# Chapter 3

## Future trends in serious and organised crime

## Introduction

3.1 From the outset, it is difficult to predict accurately and in a detailed way the future trends in serious and organised crime. However, the committee has identified present and emerging activities of organised crime groups and has used this evidence to make observations about how these relate to likely future trends in the activities of organised crime.

## High-tech crime<sup>1</sup>

3.2 The inquiry found that high-tech crime is a major area of opportunity for organised crime groups to pursue existing and new types of crime. The evidence provided some idea of the potential scope of high-tech crime, which includes:

...electronic piracy; counterfeiting and forgery; credit card fraud...child pornography; communications in the furtherance of criminal conspiracies; electronic funds transfer fraud; money laundering; advance fee frauds, like the Nigerian 419 offences; online dealing in illicit products of all kinds, from Viagra to drugs and so on; intelligence and counterintelligence—[and] there is a lot going on there in terms of industrial espionage, formal intelligence and counterintelligence; and, I think, denial of service...<sup>2</sup>

3.3 The committee heard that there are two aspects of high-tech crime: enabling and facilitating. Technology enabled crime is where technology creates entirely novel opportunities for criminal gain; for example, phishing.<sup>3</sup> Technology facilitated crime occurs where technology facilitates traditional or known types of crime, such as using the internet to launder the proceeds of real-world crimes.<sup>4</sup>

<sup>1</sup> This report uses the term 'high-tech crime' as opposed to 'cybercrime'.

<sup>2</sup> Professor Rod Broadhurst, Private Capacity, *Committee Hansard*, 7 June 2007, p. 67.

<sup>&</sup>lt;sup>3</sup> 'Phishing' is the act of 'sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organisation already has. The website, however, is bogus and set up only to steal the user's information': Australian High Tech Crime Centre, http://www.ahtcc.gov.au/glossary/, viewed 5 September 2007.

<sup>4</sup> Deputy Commissioner John Lawler, National Security, Australian Federal Police, *Committee Hansard*, 5 July 2007, p. 70.

## Incidence and growth of high-tech crime<sup>5</sup>

3.4 New and improved technologies offer great potential for serious and organised crime groups to undertake their existing activities and to enable new means and methods of criminal gain.

...organised crime groups will continue to exploit society's increasing uptake of technology and the opportunities it provides to both target victims and make their own operations more efficient and secure.<sup>6</sup>

3.5 The Australian Institute of Criminology (AIC) submission highlights costbenefit reasons for the growth in high-tech crime and argues that the movement by traditional transnational organised crime groups into fully-fledged high-tech crime 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.<sup>7</sup>

3.6 The committee notes that the benefits of technology are being delivered in near-equal measures to the criminal world as to legitimate business operations, and that developments in communications and information management, which have greatly enhanced the efficiency of legitimate businesses, are also being exploited by criminal organisations to enhance the efficiency and effectiveness of their own operations.<sup>8</sup> Advances in technology, readily available and often low cost, are increasing the effectiveness of many criminal activities.<sup>9</sup>

3.7 However, despite evidence of organised crime's growing online presence, organised crime groups have not as yet fully engaged with the online environment and still use the internet primarily to facilitate or commit real-world crimes.<sup>10</sup>

3.8 Nevertheless, once organised crime ultimately harnesses the online environment, the impact on society will be significant.<sup>11</sup> The committee heard that the this trend has already emerged with the activities of 'super-empowered criminals'— groups that use the internet to advertise their services to other criminal groups:

There have been examples of criminal elements (known colloquially as 'super-empowered criminals') operating in the online environment as

<sup>5</sup> The committee notes the recent release by the Australian Institute of Criminology of the paper 'The future of technology-enabled crime in Australia', *Trends & issues in crime and criminal justice*, no. 341, July 2007.

<sup>6</sup> Commissioner Mick Keelty, Australian Federal Police, *Committee Hansard*, 5 July 2007, p. 53.

<sup>7</sup> *Submission 4*, p. 2.

<sup>8</sup> Professor Rod Broadhurst, Private Capacity, *Committee Hansard*, 7 June 2007, p. 65.

<sup>9</sup> Australian Crime Commission, *Submission 17*, p. 8.

<sup>10</sup> Mr Rob McCusker, Research Analyst, Transnational Crime, Australian Institute of Criminology, *Committee Hansard*, 5 July 2007, p. 89.

<sup>11</sup> Mr Rob McCusker, Research Analyst, Transnational Crime, Australian Institute of Criminology, *Committee Hansard*, 5 July 2007, p. 89.

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...<sup>12</sup>

#### Crime in virtual worlds

3.9 High-tech crime is likely to pose considerable challenges to LEAs because the online environment blurs notions of identity and jurisdiction. A number of examples indicate the potential for technology to undermine some of the established foundations of Australia's criminal justice system.

3.10 One such example is the virtual world, such as *Second Life* or *World of Warcraft*. Large values of real-world money are transacted in virtual worlds. These developments make it difficult to identify offenders and capture virtual-world criminal communications.<sup>13</sup> Commissioner Mick Keelty, Australian Federal Police, commented that such developments had already changed the nature of how [the AFP] approached policing and how it would approach policing in the future.<sup>14</sup>

3.11 The jurisdictional issues raised by crime located in virtual worlds need to be settled so that clear approaches can be applied to the investigation and prosecution of online and high-tech crime:

...the internet poses a whole array of jurisdictional issues. One of the key planks in treating that risk...is to have strong linkages with our international counterparts and strong linkages with the attorneys-general departments and the departments of justice in the various jurisdictions, so that...we are able to nimbly, quickly and efficiently gather the data and the evidence that is needed to track these global criminals as they move in cyberspace.<sup>15</sup>

3.12 Detective Chief Superintendent Ross Barnett, Queensland Police Service, also drew attention to anticipated jurisdictional difficulties:

High take-up rates of home internet usage make the Queensland and Australian communities vulnerable to victimisation from groups who are often overseas based, making identification, enforcement, asset forfeiture and compensation action highly problematic.<sup>16</sup>

<sup>12</sup> Australian Institute of Criminology, Submission 4, p. 2.

<sup>13</sup> Commissioner Mick Keelty, Australian Federal Police, *Committee Hansard*, 5 July 2007, p. 53.

<sup>14</sup> *Committee Hansard*, 5 July 2007, p. 53.

<sup>15</sup> Deputy Commissioner John Lawler, National Security, Australian Federal Police, *Committee Hansard*, 5 July 2007, p. 66.

<sup>16</sup> *Committee Hansard*, 7 June 2007, p. 2.

#### Denial-of-service attacks

3.13 Denial-of-service attacks involve the disruption of internet businesses and their services by concerted online attacks. Such attacks commonly involve botnets—remotely controlled individual computers—which are directed to the targeted website.<sup>17</sup> The sheer volume of traffic causes the target site to freeze, and in this way the attack causes commercial damage or facilitates extortion or some other offence. For example:

[One offender]...basically used thousands of computers as robots. He used their computer power to focus an attack on a particular enterprise in order to crash that enterprise, to bring that enterprise down so that they could not trade electronically, and he did that by stealing, without people knowing it, the computing power of thousands of individuals' PCs.<sup>18</sup>

3.14 Denial-of-service attacks have immense potential to bring down banking, finance and government systems. In a recent program on online crime on ABC Radio's *Background Briefing*, the view was expressed that America's internet security is extremely weak and could not withstand a concerted denial-of-service attack. Elsewhere, the government computer network of Estonia has been disabled using botnets; the attackers were thought to be an organised crime group.<sup>19</sup>

3.15 In the same program, Mr David Vaile, from the Cyberspace Law Policy Centre at the University of New South Wales, expressed concerns about the vulnerability of government IT security generally, and how this could ultimately undermine systems vital to the maintenance of national security:

I'm hearing more and more about specifically targeted...attackers trying to breach the IT security of government agencies. But the other national security issue is probably a wider one, and that's to do with critical infrastructure. Both the Internet in general and the electronic payment systems are at the hear [sic] of what you'd call critical financial infrastructure, and to the extent that malware and other sorts of threats to that system, or even just the confidence in that system, undermine the capacity of that infrastructure to work, then it's a threat to national infrastructure.<sup>20</sup>

<sup>17 &#</sup>x27;Botnet' is jargon for a collection of software robots, or bots, which run autonomously. A botnet's originator can control the group remotely, usually for nefarious purposes. A botnet can comprise a collection of compromised computers running programs—referred to as worms, Trojan horses, or backdoors—under a common command and control infrastructure: Australian High Tech Crime Centre, http://www.ahtcc.gov.au/glossary/#botnet, viewed 5/09/2007.

<sup>18</sup> Professor Rod Broadhurst, Private Capacity, Committee Hansard, 7 June 2007, p. 67.

ABC Radio National, 'Your money dot con', *Background Briefing*, 24 June 2007, transcript, p. 4.

<sup>20</sup> ABC Radio National, 'Your money dot con', *Background Briefing*, 24 June 2007, transcript, p.18.

3.16 The Attorney-General's Department submission notes that the potential for damage from such attacks develops in step with society's increasing reliance on electronic infrastructure for dealing with information, transacting business and communicating.<sup>21</sup> The committee concurs with the Attorney-General's Department conclusion that attacks on electronic infrastructure motivated by political, malicious or criminal agents could have considerable and threatening consequences for Australia in the future.<sup>22</sup>

3.17 The committee accepts that organised crime groups have rapidly pursued high-tech opportunities for the support and furtherance of their criminal activities, and concludes that there is a vast potential for such exploitation of technology in the future. The characteristics of modern organised crime groups appear well suited to exploiting a range of opportunities provided by the internet.

3.18 The committee believes that technology enabled crime is a significant trend and area of growth in the activities of organised crime groups in Australia. In this, the committee agrees with the majority of witnesses, who saw high-tech crime as a considerable present and future danger:

...looking ahead over the next two to three years, I do not see it getting better in terms of the way organised crime is going to play with these sorts of new technologies. I see it getting more dangerous.<sup>23</sup>

3.19 The committee therefore believes that it is essential for Australian police forces to have the workforce, skills and legislative environment that allow them to quickly identify, adapt and react to technology based crime. The committee examines the need for appropriate numbers and training for LEAs to counter high-tech serious and organised crime in depth in chapter 7. The committee commends the AFP and other state and territory police services and agencies that are directing resources at this growing and harmful area of crime.<sup>24</sup>

## Money laundering

3.20 Money laundering is a longstanding activity of organised crime groups that 'provides a cloak of legitimacy to wealth derived from crime and provides a funding base from which further criminal activity can be financed'.<sup>25</sup> The AIC submission notes:

The economic driver of serious and organised crime...remains a constant and this will continue to necessitate an understanding of money laundering typologies, both current and prospective.<sup>26</sup>

<sup>21</sup> *Submission 21*, p. 6.

<sup>22</sup> *Submission 21*, p. 6.

<sup>23</sup> Professor Rod Broadhurst, Private Capacity, *Committee Hansard*, 7 June 2007, p. 69.

<sup>24</sup> Commissioner Mick Keelty, Australian Federal Police, *Committee Hansard*, 5 July 2007, p. 53.

<sup>25</sup> Australian Transaction Reports and Analysis Centre, *Submission 10*, p. 4.

<sup>26</sup> Submission 4, p. 2.

3.21 A range of criminal activities are undertaken by organised crime groups solely to facilitate money laundering. For example, while identity fraud and credit card fraud may be used to steal funds from individuals, they may also be utilised to legitimise illegally obtained funds. Of all organised crime activities, money laundering is perhaps the most consistently evolving activity.

3.22 The Australian Crime Commission (ACC) indicated that the estimated amount of money laundered globally in one year ranges between \$500 billion and \$1 trillion. The likely extent of money laundering in and through Australia has been estimated to be at least \$3.5 billion and represents, among other consequences, a significant loss to taxation revenue. Furthermore, money laundering places a sizeable financial burden on associated regulatory and law enforcement response and control measures as well as on private sector companies.<sup>27</sup>

3.23 Much of the evidence received indicates a significant and growing nexus between money laundering and technology. For example, apart from money laundering opportunities through online banking and identity fraud, a range of new opportunities for organised crime groups to launder money are emerging:

One new prospective avenue for illicit transfer of money...is that of new payment methods (NPMs) such as internet payment systems, mobile payments and digital precious metals...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.<sup>28</sup>

3.24 The AUSTRAC submission notes that developments in technology offer criminal groups anonymity, opacity and liquidity in their money laundering activities.<sup>29</sup> The committee considers that the migration towards electronic banking and funds transfer will see the continued escalation of this area of organised crime; it will provide an environment that will cloud financial trails and make the recovery of proceeds of crime by authorities difficult and protracted.

## **Identity crime**

3.25 Identity crime involves either the theft and fraudulent use of another's personal information or the manufacturing and use of entirely fictitious identities.<sup>30</sup> Identity theft is described as 'one of the world's fastest growing crimes'.<sup>31</sup>

<sup>27</sup> Australian Crime Commission, *Submission 17*, p. 8.

<sup>28</sup> Australian Institute of Criminology, *Submission 4*, p. 2.

<sup>29</sup> Submission 10.

<sup>30</sup> NSW Police Force, *Submission 20*, p. 3.

<sup>31</sup> Attorney-General's Department, *Submission 21*, p. 7.

3.26 Commissioner Ken Moroney,<sup>32</sup> NSW Police Force, highlighted the growth in identity crime and provided a useful overview of the various types of identity crime:

Identity crime is an issue of concern...[and] would appear to us to be becoming more prevalent. The use of stolen identity information to commit offences appears to be on the rise. Technology has enhanced criminal capability to produce false identities. We note the emergence of fraudulent identity manufacturers to service a number of separate organised crime groups at the one time. We also note the ease with which equipment capable of manufacturing identification can be bought...<sup>33</sup>

3.27 The Queensland Crime and Misconduct Commission rates the threat of identity crime as 'high' and as a priority for a whole-of-government response across Australia.<sup>34</sup> Incidents of identity theft and fraud are increasing, with the centralised online processing of banks and credit providers being chief targets.<sup>35</sup>

3.28 The illegal exchange and retrieval of personal information is also occurring,<sup>36</sup> with stolen identities being used as a means to commit further crimes.<sup>37</sup> The South Australia Police submission notes that advances in technology have enabled the production of better forgeries of identity documents.<sup>38</sup> This was confirmed by the South Australian Director of Public Prosecutions, who highlighted the use of forged identity documents to apply for personal loans:

...it has become a relatively easy matter for an offender to make an application for a personal loan or credit card with a significant credit facility either over the telephone, by facsimile or online...supported by forged documents as to the applicant's employment and financial status.<sup>39</sup>

3.29 The value of identity information to organised crime groups will result in the infiltration of legitimate businesses in order to access personal identity data.<sup>40</sup> The committee notes the involvement in this trend of transnational criminal groups:

This sharing has extended internationally, with evidence that international criminal syndicates have financed criminals to travel to Australia to commit identity theft offences.<sup>41</sup>

41 NSW Police Force, *Submission 20*, p. 4.

<sup>32</sup> The committee notes that Commissioner Ken Moroney has since retired from the NSW Police Force and acknowledges the long and valuable service he has given to law enforcement.

<sup>33</sup> Committee Hansard, 7 June, 2007, p. 3.

<sup>34</sup> Submission 8, p. 6.

<sup>35</sup> Queensland Crime and Misconduct Commission, *Submission 6*, p. 1.

<sup>36</sup> Mr Rob McCusker, Research Analyst, Transnational Crime, Australian Institute of Criminology, *Committee Hansard*, 5 July 2007, p. 95.

<sup>37</sup> NSW Police Force, *Submission 20*, p. 2.

<sup>38</sup> Submission 7, p. 6.

<sup>39</sup> Submission 6, p. 1.

<sup>40</sup> Western Australia Police, *Submission 15*, p. 3.

3.30 The anonymity and flexibility of the online environment suggests that identity crime is likely to continue to expand and to present ongoing costs and challenges for LEAs:

There are any number of variations of...[identity crime] limited only by the imagination of the offenders and the credulity of the potential victims. In most cases the relative anonymity afforded by electronic banking and communications is used to advantage by the offenders. This...can be difficult to prove and is investigated and prosecuted at great expense to the community.<sup>42</sup>

3.31 The committee considers that the intersection of technology and identity crime is a significant challenge for Australian authorities.<sup>43</sup> Identity crime is likely to be a major area of future organised crime activity, particularly as a facilitator of money laundering activities and the illegal attainment of funds, goods and services.

## Credit card fraud

3.32 The escalation in credit card fraud is connected to the growth of opportunities for identity and fraud crime over the internet.<sup>44</sup> In a report on its inquiry into cybercrime, this committee previously observed:

With the credit card purchasing power...[comes] the potential for large scale fraud.  $^{\rm 45}$ 

3.33 The use of credit cards offers multiple ways to commit offences. For example, certain groups are engaging in the online theft and sale of credit card information to other criminal groups. Credit card fraud is often associated with identity fraud, and involves the fraudulent purchase of goods over the internet. In yet another example of organised crime's adaptable opportunism, recent security enhancements incorporating security chips and PINs in credit cards are being circumvented by online 'card not present' transactions.<sup>46</sup>

#### **Financial crime**

Tax-related crime

3.34 The Australian Taxation Office (ATO) reported a shift from opportunistic crime to organised crime, and an increasing degree of sophistication, organisation and

<sup>42</sup> Office of the Director of Public Prosecutions South Australia, *Submission* 6, p. 1.

<sup>43</sup> Queensland Crime and Misconduct Commission, *Submission* 8, p. 5.

<sup>44</sup> Detective Chief Superintendent Ross Barnett, Queensland Police Service, *Committee Hansard*, 7 June 2007, p. 2.

<sup>45</sup> Parliamentary Joint Committee on the Australian Crime Commission, *Cybercrime*, March 2004, p. 41.

<sup>46</sup> Mr Rob McCusker, Research Analyst, Transnational Crime, Australian Institute of Criminology, *Committee Hansard*, 5 July 2007, p. 95.

collusion in taxation crimes.<sup>47</sup> Evidence suggests a relationship between taxation and other forms of crime—notably, money laundering and identity theft.<sup>48</sup> Tax crime usually involves the theft of another's identity to make a false taxation refund claim. The committee heard from the ATO that organised crime groups are systematically attacking the process:

We have seen...some fairly sophisticated attempts, where it almost looks like they have been piloting our system and trying a few to see if they get under the radar before going for one big attack. We have seen an instance of an operation almost like a call centre to change details in the system.<sup>49</sup>

#### Superannuation-related crime

3.35 The introduction in Australia of compulsory superannuation has seen massive wealth accumulate in superannuation funds. Considering the opportunism of organised crime groups, the committee considers it highly likely that such funds could be the target of serious and organised criminal activity. Additionally, retirees who are the recipients of a substantial superannuation payment may also be targeted by organised crime groups. The ACC submission notes:

Organised criminal groups will also continue to be attracted to opportunities for substantial levels of fraud across the financial sector (including superannuation, banks and securities) and in other related industries such as telecommunications and insurance. Characteristics of these sectors that are especially attractive to criminal groups include the availability of 'arm's length' transactions and the growth, size and complexity of the markets, particularly those that facilitate cross-border trade.<sup>50</sup>

#### **Illicit drugs**

#### Amphetamines and other synthetic drugs

3.36 Illicit drugs have long been a significant aspect of organised criminal activity in Australia. In the 1970s, three royal commissions investigated organised crime and the drugs trade, finding substantial connections between the two.<sup>51</sup> Mr Christopher Keen, Director, Intelligence, Queensland Crime and Misconduct Commission, bluntly observed that illicit drugs are 'the major cash cow of organised crime';<sup>52</sup> and AOSD-

<sup>47</sup> Ms Jennie Granger, Second Commissioner of Taxation, Australian Taxation Office, *Committee Hansard*, 2007, 5 July 2007, p. 24.

<sup>48</sup> Ms Jennie Granger, Second Commissioner of Taxation, Australian Taxation Office, *Committee Hansard*, 2007, 5 July 2007, p. 25.

<sup>49</sup> Ms Jennie Granger, Second Commissioner of Taxation, Australian Taxation Office, *Committee Hansard*, 2007, 5 July 2007, p. 27.

<sup>50</sup> *Submission 17*, p. 7.

<sup>51</sup> Corruption and Crime Commission of Western Australia, 'Organised crime report to the Joint Standing Committee on the Corruption and Crime Commission', December 2005, p. 2.

<sup>52</sup> *Committee Hansard*, 7 June 2007, p. 44.

related crime is the most significant organised crime activity in Australia at present.<sup>53</sup> Organised crime groups have gravitated toward the production of AOSD,<sup>54</sup> with OMCGs, in particular, largely responsible for their production and distribution.<sup>55</sup>

3.37 In the context of transnational crime, Australia is geographically vulnerable to the illicit drug trade, as pursued by organised crime groups:

Political instability in the South Pacific region presents opportunities for organised crime groups to base offshore operations focused on the large-scale production and/or transhipment of illegal drugs and precursor chemicals. Australia generally and Queensland specifically, due to its geographic proximity, loom as likely markets for both, based on the expanding demand for amphetamine type substances.<sup>56</sup>

3.38 The committee notes that the locating of illicit drug activities in overseas jurisdictions has the potential to increase, following recent moves to combat AOSD, such as the Project STOP program, which is a reporting initiative designed to reduce access to precursor chemicals in Australia.<sup>57</sup> It is likely that organised crime groups have already adjusted their production processes in response to stricter regulatory and legislative schemes.<sup>58</sup>

3.39 Given the importance of the profit motive to organised crime groups, these groups are not attached to a particular drug or method of production. These groups are already altering their behaviours in response to anti-AOSD initiatives:

...[organised crime groups] are very market driven, so where there is an opportunity to make inroads into a market—we are talking crime markets here, drug markets—we are seeing a move back into large-scale cannabis production. We have had some detections recently indicating that. Where there is money to be made, they have the distribution networks that they can utilise and exploit to be able to meet market demand.<sup>59</sup>

3.40 The committee notes that the involvement of organised crime in the illicit drug market is long established, and this is unlikely to change fundamentally in the

<sup>53</sup> Detective Chief Superintendent Ross Barnett, Queensland Police Service, *Committee Hansard*, 7 June 2007, p. 10.

<sup>54</sup> Parliamentary Joint Committee on the Australian Crime Commission, *Inquiry into the manufacture, importation and use of amphetamines and other synthetic drugs (AOSD) in Australia*, 28 February 2007, pp 10-20.

<sup>55</sup> Detective Superintendent Stephan Gollschewski, Queensland Police Service, *Committee Hansard*, 7 June 2007, pp 29-30.

<sup>56</sup> Detective Chief Superintendent Barnett, Queensland Police Service, *Committee Hansard*, 7 June 2007, p. 1.

<sup>57</sup> Detective Chief Superintendent Barnett, Queensland Police Service, *Committee Hansard*, 7 June 2007, p. 2.

<sup>58</sup> Commissioner Ken Moroney, NSW Police Force, *Committee Hansard*, 8 June 2007, p. 2.

<sup>59</sup> Detective Superintendent Stephan Gollschewski, Queensland Police Service, *Committee Hansard*, 7 June 2007, p. 24.

foreseeable future. Whether it is new or newly in-vogue drugs, such as AOSD, the primacy of drugs as the economic engine of organised crime will undoubtedly continue.

3.41 The committee draws attention to its recent inquiry into the manufacture, importation and use of AOSD in Australia, in which it canvasses the growing trend in the supply and use of AOSD. $^{60}$ 

## Paedophilia

#### Online paedophilia

3.42 New technology has allowed the online and offline activities of paedophiles to converge. The online environment supports the easy exchange of images and information related to the procuring and abuse of children, and allows predators to groom children for future contact. The online environment presents an area of escalating risk to children.<sup>61</sup>

3.43 Commissioner Keelty outlined the issues for policing arising from these new forms of criminal congregation, communication and behaviour:

This convergence...is a new phenomenon and makes evidence gathering quite difficult. It will be a problem for us into the future, as will be the simple art of telephone interception and listening device activity. If you think about it, a lot of that activity could actually happen in the virtual world, where it will be difficult, if not almost impossible, to prove who indeed has had the conversations or who indeed has been part of the conspiracy...<sup>62</sup>

3.44 The internet is a 'powerful distributive network' for pornography.<sup>63</sup> The potential for this environment to provide paedophiles with the means of organisation and communication, as well a new forum for exchanging information on and targeting of victims is a development of great concern.

#### Family-based ritual child sexual abuse

3.45 The committee received a submission from the Advocates for Survivors of Child Abuse (ASCA), which raised allegations of organised family-based paedophilia, involving the exchange of children for the purposes of ritual or ongoing sexual abuse.

<sup>60</sup> For a detailed examination of the AOSD market in Australia see Parliamentary Joint Committee on the Australian Crime Commission, *Inquiry into the manufacture, importation and use of amphetamines and other synthetic drugs (AOSD) in Australia*, February 2007.

<sup>61</sup> Detective Superintendent Barnett, Queensland Police Service, *Committee Hansard*, 7 June 2007, p. 2.

<sup>62</sup> *Committee Hansard*, 5 July 2007, p. 66.

<sup>63</sup> Professor Rod Broadhurst, Private Capacity, *Committee Hansard*, 7 June 2007, p. 55.

3.46 Mr Michael Salter, a member of the ASCA board, informed the committee that these groups employ psychologically damaging methods to subordinate their child victims and undermine their trust of law enforcement and health professionals. Such acts were claimed to successfully prevent the reporting and subsequent detection and prosecution of the offences alleged.<sup>64</sup>

3.47 The committee regards allegations of paedophilia with the utmost seriousness, and has carefully considered the evidence of ASCA as provided in their submission and at the Sydney hearing. The committee sought to establish the extent to which family-based sexual abuse of children was organised by criminal groups. At the Brisbane hearing, Ms Elizabeth Foulger, Manager, Intelligence, Queensland Crime and Misconduct Commission, told the committee that investigations of paedophile groups in Queensland had revealed a culture of 'loose associations' among paedophiles, as opposed to highly developed or sophisticated networks of offenders.<sup>65</sup>

3.48 Ultimately, the committee was unable to determine the extent of organised intra-familial ritual sexual abuse of children on the evidence received. The committee commends ASCA for its support of around 600-800 members, and acknowledges that the service this organisation renders is done without any government assistance. The committee believes that governments should give consideration to ensuring that funding for organisations such as ASCA is available.

## Conclusion

3.49 The committee is concerned about the developing trends in serious and organised crime. Regardless of the type of activity, the increasing use of technology, transnational connections and fluidity of organised crime groups will make law enforcement's task of policing organised crime's illicit activities more difficult. The committee considers that trends in serious and organised crime will require an increasingly coordinated approach involving partnerships across agencies and jurisdictions as well as internationally. In the following chapter, the committee highlights matters around which successful strategies for countering serious and organised crime should be built.

<sup>64</sup> *Committee Hansard*, 7 June 2007, pp 33-34.

<sup>65</sup> *Committee Hansard*, 8 June 2007, p. 52.