Australian Government
Australian Institute of Criminology

International Serious and Organised Crime Conference

Organised identity crime in a global perspective

Dr Russell G Smith
Principal Criminologist

Outline

Defining organised identity crime

- Defining organised criminal groups
- UNODC typologies of organised crime
- Types of organised crime groups that are engaged in identity crime

The nature of organised identity crime

- UNODC identity theft threat assessment 2010
- Identity crime scripts and procedures – ATM skimming; data breaches

Quantifying the extent of the problem

- International surveys and card fraud statistics

Responding to identity crime

- Applying principles of environmental crime prevention
- Victim support, consumer education, research and statistics
- Challenges for the future

United Nations Palermo Convention (2000)

‘Organised criminal group’ *Article 2*

- A ***structured group*** of three or more persons
- Existing for a period of time and acting in concert with the aim of committing one or more ***serious crimes***
- Obtaining directly or indirectly, a financial or other material benefit

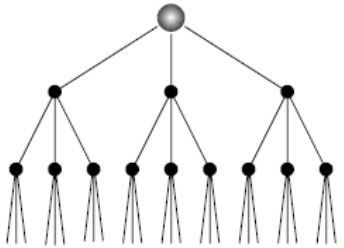
‘Structured group’

- A group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership, or a developed structure

‘Serious crime’

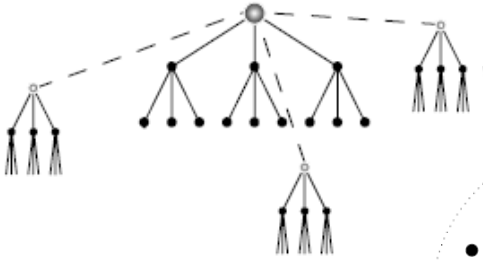
- Conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty

UNODC Typologies



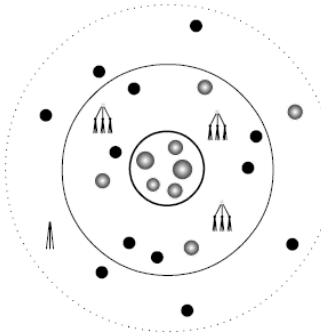
Rigid hierarchy

- Single leader and name, social / ethnic identity, violence, disciplined



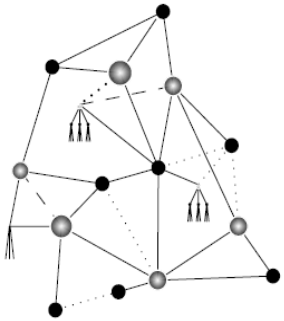
Devolved hierarchy

- Single leader, autonomy at regional leve



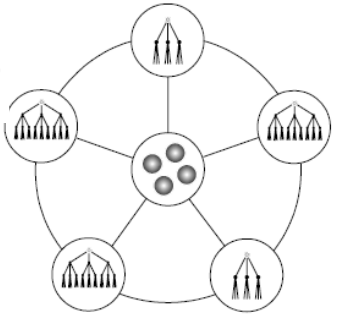
Core criminal group

- Small core group with loose network, no social/ethnic ties



Organised criminal network

- Key individuals, personal loyalties, no name, low profile, contacts/skills maintain network

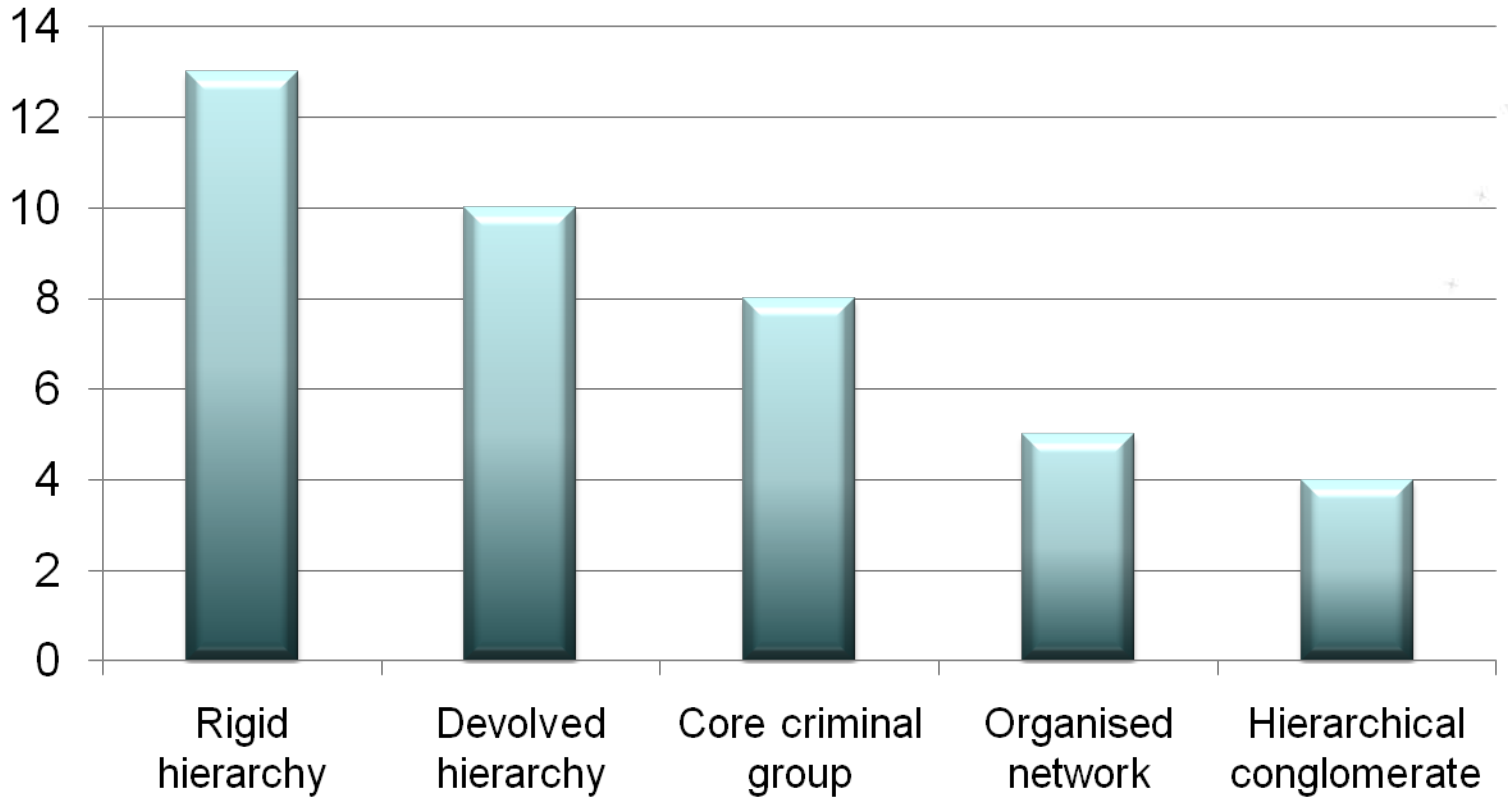


Hierarchical conglomerate

- A number of criminal groups, each having autonomy with social historical links, relatively rare, strong identity

UNODC survey of 40 organised crime groups

Number of organised crime groups by type of structure



Source: Mark Shaw UNODC (2002)

Organised identity crime groups

Traditional organised criminal groups *(rigid hierarchy)*

- Traditional organised crime groups that generate funds using ID crime
- Software piracy, plastic card fraud, card skimming
- *e.g. Japanese Yakuza, Asian triads, Eastern European gangs*

Organised identity crime groups *(core criminal groups)*

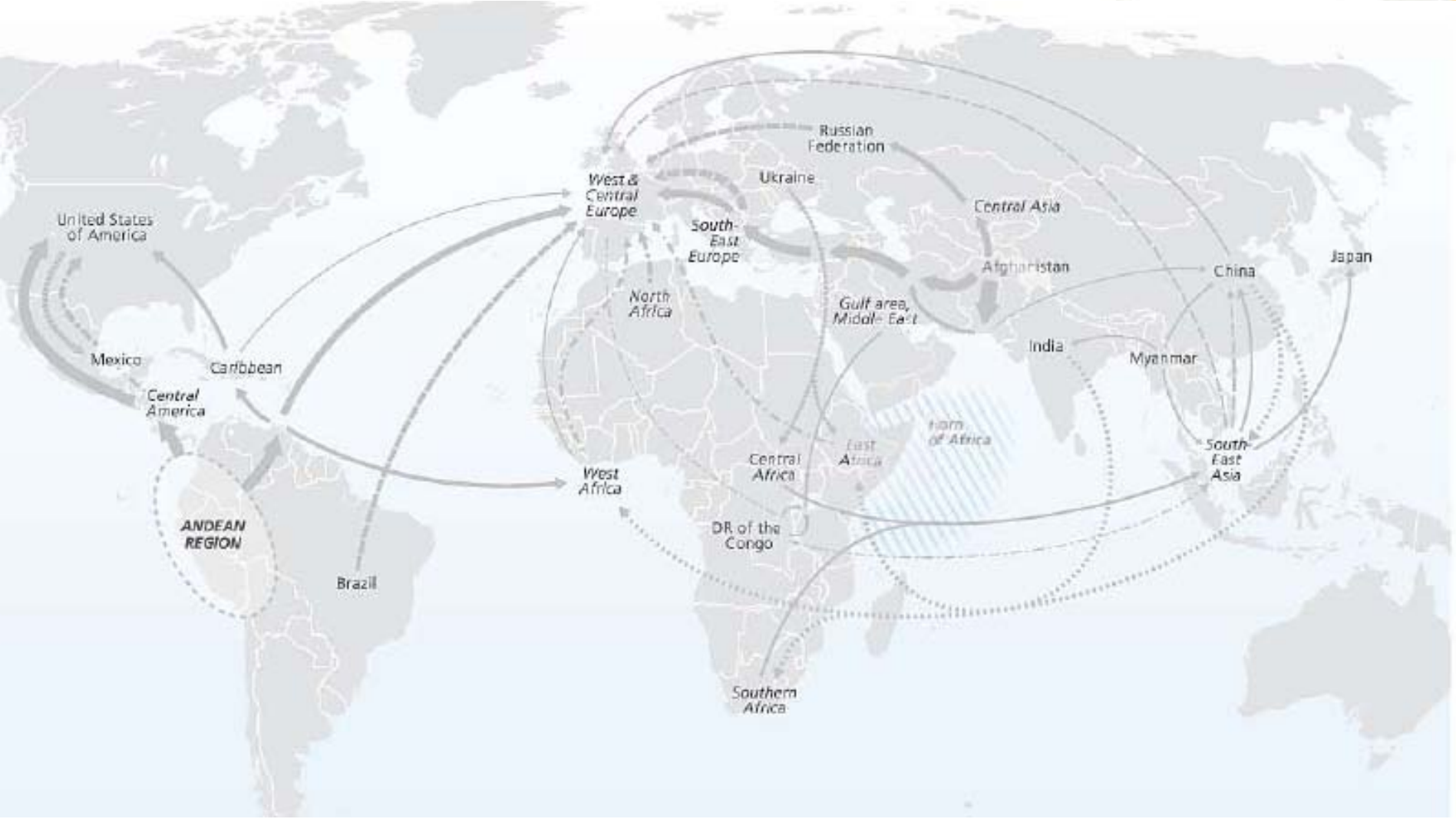
- Small groups with common objectives to perpetrate ID crime
- Carding, underground malware markets, organised identity theft
- *e.g. Shadowcrew, Carderplanet, CardersMarket, Theft Services, DrinkOrDie, Rock-Phish, BotMaster, Mpack*

Ideologically/politically motivated groups *(various types)*

- Terrorist groups formed to raise funds for religious or political change
- Financing of terrorism, fraud, money laundering, planning attacks
- *e.g. Imam Samudra (Bali), Tariq Al-Daour* (UK *Al Qaeda cell)*

Sources: Choo & Smith (2007), Peretti (2009)

UNODC identity theft threat assessment (2010)



Source: UNODC (2010: 205)

UNODC identity theft threat assessment (2010)

Route

- Internet vector
- 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
- “Cashing out” may involve organised crime groups

Threat level

- General decline in identity theft; trend in electronic dimension unclear

Source: UNODC (2010: 205)

Identity crime scripts

The tasks involved in identity crime

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

Skill sets required of others

- Mass-marketed scams, malware, phishing, hacking, insider corruption
- Card skimming, ATM and card reader attacks, card counterfeiting
- Obtaining funds (cashing-out), money laundering

Sources of information

- Online, personal contacts locally and internationally, professional advice

Based on Levi (2010: 392)

Example – ATM skimming

Source: LINK Scheme (July 2010) www.link.co.uk

Identity crime procedures

Preparation

- Locate a crime opportunity
- Obtain financial resources
- Seek professional advice in connection with laundering
- Obtain equipment and data
- Locate potential victims
- Minimise law enforcement operational risks

Offending

- Perpetrate scam to obtain personal information needed for the crime
- Obtain merchandise, financial advantage, cash, credit

Post-offending activities

- Convert goods into cash and proceeds into laundered funds
- Move assets into low-risk jurisdictions where they can be enjoyed

Based on Levi (2010: 392)

Acquiring identity information


Bryn Wellman 2007

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

Quantifying the extent of the problem

United States

- 8 million victims of ID theft (4% of population) losing US$45 billion
- Decrease since 2003 (US$54b) (*Javelin Strategy and*

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

- Organised crime A$10-15 billion (*ACC 2010*)
- 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; 92% increase from 2006-07 to 2008-09 (*APCA 2010*)

Responding to identity crime

Assessing levels of risk

- Estimated identity fraud losses in excess of A$1b
- 1 in 20 household users victimised by scams or identity fraud in 2008
- 0.02% credit/charge card transactions were fraudulent 2008-09

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

Responding to identity crime

AUSTRALASIAN CONSUMER FRAUD TASKFORCE

AN INITIATIVE OF THE STATE, TERRITORY AND AUSTRALIAN AND NEW ZEALAND GOVERNMENTS

Victim support

- Improving victim support – reporting, loss recovery, counselling
- Identity fraud court victimisation certificates

Consumer protection

- Australasian Consumer Fraud Taskforce
- Attorney-General's Department identity fraud prevention kit
- Enhanced training of users to maintain computers adequately
- Computer driving licence
- Enhanced training of users to avoid risky behaviours

Research and statistics

- Standardisation of terminology for identity crime
- National victimisation surveys
- Coordinated data collection amongst stakeholders

Challenges for the future

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

Australian Government
Australian Institute of Criminology

Russell.Smith@aic.gov.au