arrested by the Australian Federal Police for 1,123 charges relating to online child sexual exploitation.[136]

Police operations have continued to disrupt sophisticated online child exploitation material syndicates, including through improved use of computer programs to identify Internet protocol addresses of those accessing or sharing child exploitation material.

128 *Inquest into the death of Mohammed Hassan Ayubi, Muzafar Ali Seferali, Mohammed Amen Zamen, Awar Nadar, Baquer Husani [2010] NTMC 014* (online), viewed 10 April 2013, <http://www.nt.gov.au/justice/courtsupp/coroner/documents/D0061-D0063D0118-D0119Ashmore.pdf>.

129 Phillips, J & Spinks, H 2012*, Immigration detention in Australia,* Background Note, Parliamentary Library, 23 January 2012, viewed 13 March 2013, <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BN/2011-2012/Detention>.

130 Department of Immigration and Citizenship 2011, *Fact sheet 65 – Onshore processing arrangements for irregular maritime arrivals* (online), viewed 4 April 2013, <http://www.immi.gov.au/media/fact-sheets/65onshore-processing-irregular-maritime-arrivals.htm>.

131 These figures relate only to protection applications lodged by asylum seekers who have arrived in Australia. Applications for protection lodged by asylum seekers offshore are not included in the data.

132 Department of Immigration and Citizenship 2012, *Asylum trends – Australia: 2011–12 annual publication*, Department of Immigration and Citizenship, Canberra.

133 Expert Panel on Asylum Seekers 2012, *Report of the Expert Panel on Asylum Seekers*, Australian Government, Canberra, p. 27.

134 Department of Immigration and Citizenship 2012, *Asylum trends – Australia: 2011–12 annual publication*, Department of Immigration and Citizenship, Canberra.

135 ECPAT International n.d., ECPAT introduction brochure (online), viewed 14 March 2011, <http://www.ecpat.net/EI/EI_publications.asp>.

136 Australian Federal Police 2012, *National investigation disrupts child exploitation network*, media release (online), 23 March 2012, viewed 27 March 2012, <http://www.afp.gov.au/media-centre/news/afp/2012/march/national-investigation-disrupts-child-exploitation-network.aspx>.

THE OUTLOOK

COMBATING SERIOUS AND ORGANISED CRIME IN AUSTRALIA

As Australia's national criminal intelligence agency, the ACC plays a crucial role in developing responses to serious and organised crime through the production of a national intelligence picture of organised crime activities in Australia. This intelligence picture has formed a solid foundation for intervention and policy responses alike.

Organised crime has evolved well beyond a simple law and order problem within the remit of an individual agency, jurisdiction or country. Each year, businesses can lose millions in revenue from the exploitation of their brands, from hacking into their secure networks and from unfair competition from criminal enterprises using counterfeit materials or intellectual property. The social, economic, systemic, environmental, physical and psychological harms caused by serious and organised crime have a very real impact on the whole community.

SERIOUS AND ORGANISED CRIME: A THREAT TO NATIONAL SECURITY

Serious and organised crime is not only a threat to civic law and order and community safety; it is a threat to Australia's national security.

On 23 January 2013, the Australian Government launched Australia's first National Security Strategy, *Strong and secure: a strategy for Australia's national security*, which provides an overarching framework to guide Australia's security efforts over the next five years. The strategy recognises that preventing, detecting and disrupting serious and organised crime is one of the eight key pillars to securing the nation and its citizens, and identifies the following key features of Australia's approach to combating serious and organised crime:

- *Implementing the ACC-led National Criminal Intelligence Fusion Capability, which brings together specialists from a wide range of agencies to better prevent, disrupt, investigate and prosecute organised crime*.

By working collaboratively through the Fusion Capability, Australia's law enforcement community is developing a greater understanding of criminal targets, risks, threats and vulnerabilities than would otherwise be possible in isolation. Not only is this significantly augmenting Australia's intervention efforts, but it is also informing innovative prevention strategies to harden Australia against organised crime.

- *Working with the states and territories through the Commonwealth Organised Crime Strategic Framework and the National Organised Crime Response Plan to focus on key cross-jurisdictional threats*.

  The Organised Crime Strategic Framework was first launched in 2009 to drive an integrated and collaborative government approach to combating organised crime and set the strategic priorities for Australia's efforts against organised crime. It identifies five capabilities required to respond to organised crime:

  - intelligence, information sharing and interoperability
  - targeting the criminal economy
  - investigation, prosecution and offender management
  - preventative partnerships with industry and the community, and
  - international, domestic and Commonwealth partnerships.

  A recent evaluation of the Framework found that it has assisted key agencies in strategic planning, and has enhanced cooperation and information sharing between agencies. Greater collaboration has included harnessing the skills and tools of agencies not traditionally considered law enforcement agencies, such as the Australian Taxation Office and the Australian Transaction Reports and Analysis Centre.

  The Framework is underpinned by the National Organised Crime Response Plan 2010–13, which aims to strengthen collaborative responses to serious and organised crime between Commonwealth, state and territory governments. The Response Plan recognises that serious and organised criminals increasingly operate across jurisdictions, and that a nationally consistent approach is required to combat the threat. The Response Plan has led to key initiatives such as the development of the National Target Management Framework, which outlines processes for establishing and sharing organised crime priorities and targets, and establishment of the Serious and Organised Crime Coordination Committee (SOCCC).

  The SOCCC is a national law enforcement forum that aims to support the prioritisation, endorsement and coordination of operational strategies for dealing with multi-jurisdictional serious organised crime investigations. The SOCCC is supported by state and territory Joint Management Groups (JMGs), which are key forums for policing agencies and criminal intelligence agencies to share information and discuss operational initiatives. The SOCCC and JMGs have played a crucial role in facilitating the sharing of information and ideas and for harmonising national efforts to combat serious and organised crime.

  The National Border Targeting Centre within the Australian Customs and Border Protection Service is another initiative that allows law enforcement agencies to work together to combat organised crime at the border.

- *Using multi-agency taskforces to combine and coordinate a broad range of Commonwealth, state and territory capabilities, enabling more effective and sophisticated responses to organised criminal activities*.

  Joint agency task forces have been a historical staple of law enforcement's intervention strategy to address serious and organised crime; however, these collaborative task forces have often been limited to a small collection of agencies. In recent years, the Board of the Australian Crime Commission has been instrumental in broadening this collaboration to a national scale through the establishment of a number of crucial national task forces. These have included the National Organised Crime Task Force and the Attero National Task Force, both of which have incorporated the efforts of Australia's nine police forces and the ACC, as well as dedicated resources from several Commonwealth agencies, to tackle high-threat and resilient organised crime groups.

  Task Force Galilee, which was established in 2011, extended this concept to include over 40 partner agencies and industry organisations to better understand serious and organised investment fraud in Australia and develop policy initiatives to reduce the threat posed by this fraud and its impact on the community. Task Force Galilee drew on the collective capabilities of all Australian law enforcement agencies, federal regulatory agencies and key private sector industry bodies to tackle organised crime.

  Joint agency task forces and forums will continue to play an important role in unifying Australia's efforts to combat organised and nationally significant crime.

- *Targeting the proceeds of crime through the Criminal Asset Confiscation Taskforce, and ongoing prevention and detection of money laundering through comprehensive anti-money laundering arrangements*.

  The Criminal Assets Confiscation Taskforce was established in 2011 to take the profit out of crime by both removing the proceeds of crime and preventing its reinvestment into criminal activity. The Taskforce combines specialist knowledge and expertise from a range of agencies, including the Australian Federal Police, the Australian Taxation Office and the ACC. It is already having an impact, with approximately $41 million of assets restrained in the 2010–11 financial year and $97.4 million restrained in 2011–12.

- *Working with industry to make Australia a harder target for organised crime*.

  Recognising the vital role that industry plays in detecting and preventing serious and organised crime, law enforcement has increased its engagement with key industry bodies. In June 2012, the *Australian Crime Commission Act 2002* was amended to grant the ACC the ability to disclose ACC information to prescribed bodies corporate in the public sector. These extended powers of disclosure have enhanced the ACC's capability to share criminal intelligence with industry and enhanced Australia's ability to engage with industry to prevent organised crime.

- *Sharing intelligence and cooperating on formal criminal proceedings with international law enforcement partners*.

  Australia shares intelligence and cooperates with international law enforcement partners on both a police-to-police and a government-to-government basis.

  The Australian Federal Police (AFP) has primary responsibility for managing international law enforcement cooperation on behalf of the Commonwealth and works closely with foreign law enforcement partners through the AFP International Network across 28 AFP International Posts around the world. Cooperative police-to-police relationships allow the AFP to work closely and proactively with its foreign partners to combat crime at its source, actively pursuing transnational serious and organised crime syndicates in any location. The AFP has a number of police-to-police agreements (MOUs) to enable the direct sharing of criminal intelligence and investigative information with foreign partner agencies.

  The International Crime Cooperation Central Authority (ICCCA) in the Attorney-General's Department liaises with international law enforcement and justice partners in formal government-to-government requests for mutual assistance and extradition. The ICCCA liaises with foreign counterparts to:

  - obtain evidence to assist with domestic investigations and prosecutions
  - provide evidence to assist with foreign investigations and prosecutions
  - seek coercive action to support domestic investigations and prosecutions
  - undertake coercive action to support foreign investigations and prosecutions, particularly in matters involving drug trafficking, fraud, money laundering, child exploitation and terrorism offences.

- *Assisting partner countries to strengthen legal, administrative and security institutions by supporting their implementation of the UN Convention Against Corruption and adoption of the Organisation for Economic Co-operation and Development (OECD) Anti-Bribery Convention*.

  Global corruption harms national security by subverting the rule of law, entrenching weaknesses in fragile states, undermining development goals, and aiding terrorism. Corruption is also a key enabler of transnational crime, including people smuggling and trafficking.

  Australia will continue to assist partner countries to build the modern integrity systems embodied in the UN Convention against Corruption (UNCAC), including the powerful anti-money laundering and asset recovery provisions of the convention. Australia will provide over $25 million in the period 2011 to 2015 for a range of UNCAC capacity-building measures, including the UN Office on Drugs and Crime global program on anti-corruption, the joint UN Development Program–UNODC Pacific Regional Anti-Corruption Program, the

joint World Bank–UNODC Stolen Asset Recovery (STAR) initiative, and the United Nations Development Programme's Global Thematic Program on Anti-Corruption for Development Effectiveness. Australia also has a global partnership with Transparency International (TI), which aims to strengthen the TI network and foster greater citizen engagement in the fight against corruption in the Asia-Pacific region, Sub-Saharan Africa and Latin America (A$18.2 million from 2011–12 to 2014–15). The Australian Government will continue to provide direct government-to-government assistance to priority countries to strengthen regional proceeds of crime and anti-money laundering legal frameworks.

As a member of the OECD Working Group on Bribery in International Business Transactions, Australia will continue to be involved in reviewing members' implementation of the Anti-Bribery Convention. The peer review mechanism strengthens implementation of the Convention. The Working Group also works closely with invitees, including China, India and Indonesia, on developments in combating foreign bribery.

- *Supporting analytical work by the United Nations and others to better understand corruption and transnational crime trends in East Asia and the Pacific*.

  The ACC engaged with the UN Office on Drugs and Crime in 2012 to provide assistance during the development of its report *Transnational organized crime in East Asia and the Pacific: a threat assessment*. Australia is also a consistent contributor to the UNODC's *World drug report*, which paints a picture of trends in the global illicit drug market. These engagements are an important contribution to the global effort to detect, deter and prevent organised crime. Australia will also support the analytic work conducted by the Asia-Pacific Economic Cooperation (APEC) Anti-Corruption and Transparency Experts Task Force into disrupting transnational crime and corruption threats in the Asia-Pacific region.

  Australia is a member of the Asian Development Bank / Organisation for Economic Co-operation and Development Anti-Corruption Initiative, which supports national and multilateral efforts to reduce corruption in the Asia-Pacific region. Australia has encouraged the Initiative to give greater priority to engagement with the UNODC.

HARDENING AUSTRALIA AGAINST ORGANISED CRIME THREATS

The advent of globalised organised crime in recent decades has forced law enforcement to reconsider how it targets, disrupts and prevents organised criminal activities. Traditional investigative techniques and capabilities alone are no longer adequate to detect serious and organised criminal activity or develop appropriate counter-measures. The measures identified in the National Security Strategy represent some of the innovative ways in which Australia's law enforcement community is collectively tackling organised crime. There are, however, a number of other initiatives being pursued by Australia's law enforcement and regulatory agencies. These are being led by Australia's various intergovernmental ministerial and senior law enforcement advisory councils, including the Standing Council on Police and Emergency Management, the Standing Council on Law and Justice, the national policing Senior Officers Group, and the Heads of Commonwealth Operational Law Enforcement Agencies.

A number of Commonwealth parliamentary committees have conducted inquiries into a range of organised crime matters in recent years. Australia's law enforcement community has engaged closely with many of these parliamentary inquiries, including:

- the Parliamentary Joint Committee on Law Enforcement's inquiries into
  - *the gathering and use of criminal intelligence*
  - *Commonwealth unexplained wealth legislation and arrangements*, and
  - *the adequacy of aviation and maritime security measures to combat serious and organised crime*
- the Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity's inquiries into:
  - *the integrity of overseas Commonwealth law enforcement operations*, and
  - *integrity testing*
- the Parliamentary Joint Committee on Intelligence and Security's inquiry into *potential reforms of national security legislation.*

These inquiries have been beneficial to the progression of key policy initiatives and legislative reforms. For example, the *Customs and AusCheck Legislation Amendment (Organised Crime and Other Measures) Bill 2013* was passed by Parliament on 16 May 2013 and will amend the *Customs Act 1901* (Customs Act) and the *AusCheck Act 2007* to mitigate vulnerabilities at Australia's borders. The Bill forms the latest activity in a package of measures to deter and prevent infiltration by serious and organised crime into Australia's seaports, airports and cargo supply chain.

State and territory governments are also taking measures to combat organised crime in their jurisdictions. Following the agreement of the former Standing Committee of Attorneys-General in April 2009, New South Wales, South Australia, the Northern Territory and Western Australia have introduced legislation aimed at targeting organised crime groups and curbing criminal associations and recruitment strategies.

Some jurisdictions, including the Commonwealth, have also tightened laws relating to illicit drugs and precursor chemicals, firearms and prohibited weapons, and criminal wealth, and have taken steps to ensure that police forces have the capabilities required to collect evidence and intelligence.

The Australian Taxation Office has implemented a number of initiatives in recent years in an effort to address tax crime and target criminal wealth. The foremost of these has been the prescription of the Criminal Assets Confiscation Taskforce and the National Criminal Intelligence Fusion Capability as prescribed task forces for information-sharing purposes under section 355-70(1) Item 4 of the *Taxation Administration Act 1953*. This has proven valuable for law enforcement investigations into criminal wealth and money laundering activities. The ATO is also engaging closely with foreign revenue authorities through the Multilateral Convention on Mutual Administration Assistance in Tax Matters, to collect outstanding tax debts from offshore citizens.

With an increasing number of Internet users in Australia, the opportunities for criminals to engage in cybercrime are increasing. In response, the Commonwealth is leading a number of initiatives to address cybercrime. For example, Australia's recent accession to the Council of Europe Convention on Cybercrime will improve the ability of Australian law enforcement agencies to cooperate effectively with international counterparts as part of the global response to cybercrime. The increased focus on preventing, detecting and prosecuting cybercrime aims to protect Australia's digital economy and Australian citizens in cyberspace.

The *National Plan to Combat Cybercrime*, which was developed in consultation with Commonwealth, state and territory agencies involved in responding to cybercrime, provides a strategic framework for a coordinated national response to cybercrime. The Plan represents a commitment by Australian government to work collaboratively to address cybercrime and the criminal use of technology.

The Plan acknowledges the need for a more accurate intelligence picture to assist in identifying emerging trends and better direct resources to areas which would have the most substantial impact on the activities of cyber criminals. Understanding the scale and impact of these crimes across the victim spectrum — from the individual through to government — will provide the foundation for the development of effective strategies to combat the cybercrime threat.

Australia's law enforcement community recognises that protecting the community from organised crime requires a comprehensive national approach based on cooperation, cohesion and information sharing. Australia's Commonwealth, state and territory governments, and their respective law enforcement agencies, are working as closely as ever before to tackle the ongoing threat posed by organised crime. However, the fight against organised crime is as much about prevention as it is about interdiction, and effectively preventing crime is not something that can be achieved by government in isolation. Private industry and individual citizens have an important role to play in protecting themselves from these threats.

Recognising the valuable role of the Australian community, law enforcement agencies are increasingly engaging with the community and industry to better understand the extent and impact of serious and organised crime. These partnerships provide law enforcement and justice agencies with more accurate data to assist in developing more targeted responses to address identified areas of community and industry need. Public intelligence reports, such as the ACC's *Organised crime in Australia*, Crime Profile Series and *Illicit drug data report*, the Australian Taxation Office's *Targeting tax crime* publication, and AUSTRAC's *Money laundering in Australia 2011*, play an important role by arming the community with the information needed to make informed decisions and protect themselves against sophisticated crime.

Law enforcement has also undertaken a number of community awareness activities in recent years. These engagement strategies have endeavoured to raise community awareness of a range of criminal markets, including serious and organised investment fraud, card-not-present fraud, identity crime and cybercrime. By working with the community, law enforcement is strengthening Australia's resistance to organised crime.

Australia's response to the threat of organised crime is multi-faceted and ever-evolving. As the picture of criminality in Australia continues to develop and transform over time, Australia's response strategies will also adjust and develop to meet new challenges and opportunities in the fight against organised crime.