

Invited presentation to the 9th National
Security Conference, Sydney 21-22
February 2011.



Australian Government

Australian Institute of Criminology

Emerging and future trends in organised crime

Dr Adam Tomison

The Director gratefully acknowledges the assistance of AIC research staff Peter Homel, Russell Smith, Samantha Bricknell and Raymond Choo in preparing this paper.

Organised crime

- The ACC highlights seven broad areas of particular concern to Australia
 - drugs
 - **environmental threats**
 - money laundering
 - intellectual property crime
 - **fraud**
 - firearms
 - **technology-based attacks**



Quantifying the extent of the problem



United States

- 8 million victims of ID theft (4% of population; \$US 45 bn)
- Decrease since 2003 (US\$54b) (*Javelin Strategy and Research 2008*)

United Kingdom

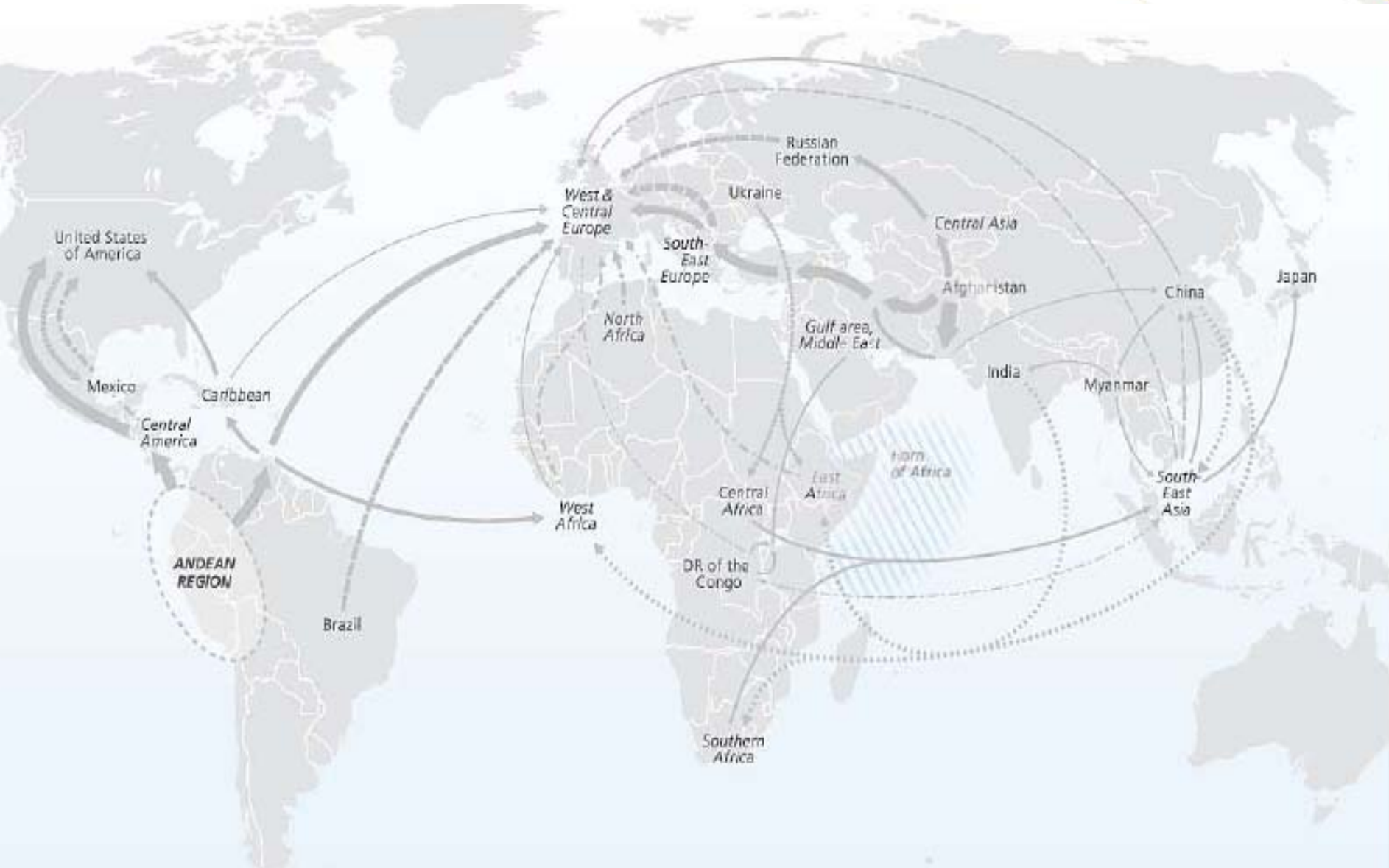
- £1.3 billion identity fraud losses involving 80,000 victims (ACPO 2005)
- 32% increase in identity fraud in 2009; 85,000 victims of impersonation fraud; 24,000 victims of ID takeover (*National Fraud Authority 2010*)

Australia

- Identity fraud A\$1.1 billion (*SIRCA 2002*)
- 499,500 victims of identity fraud (3.1% population) (*ABS 2008*)
- 242,150 counterfeit transactions 2008-09 worth \$111 million; up 92% from 2006-07 to 2008-09 (*APCA 2010*)



UNODC identity theft threat assessment (2010)



UNODC identity theft threat assessment (2010)

Route

- Internet as the modern vehicle
- Perpetrators from both developed and developing countries
- Victims mainly located in developed countries (USA, EU, Australia etc)

Dimensions

- Annual volume – 1.5 million victims globally (Aust 499,500 victims 2007)
- Annual value – US\$1 billion (Australia A\$1.1 billion in 2003)

Offenders

- Data acquisition primarily carried out by individuals or small groups
- “Cashing out” may involve organised crime groups

Threat level

- General decline in identity theft; electronic-based theft ‘unclear’



Committing identity crime in the 21st century: key tasks



- Acquiring skills and expertise
- Gathering personal information – stolen, fabricated or borrowed – internet is the ideal vehicle
- Perpetrating fraud – card counterfeiting, obtaining finance etc.
- Disbursing proceeds – purchasing assets, storing funds
- Laundering proceeds – placement, layering, integration



Acquiring identifying information

Data leakage cases

- Card Systems Solutions lost details of 40 million accounts in May 2005 with >130,000 Australians affected
- TJ Maxx lost details of 90 million customers over 2 years
- HM Revenue & Customs – 25 million child benefit records lost
- UK Ministry of Defence – 600,000 personnel details of recruits lost

Verizon Business Data Breach Investigations Report 2010

- In 2009 – 141 breaches involving 143 million compromised records
- 85% attributable to organised crime groups; 70% from external sources
- 40% from hacking; 38% used malware; 28% social tactics

Data trafficking via the digital underground economy

- USA *Operation Firewall* – 28 people from 6 countries – *Shadowcrew* members buying and selling 1.5 million credit card numbers in 2004



Responding to identity crime



Increasing the effort required to offend

- Chip/PIN roll-out, Liquid Encryption Numbers, anti-skimming ATMs, biometrics, customer education (*Protect Your PIN*), merchant education

Increasing the risk of apprehension

- Real-time transaction monitoring, notification and blocking, data-sharing, data matching, verification of evidence of identity, task force policing

Reducing the rewards of offending

- Harmonisation of laws across jurisdictions, skimming and identity crime offences, enhanced sanctions, unexplained wealth laws, confiscation of the proceeds of crime, anti-organised crime measures, AML regime



Challenges



Geography

- Offenders located in overseas countries
- Different languages and time-zones
- Barriers to sharing information between countries
- Problems of mutual assistance and extradition

Anonymity

- Ability to transact anonymously
- Difficulty for law enforcement in linking offender with computer user
- Lack of visibility of organised crime groups

Flexibility

- Difficulties in tracking changing crime typologies
- Risks of replacement of key figures following law enforcement action
- Need to share information 24/7 for rapid response



Cybercrime - Online child exploitation

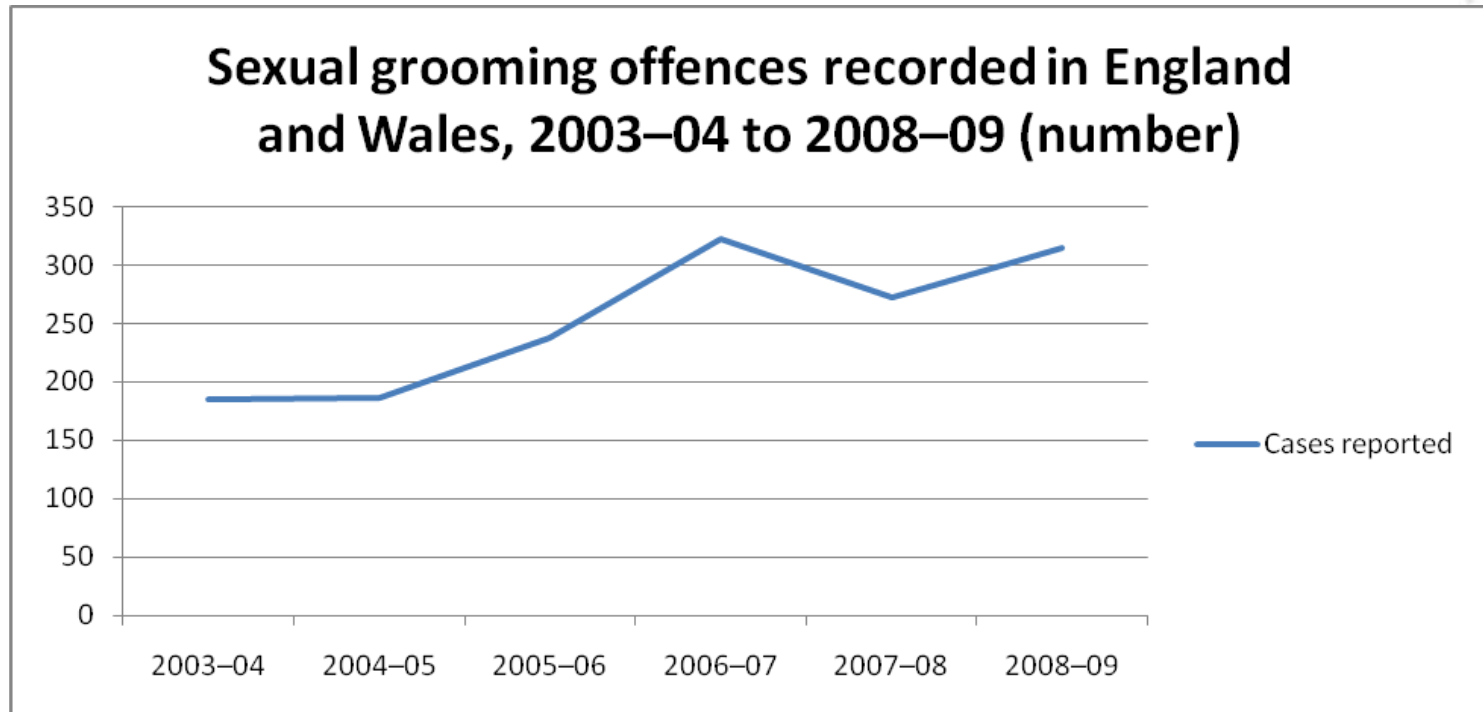
Australia

- Until 2007, >130 completed prosecutions for online procuring, grooming and exposure offences
- FY 2008-09, >150 individuals charged with online child sex exploitation
- More cases of attempted child grooming on social network sites;
- Excludes the increasing number of cases where sexual and physical assaults are filmed and put online by peer perpetrators + uploading of inappropriate material of friends by other juveniles



Size of the problem

- A UK cybercrime survey estimated that 850,000 cases of unwanted online sexual approaches were made in chat rooms during 2006
 - c/f the 238 recorded offences for meeting a child following online sexual grooming.



- In an Irish Survey of Children's Use of the Internet (2005-2006),
 - 19% of the 848 students aged 9-16 years indicated that they had been harassed, upset, bothered, threatened or embarrassed by someone when chatting online,
 - 7% reported meeting someone in real life after knowing them on the internet
 - 24% indicated that the person who had introduced themselves as a child on the internet turned out to be an adult.
- In the US:
 - Youth Internet Safety Survey (2006), 1,500 young people aged between 10 and 17 years reported frequent exposure to unwanted sexual material, sexual solicitations and harassment online.
 - In the Growing Up with Media survey, 35 percent of the 1,588 young people aged 10-15 years reported being the victim of either internet harassment or unwanted sexual solicitation.



Future risks and responses

- Ongoing improvements to anonymising protocols, password authentication techniques, encryption and steganographic techniques
- Trafficking child pornography, particularly movie files and real-time images through more powerful broadband services
- Using search engines to locate children for the purpose of sexual abuse online
- Obtaining personal information on children online by sexual offenders and fraudsters alike – the rise and rise of social networking
- Online child grooming prosecutions involving multiple jurisdictions will continue to rise
- Increasing demand for new strategies for investigating, prosecuting and preventing online multijurisdictional child grooming crimes.



Future responses

- How will Law Enforcement manage exponential growth?
- Process of targeting:
 - Organised vs amateur
 - Producer vs viewer
 - Active groomer vs viewer
- Is there a place for triaging and 'regulatory' approaches for those matters not able to be investigated?
- Should there be a therapeutic jurisprudence approach to 'minor' offending? What would the impact be?
- Are current covert 'sting' operations adequate to catch contact-focused offenders (esp. the male-focused)?



Environmental crime

- Pollution and other contamination of air, land and water
- Illegal discharge, transport or dumping of hazardous and other waste
- Illegal trade in prohibited and regulated substances
- Illegal trade in fauna and flora and harms to biodiversity
- Illegal, unregulated and unreported (IUU) fishing
- Illegal logging and timber trade
- Illegal native vegetation clearance
- Illegal water usage (eg 'water theft')



Size and dynamics

- One of the fastest growing areas of criminal activity and may become as lucrative as the illegal drugs and arms trade
 - \$US22–31 billion generated just from illegal transfer and dumping of hazardous waste and the illegal wildlife trade
- The majority of environmental crimes are perpetrated by ‘loosely organised networks of individuals with some specialist knowledge’ BUT...
- Sophisticated, transnational operations do exist, primarily involving:
 - Illegal transport and disposal of hazardous waste
 - Illegal wildlife trade
 - IUU fishing
 - Illegal logging and timber trade



Domestic illegal fishing

- Infiltration of organised criminal activity in the taking of high profit species eg abalone, rock lobster, shark (fin)
- Most organised illegal activity is by commercial fishers
 - 26% of fisheries officers interviewed in AIC study described ‘a lot’ of organised illegal fishing in their jurisdiction and 58% described ‘some’ organised activity. Involves fishers, processors and distributors
- High level organised offending (eg OMCG and Asian Crime gangs)
 - For example, illegal abalone trade and link to other illegal activities (purchase of fishing vessels to distribute drugs)
- Key risk factors
 - Structural nature of industry (competition between local & overseas operatives; itinerant nature of workforce)
 - Profitability
 - Entrepreneurship of organised criminal groups



Illegal wildlife trade

- Size of trade described as ‘small’ but increasing and involving more organised and sophisticated operatives
 - 26,500 wildlife and wildlife products seized between 2002–03 and 2006–07
 - <1 percent described as ‘major’ breach
 - 46% of prosecutions for illegal export of native fauna; 34% for import of exotics
- Trade mostly involves reptiles (snakes, lizards), birds/birds eggs, insects and spiders
- Generally, small organised groups involving supplier, courier, receiver and buyer BUT
 - Evidence for extensive bird trafficking rings involving co-mingling of wild and captive bred birds and import/export to southern Africa and SE Asia
 - Involvement of OMCG in illegal import of exotics



Illegal waste disposal

- The most likely setting for organised criminal activity
 - Smaller operatives and ‘boundary riders’ (bigger players have a reputation to lose)
 - May escalate because of economic restraints and desire to avoid payment of increasing fees, levys etc
 - Formation of alliances between waste producers, transport drivers and location scouts/site owners
- Illegal shipments of hazardous and e-waste offshore (eg China, Philippines)
 - Waste and recycling companies ‘regularly’ approached by traders to illegally move waste OS
 - Multiple ships intercepted by ACBPS each year



Overall...

- Significant impact of information and computer technology on crime – renewing and metamorphosing of old crimes
- Increased flexibility and dynamism of criminal behaviour – facilitated by ICT
- Law enforcement and security services must continue to develop effective, flexible responses
- Ongoing need to improve interagency communication and collaboration
- Need to ensure intelligence processes and law enforcement interventions are evaluated and outcomes measured to verify their effectiveness and inform future developments

