PARLIAMENTARY JOINT COMMITTEE ON LAW ENFORCEMENT

Examination of the ACC Annual Report

Question on notice:

Question No. 5
The committee has a responsibility to monitor trends and changes in criminal activities, practices and methods with the report providing some good information in this regard. What do you see as the emerging threats to the community in terms of serious and organised crime, and how can these threats be disrupted?

Response

The ACC has chosen to divide this question into two parts. These two parts have been answered separately below.

What do you see as the emerging threats to the community in terms of serious and organised crime?

Emerging threats to the community from serious and organised crime derive both from the international and domestic environment and from deliberate decisions by organised crime groups. Organised crime groups are adept at identifying opportunities and taking advantage of systemic and sectoral vulnerabilities.

For example, the impacts of globalisation, advances in telecommunications and computer technology, the rise of Asia as the world's economic powerhouse and trends in world trade have increased the threat posed by transnational crime to Australia because we are no longer isolated and immune to world trends. Similarly, Australia's stable political system, tolerant social attitudes, relatively robust economy and high standard of living make it an attractive target country for crime groups. As a general rule, there is sufficient demand for illicit commodities in Australia to make importation profitable and users of illicit commodities seem prepared to pay a premium for the products. Australians by world standards have a very high take-up rate for new technology and of necessity we have large volumes of air and sea cargo, factors which also play into the hands of organised crime. Australia has a multicultural society which contains a range of diaspora groups. Criminally minded elements within some of these groups are being exploited by transnational crime groups to establish a domestic beach-head and to broaden their reach into new illicit markets. Advances in telecommunications and e-commerce make the Australian community vulnerable to exploitation by transnational groups because they negate Australia's geographic isolation from larger international crime markets. Transnational crime groups which impact on Australia are increasingly operating from failed or failing states where corruption is rife and law enforcement is limited and compromised.

Against this background, it is unsurprising that one of the evolving threats having a diverse and increasingly significant impact on the Australian community is cyber crime. Organised crime groups exploit the cyber environment in a number of ways, including:

- as an enabler for traditional crimes such as fraud (including serious and organised investment fraud), drug trafficking, the theft of personal identity information and child exploitation
- as a facilitator of criminal activity (including the use of the Internet to access expertise, to communicate covertly with other criminal groups, to shift and launder illicit wealth and to drive and shape illicit drug markets), and
- to conduct criminal activity against computers (including denial of service attacks).

The rapid uptake of Internet connectivity across the world will continue to provide new opportunities for those motivated by monetary gain to operate illegally within that environment.

Australia's illicit drug markets continue to provide the major source of profit for organised crime groups and this will continue. Increasingly, however, drug markets are being shaped by international trends. Markets for drug analogues and novel substances and illicit pharmaceuticals have an increasing threat trajectory without traditional organised crime groups having a significant presence in the markets. The markets are characterised by direct (and often remote) transactions between illicit users and suppliers (overseas and domestically) and are dominated by large numbers of entrepreneurial and opportunistic crime groups made up of persons who are tech savvy and respond rapidly to changes in demand.

Imports and domestic distribution of illicit drugs, tobacco, counterfeit goods and other illicit commodities are facilitated by corruption and infiltration by organised crime groups of sea and air ports and the transport, security and entertainment sector. Vulnerabilities at the border are identified and exploited by organised crime groups.

The laundering of criminal proceeds and the financial arrangements used by organised crime groups will continue to evolve and create a challenge for law enforcement. The inter-mingling of criminal proceeds with the legitimate economy is an area of increasing concern, which makes the identification of criminal proceeds more difficult (when compared to traditional cash based laundering techniques). The use of overtly legitimate companies as the vehicles for the commission of complex frauds, large-scale money laundering and income tax evasion is becoming more common, as is the malicious infiltration of legitimate companies by organised crime identities.

How can these threats be disrupted?

It has long been recognised that effective disruption of organised crime requires multi-dimensional and whole of Government responses. The more diverse and complex the threat

from organised crime, the more important this becomes. The Organised Crime Strategic Framework and its underpinning response planning processes enable the development of co-ordinated and integrated strategies, which encompass prevention, target hardening, education, legislative and traditional law enforcement responses (such as interdiction, investigation and criminal prosecution). The operating model of the ACC also recognises the need to identify and implement strategies that will harden the environment and address identified vulnerabilities and the mechanisms that enable organised crime to operate.

Appropriate legislative reform is an important component of both target hardening and disrupting organised crime. In this context the ACC offers the following for the Committee's consideration:

Making ACC Information and Intelligence more widely available

An important element of target hardening and prevention programs is direct engagement and sharing of information between the ACC, the public and private sectors and the general public. To this end the ACC continues to seek and support reform such as the Crimes Legislation Amendment (Powers and Offences) Bill 2011,. This legislation permits the ACC to disseminate, subject to appropriate security considerations, criminal intelligence to private sector bodies such as banks and other financial institutions. This will enable the private sector to more effectively contribute to hardening the Australian environment against the activities of organised crime groups.

Use of Criminal Intelligence

Mindful of the recommendations of the Parliamentary Joint Committee on Law Enforcement's (PJC-LE) inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime, the ACC, working in a joint Commonwealth / State Task Force and with Attorney-General's Department, and the Department of Infrastructure and Transport, is considering models for taking serious indictable offences as well as criminal intelligence holdings into consideration in the granting and revocation of Maritime Security Identity Cards (MSIC).

Novel approaches to emergent and analogue drug types

Ensuring that newly identified illicit substances can be quickly included in the ambit of controlling legislation will require novel policy and legislative approaches. The rapid evolution of illicit drug markets also underlines the importance of ensuring consistency in drug control legislation across jurisdictions, and internationally. An example of whole of Government collaboration leading to success was the scheduling of the substance BZP and the subsequent seizure of a suspected shipment of 10 kilograms of the substance in Adelaide shortly thereafter. The ACC continues to work with the Attorney-General's Department, the Australian Customs and Border Protection Service, the Department of Health and Ageing and other agencies to develop a timely and comprehensive legislative solution to the problems posed by drug analogues.

Targeting criminal wealth

Tracking the movement of illicit funds and seizing the proceeds of crime are important aspects of the Government's response to organised crime. The ACC continues to support unexplained wealth provisions as they can be an effective tool in undermining the profit motive for those serious and organised criminals who acquire wealth through illegitimate activities. However, the ACC suggests that the current unexplained wealth provisions do not lend themselves to successfully confiscating assets of people in Australia who have accumulated significant wealth from serious and organised criminal activities.

Update and reform of telecommunications interception regime

In recent years there has been significant advancement in technology and consequential change to industry practice and consumer behaviour. A rapid increase of new and converged technologies and a move to Internet protocol based infrastructure has led to industry fragmentation and globalisation. Communications are increasing in volume, becoming default-encrypted and are frequently provided by companies that reside offshore. The techniques and tools available to counter most of these challenges are available; however, use would be incompatible with the existing legislative framework, which is based on the technology used when it was enacted in 1979. The legal and regulatory framework cannot sustainably deliver effective powers to agencies to access telecommunications information for criminal intelligence purposes or to assist with investigation and prosecution of criminal offences.

Serious and Organised Investment Fraud

The ACC has commenced considering the threat to Australia and Australians posed by Serious and Organised Investment Fraud. This consideration includes gauging the scope and scale of the threat, as well as the development of whole of government strategies for early detection, warning and prevention strategies. These measures will benefit from many of the legislative innovations including dissemination of intelligence to the private sector, public awareness bulletins and the use of enhanced telecommunications interception capabilities to identify the frauds in the early stages of their operation. Additionally, working closely with non-traditional partner agencies such as the Australian Communications and Media Authority, (ACMA) and the Office of the Australian Information Commissioner (OIAC), the ACC is exploring further preventive and awareness strategies that may benefit from legislative reform.