Australian Government

Australian Institute of Criminology

# Inquiry into the future impact of serious and organised crime on Australian society

## *a) Future trends in serious and organised crime activities, practices and methods and their impact on Australian society*

Serious and organised crime threat assessments across a range of western countries are relatively similar in terms of their respective identification of criminal markets and activities. Issues identified include:

- Canada -- illicit drugs, firearms, financial crime, intellectual property theft, human smuggling and trafficking and vehicle theft (Criminal Intelligence Service Canada 2006).
- Europe -- drug trafficking (especially synthetic drugs), exploitation of trafficking in human beings and illegal immigration, fraud, Euro counterfeiting, commodity counterfeiting and intellectual property theft, economic crime, cybercrime and money laundering (Europol 2006; Council of Europe 2005).
- United Kingdom -- drugs trafficking (primarily Class A drugs such as cocaine and heroin), organised immigration crime, individual & private sector fraud and other organised crime including organised armed robbery, road freight crime, organised vehicle crime, intellectual property crime, currency counterfeiting, cultural property crime, environmental crime and wildlife crime (Serious Organised Crime Agency 2006).
- United States -- smuggling of nuclear materials and technology, drug trafficking, trafficking in persons, intellectual property crimes and money laundering (Wagley 2006).

Further analyses have been undertaken of organised crime activity based on ethnic divides and/or geographical locations/boundaries. For example, a European focused report notes patterns of criminality within south west, south east and north east Europe (Europol 2006) and a Canada/US report details the impact of Asian organised crime, Eurasian/East European organised crime groups and discusses African and Balkan criminal enterprises operating within the Canadian/US jurisdictions (Drug Enforcement Administration et al 2006).

Given the varied nature of the structures of serious and organised crime, from traditional hierarchies to networks and loose affiliations, it seems increasingly important to focus upon the facilitators of such crime. A recent report highlights horizontal facilitating factors such as document forgery and identity theft (Europol 2006). Equally, the existence of a sophisticated infrastructure consisting of specialists and niche service providers who obtain, produce and supply false documentation for subsequent use in fraud has also been observed (Serious Organised Crime Agency 2006).

The economic driver of serious and organised crime, however, remains a constant and this will continue to necessitate an understanding of money laundering typologies, both current and prospective. One new prospective avenue for illicit transfer of money (or more appropriately value) is that of new payment methods (NPMs) such as internet payment systems, mobile payments and digital precious metals (Financial Action Task Force 2006). Designed primarily to facilitate cross-border funds transfer they contain a number of potential risk factors:

- the distribution channel is the internet
- there is no face to face contact with the ‘customer’ (a process known as disintermediation)
- the NPM process operates through an open and accessible network.

The future of high tech crime sits within the broader digital environment, an environment created primarily to facilitate social and business relationships and transactions.  It is an environment which is increasingly prone to degradation, infiltration and subsequent criminal activity. There have been examples of criminal elements (known colloquially as ‘super-empowered criminals’) operating in the online environment as obtainers and disseminators of identity and identity-related information. Operation Firewall, for example, in 2004 in the US and Canada culminated in the arrest of 28 people from six countries for offences including the buying and selling of 1.7 million credit card numbers (McAfee 2005).

It is not entirely clear whether currently there are ‘traditional’ organised crime groups operating within the high tech crime environment or simply criminal groups who happen to be organised. The movement by traditional transnational organised crime groups into fully-fledged high tech crime involvement will be determined as much by the diminished profitability, or increased risk, of real world criminal activities as it will by the innate attractiveness and relatively low risk of high tech crimes. It does seem likely, however, that traditional transnational organised crime groups will not shy away from using the high tech crime environment to facilitate the operation, and/or to disguise the illicit proceeds, of real world based crimes. This could include the use of:

- denial of service attacks to pursue extortion
- online banking to transfer laundered funds
- malware and/or botnets to acquire pertinent personal information for use in identity related financial crime.

### *b) Strategies for countering future serious and organised crime*

The rise of serious and organised crime has led in recent years to the rise of intelligence led policing deemed essential to meet the complex typologies comprising transnational crime networks. However, a number of organisational pathologies exist within police intelligence systems which collectively lead to the duplication of information, differential quality of analysis and hoarding of information as a result of agency possessiveness (Sheptycki 2004).

Organisationally local law enforcement agencies will need to maintain a centralised command structure but build into it a high degree of decentralised rapid response operational capacity. Local law enforcement agencies will need to consider:

- the commitment of resources to developing an organisational structure that facilitates rather than impedes inter-organisational relationships
- the sharing of intelligence within agencies and with external agencies, with a view that other agencies are resources rather than competitors
- the selection, hiring and training of all law enforcement personnel based around issues of increasing concern, which might encompass greater familiarity with IT, intelligence gathering and counter-terrorism (Schlegel 2000).

The impact and ambit of serious and organised crime can be better mitigated through anticipation and the application of lateral thinking in terms of the nature and manner of analysis of intelligence and other information. Following the events of 9/11 the Federal Bureau of Investigation (FBI) elected to move from an organisation which was process-oriented, hierarchical and reactive to a ‘high performing organization’ typified by an approach that was results-oriented, more horizontal in structure and proactive in nature. In moving towards this arrangement, the Federal Bureau of Investigation (FBI) has created a long term ‘forecasting’ strategy which feeds into a threat based planning cycle (Federal Bureau of Investigation 2004).

Recently developed to apply to transnational crime and terrorism, the ‘Preparation of the Investigative Environment’ (PIE) process is modelled on a US military assessment process. The PIE examines the organisational composition of crime/terror networks and organisations, the environment in which they meet and the behavioural patterns of each group. The PIE analytical process includes the identification of threats, diffusion of information concerning those threats and a continued validation of hypotheses created and applied to the group under observation. The PIE process obtains information through the application of a watch list of known behaviour, activities and methodologies of serious and organised criminals including financial transactions and money laundering, organisational structures and goals, the use of IT and violence (Shelley et al 2005).

A number of models of organised crime have been created in order to provide a process by which organised crime activity might be better anticipated. Williams and Godson (2002), for example, provided five such models, namely political, economic, social, strategic and composite. A brief overview of the political model (below) serves as an example of the generic process.

**Political Model**

| **Political conditions** | **Implications** | **Result to anticipate** |
|---|---|---|
| Weak state | Opportunities for organised crime to develop with little interference | Organised crime can flourish and use the state as a home base |
| Strong state becoming weak | Initial incubation then expansion of power of organised crime as state loses power | States in transition particularly vulnerable to organised crime inhibited progress toward democracy, rule of law, and the free market |
| States characterised by ethnic conflict, insurgency or terrorism | Factions use criminal activities to fund their political struggle; and use embargoes as opportunity for trafficking and profiteering | Increase in organised crime, including violence, within the state and its neighbours. End of conflict may lead to transformation of terrorist organisations into primarily criminal organisations |
| Strong democratic states with high levels of legitimacy, transparency, rule of law | Constant struggle between organised crime and law enforcement | Organised crime provides illicit goods and seeks vulnerable economic sectors but largely on the defensive |

Source: Williams and Godson 2002

To enable law enforcement to maintain control within a fluid criminal environment, a shift in the focus of intelligence gathering and analysis has been advocated. For example, the European Union based ‘Assessing Organised Crime’ project launched a proposal for a common European approach to assessing organised crime which advocated collecting and analysing data to address questions such as ‘to what extent is crime organised?’ and ‘how do criminals cooperate?’ (van Duyne 2005). A recent European threat assessment advocates a similar approach that focuses on the functional aspects of organised crime, that is, to determine what such criminals are doing and how, rather than on identifying who they are in terms of grouping or allegiance (Europol 2006).

### *d) The adequacy of legislative and administrative arrangements, including the adequacy of cross-jurisdictional databases, to meet future needs*

There are a number of informal exchanges of information and advice which occur at regular intervals between law enforcement, government and academic agencies, departments and individual analysts, experts and commentators. Much of this occurs either through informal means or through trusted and secure networks.  As much of the intelligence data is held by states and territories, the collation of such data in a more formal systematic manner to produce databases that contain data that is both reliable and valid, requires formal inter-governmental agreements to ensure on-going commitment to the development of such long term databases.

In the development of such databases, it is important to draw on the considerable expertise of statistical/research agencies who have established cross-jurisdictional databases in the criminal justice sector.  Such agencies are all too familiar with the weaknesses that exist in the jurisdictional administrative databases that are currently available. They have a range of professional operating standards and procedures that they utilise to improve the quality of administrative data. Further, these agencies have the skill base required for sophisticated statistical analysis of the databases which is fundamentally different from operational use of the databases.

To harness capacity that already exists will require legislative and administrative arrangements to enable these agencies to work in partnership to develop more effective cross-jurisdictional databases to enhance operational responses to serious and organised crime. Such a partnership also needs to enable these agencies to value add to these databases through building a credible research evidence base that informs criminal justice policy making. Operational criminal justice agencies cannot be passive consumers of the evidence base – they must also contribute to this evidence base otherwise there will ultimately be no ‘relevant’ independent evidence base on which to make rational policy, drive strategic operational priorities and provide credible indicators on which to assess performance.

Improving the evidence base, which underpins responses to serious and organised crime and reduces its impact, will require a whole of government, cross-sectoral approach as well as private/public partnerships.  Increasingly, specific forms of expertise are required to investigate and understand certain forms of criminal activity, notably where it is facilitated through rapidly changing information and communication technology.

Monitoring trends and the impact of responses will require a commitment and a significant investment in coordinated intelligence gathering, analysis and dissemination across agencies and sectors.  In addition building links across and with the research community will better inform efforts to combat serious and organised crime through analysis of data, and qualitative research into key areas or with key groups.  Overcoming barriers to sharing information and to data linkage and access will contribute significantly to efforts to generate a comprehensive evidence base.

Experience obtained beyond the parameters of operational departments and/or outside the law enforcement/intelligence spheres is clearly of utility in assisting such agencies to tackle serious and organised crime. Arrangements can be formalised, to ensure security concerns are met, to create a partnership between operational/intelligence areas of activity and the research community.  This will enhance capacity to evaluate the impact of new initiatives and approaches and to identify good practice.  Such partnerships would generate a more comprehensive national picture of serious and organised crime.

## References

Criminal Intelligence Service Canada 2006. 2006 Annual Report on Organized Crime in Canada

Drug Enforcement Administration, Federal Bureau of Investigation and Royal Canadian Mounted Police 2006. 2006 Canada/US Organized Crime Threat Assessment

Europol 2006. EU Organised Crime Threat Assessment 2006

Federal Bureau of Investigation 2004. Strategic Plan 2004-2009

Financial Action Task Force 2006. Report on New Payment Methods

McAfee 2005. McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet

National Commission on Terrorist Attacks upon the United States 2004. The 9/11 Commission Report

Schlegel, K 2000, Transnational Crime: Implications for Law Enforcement, Journal of Contemporary Criminal Justice, Vol. 16, No.4, November, pp. 365-385, SAGE

Serious Organised Crime Agency 2006. The United Kingdom Threat Assessment of Serious Organised Crime

Shelley, L.I, Picarelli, J.T, Irby, A, Hart, D.M, Craig-Hart, P.A, Williams, P, Simon, S, Abdullaev, B, Stanislawski, B and Covill, L, 2005. Methods and Motives: Exploring Links between Transnational Organized Crime and International Terrorism. National Criminal Justice Reference Service.

Sheptycki, J 2004, Organisational pathologies in police intelligence systems, European Journal of Criminology, Vol. 1 )3), pp. 307-332, SAGE

Treverton, G. F. 2005, Making Sense of Transnational Threats, RAND

UN Security Council 2001. Press Release SC/7158

van Duyne, P. C. 2005. Proposal for a Common European Approach to Assess Organised Crime

Wagley, J. R. 2006. Transnational Organized Crime: Principal Threats and US Responses, Congressional Research Service, Report for Congress

Williams, P and Godson, R 2002, Anticipating Organized and Transnational Crime, Crime, Law and Social Change, Vol. 37, pp. 311-355