Australian Government
Australian Institute of Criminology

Fraud Liaison Forum 2009

Understanding organised cybercrime risks for government

Dr Russell G Smith
Principal Criminologist

Outline

Defining organised crime groups

- Classifying the various types of organised crime groups

Organised cybercrime groups

- Identifying the types of organised crime groups that operate in cyberspace

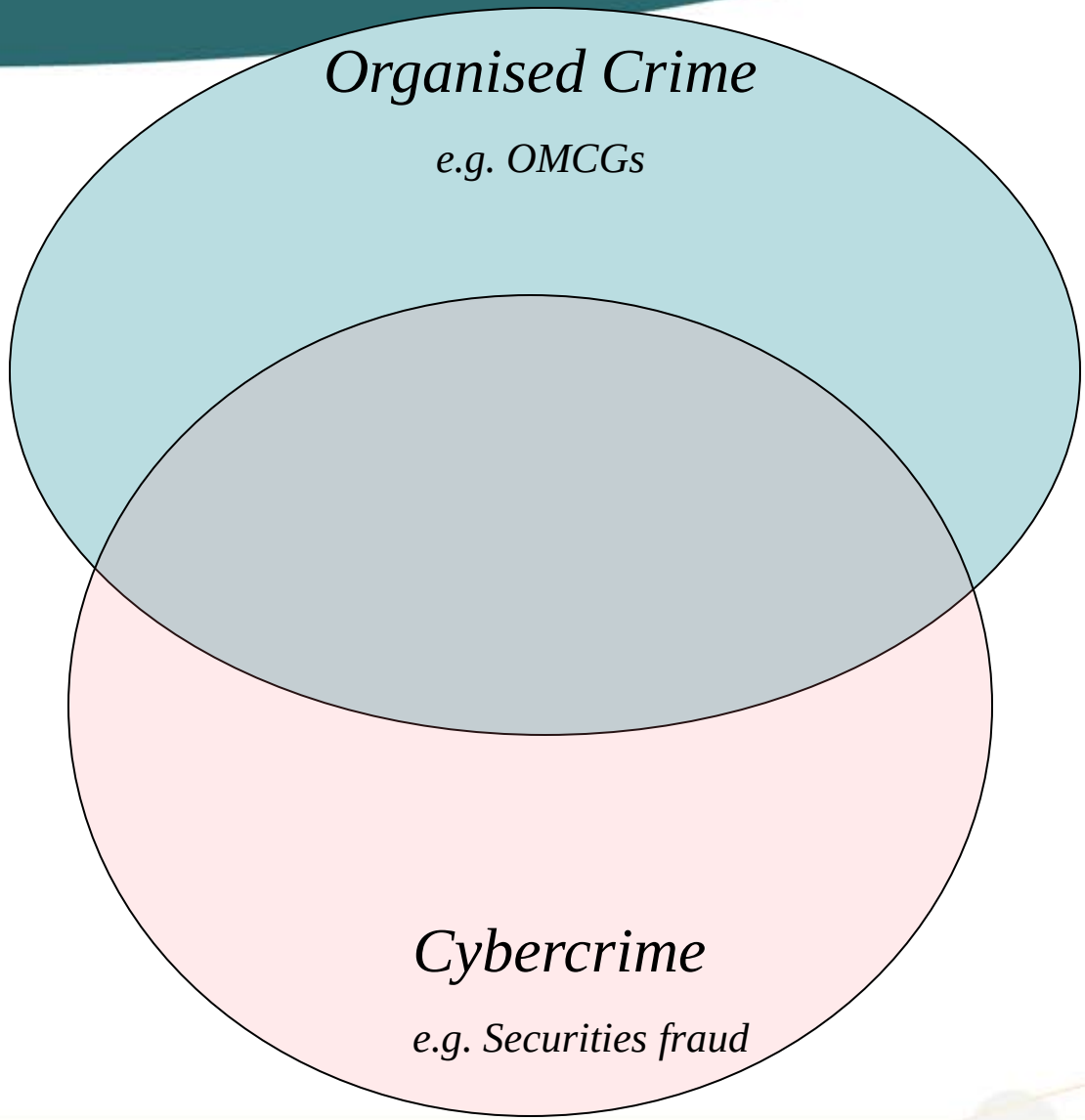
Current and emerging risks for government

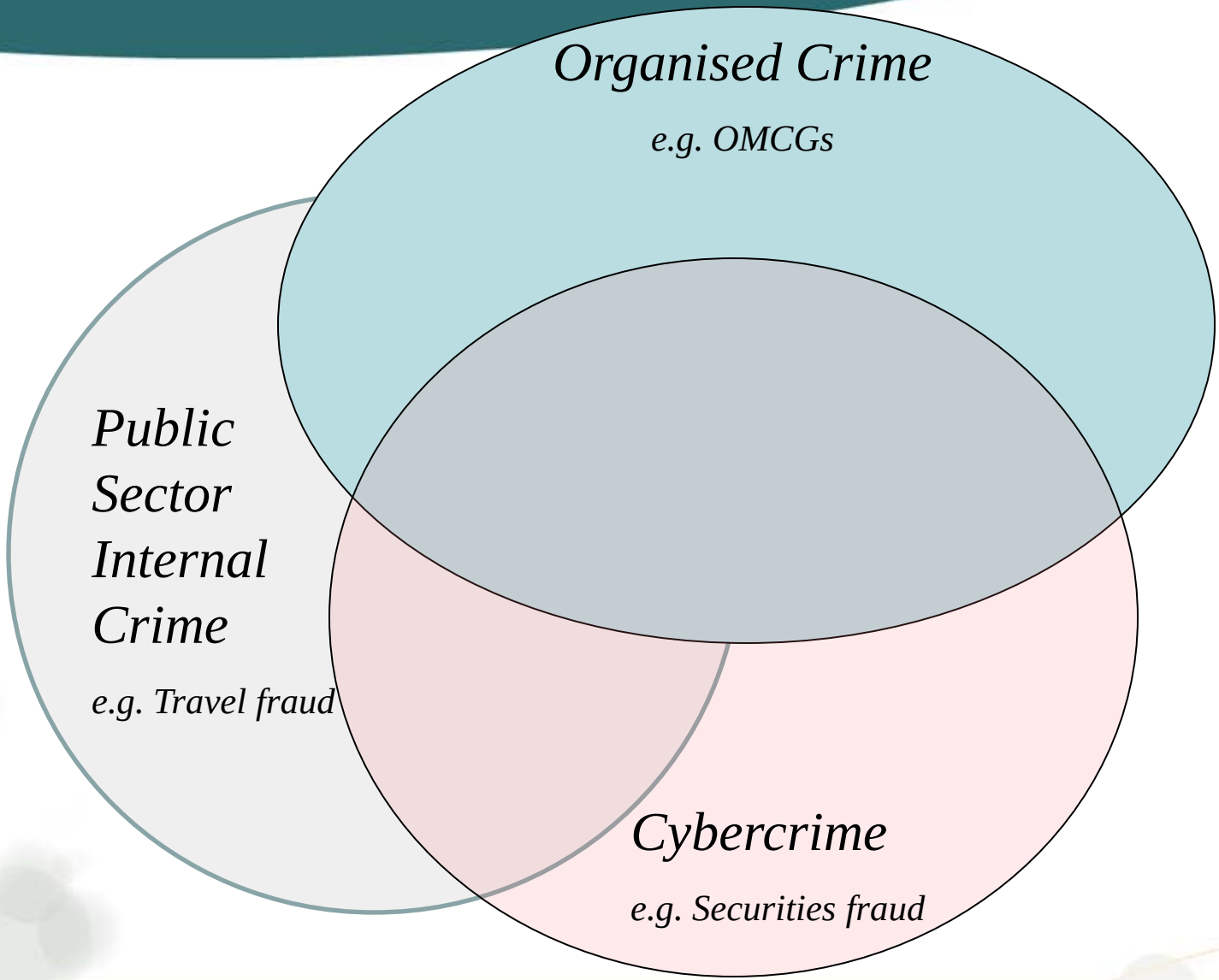
- Understanding the activities of organised cybercrime groups
- Identifying the key risk areas for government

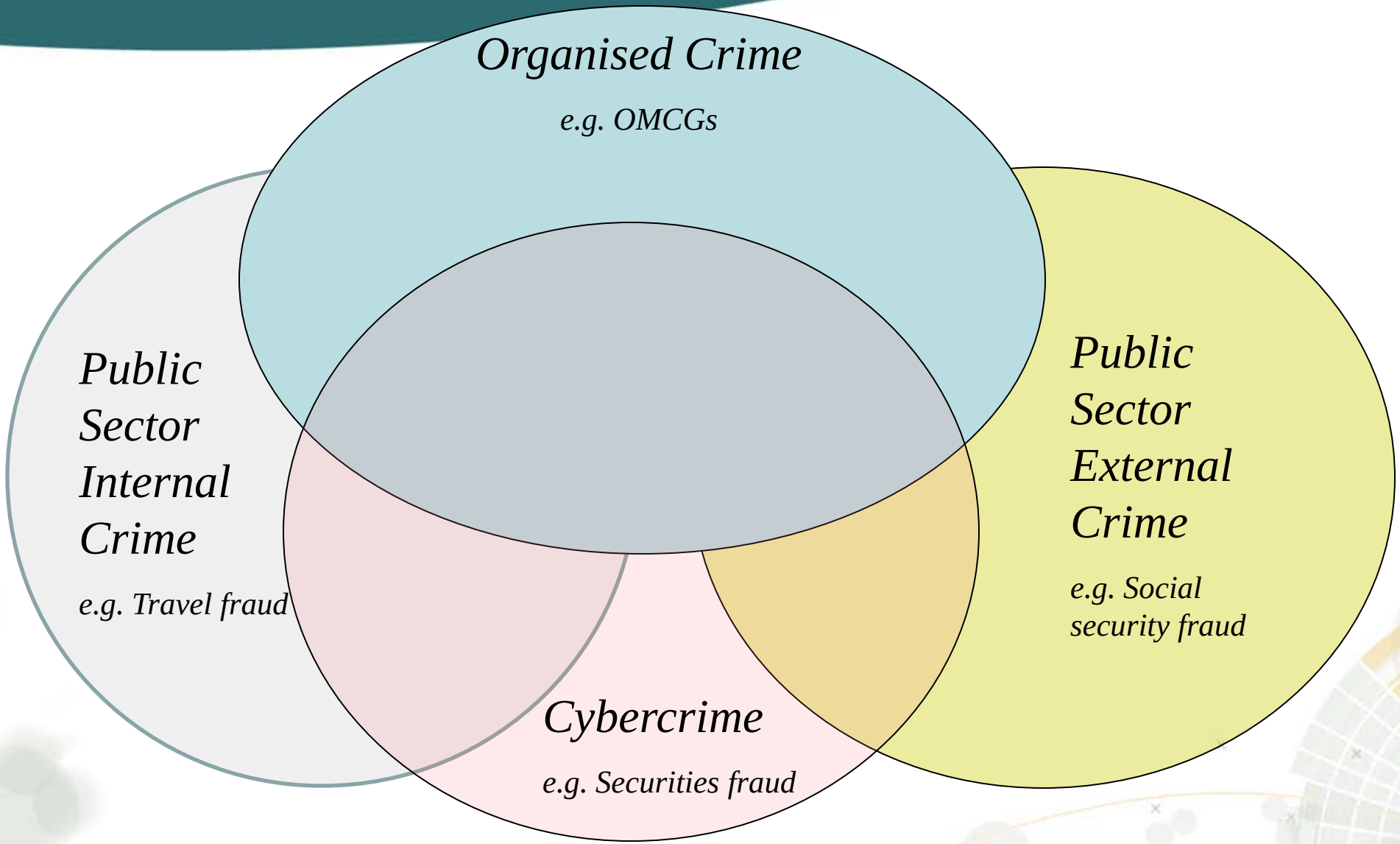
Responses

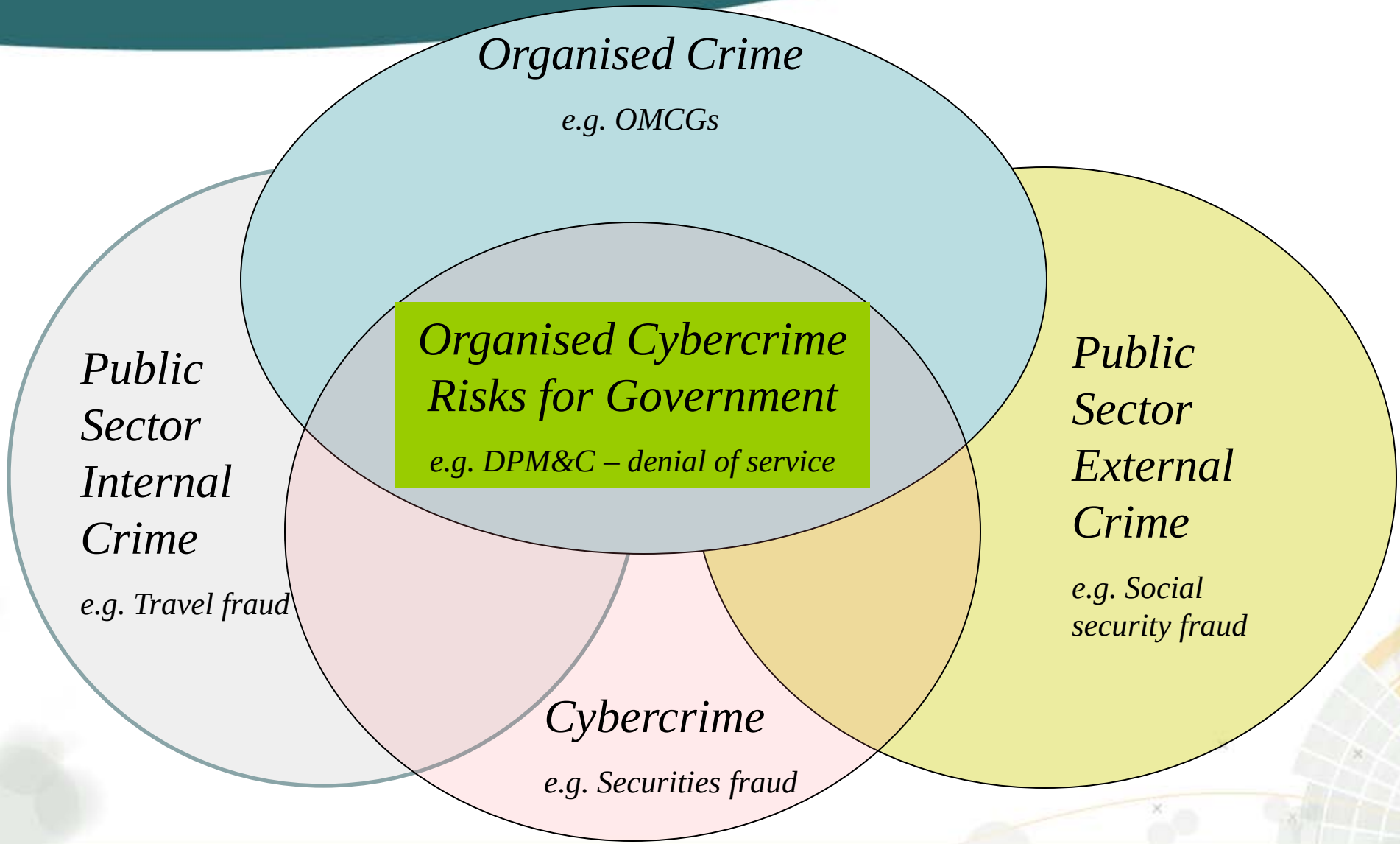
- Applying principles of environmental crime prevention
- Strategies and impediments to taking action against organised cybercrime that affects government


Organised Crime
e.g. OMCGs


Organised Crime
e.g. OMCGs
Cybercrime
e.g. Securities fraud


Organised Crime
e.g. OMCGs
Public Sector Internal Crime
e.g. Travel fraud
Cybercrime
e.g. Securities fraud


Organised Crime
e.g. OMCGs
Public Sector Internal Crime
e.g. Travel fraud
Public Sector External Crime
e.g. Social security fraud
Cybercrime
e.g. Securities fraud


Organised Crime
e.g. OMCGs
Public Sector Internal Crime
e.g. Travel fraud
Organised Cybercrime Risks for Government
e.g. DPM&C – denial of service
Public Sector External Crime
e.g. Social security fraud
Cybercrime
e.g. Securities fraud

United Nations Palermo Convention 2000 (article 2)

‘Organised criminal group’

- 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

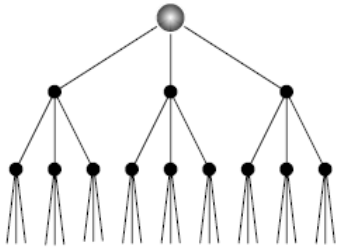
‘Structured group’

- 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’

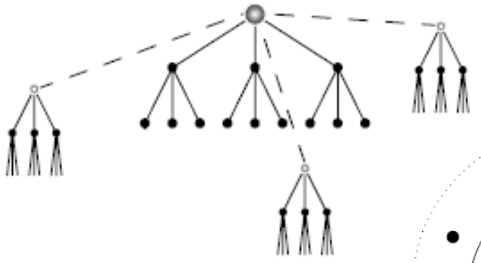
- Conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty

UNODC Typologies



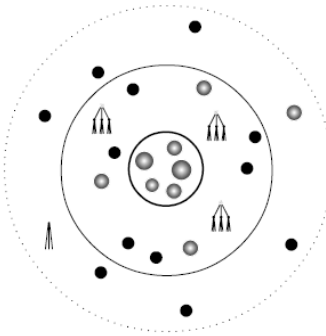
Rigid hierarchy

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



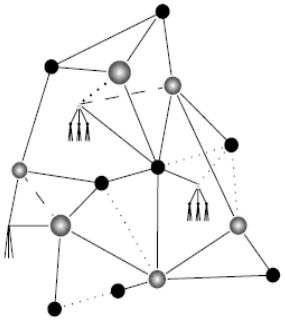
Devolved hierarchy

- Single leader, autonomy at regional level



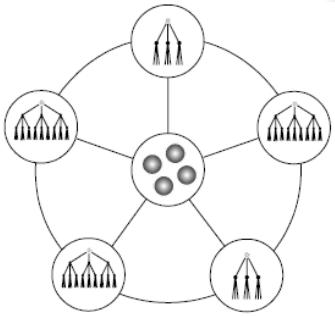
Core criminal group

- 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



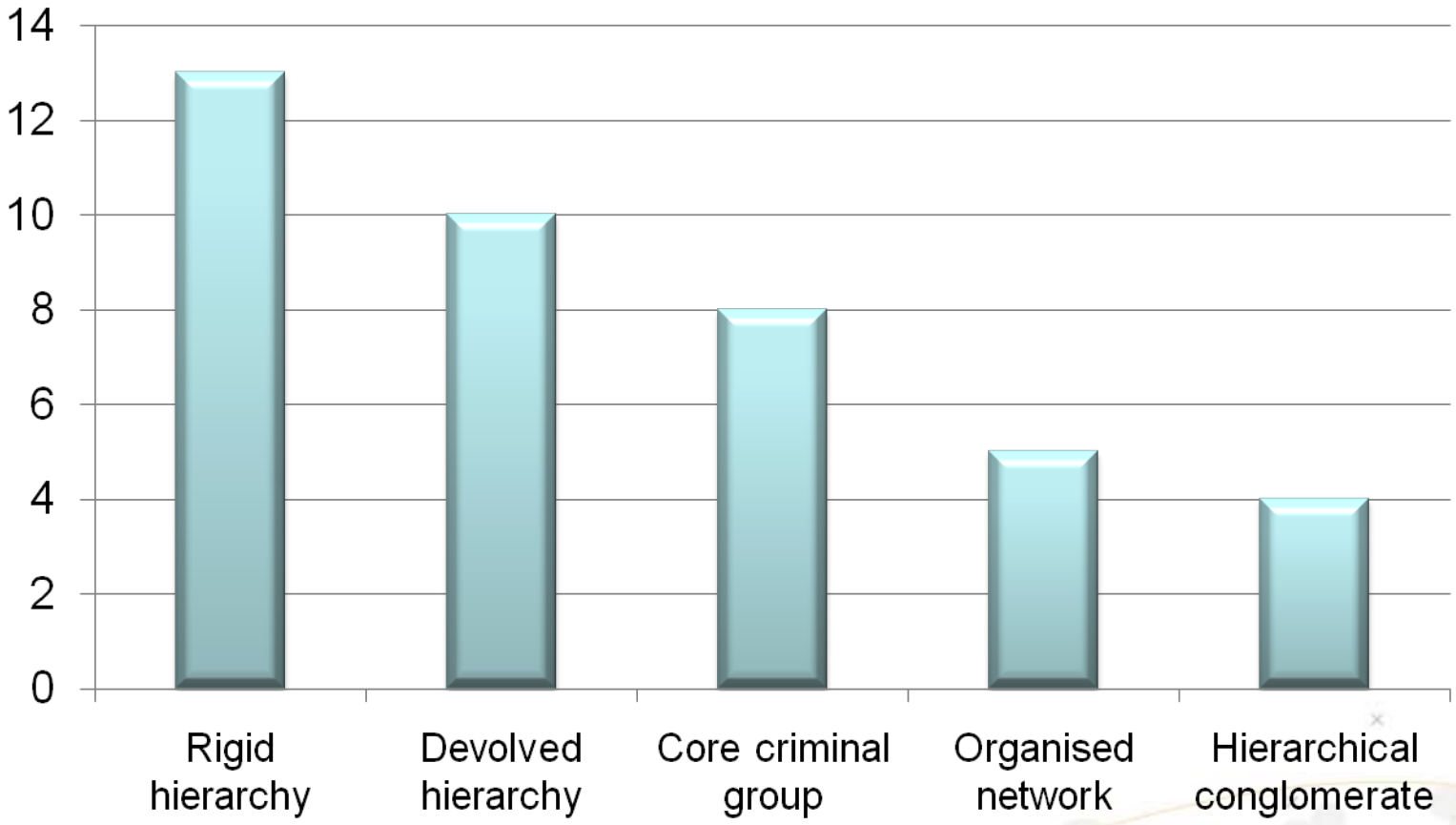
Hierarchical conglomerate

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

Source: Mark Shaw UNODC (2002)

UNODC survey of 40 organised crime groups

Number of organised crime groups by type of structure



Source: Mark Shaw UNODC (2002)

Organised cybercrime groups

Traditional organised criminal groups *(rigid hierarchy)*

- Terrestrially-based groups that make use of ICT to generate funds
- Communications, software piracy, plastic card fraud, malware attacks
- *e.g. Japanese Yakuza, Asian triads, Eastern European gangs*

Organised cybercriminal groups *(core criminal groups)*

- Small groups that only meet in cyberspace with common objectives
- Child exploitation, underground malware markets, identity crime, DDoS
- *e.g. Shadowcrew, 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. Faheem Khalid Lodhi, Al Qaeda, LTTE, Anonymous*

Source: Choo & Smith (2009)

Examples of organised cybercrime risks

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 2009

- In 2008 – 90 breaches involving 285 million compromised records
- 91% attributable to organised crime groups; 74% from external sources
- 67% from mistakes; 64% from hacking; 38% used malware

Data trafficking via the digital underground economy

- USA *Operation Firewall* – 28 people from 6 countries – buying and selling 1.7 million credit card numbers in 2004

Australian Government
Australian Institute of Criminology

Organised cybercrime risks for government

Targets

- *Revenue* – income tax, GST, customs duties
- *Benefits* – health, social security, education, training
- *Property* – computers, phones, intangible property (IP, agency logos)
- *Entitlements* – expenses, travel allowances, payroll, leave
- *Facilities* – computers and telecommunications, policies

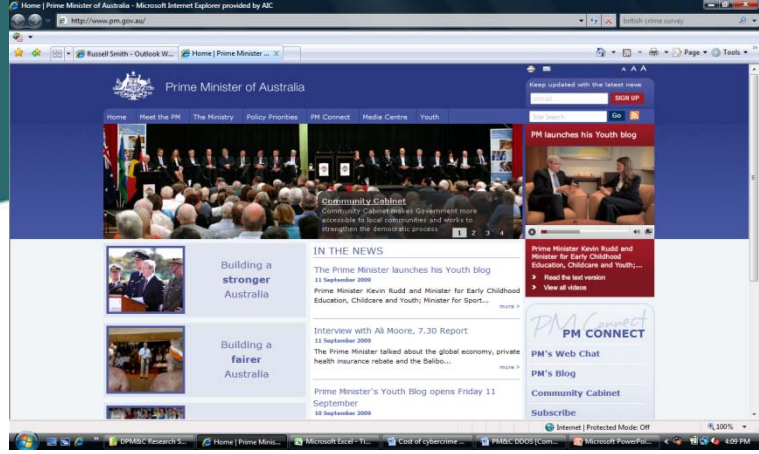
Methods

- Payment card misuse, unauthorised computer access, DDoS
- Counterfeiting documents; providing false information, identity fraud
- Bribery, corruption, abuse of office, kickbacks, collusion

Offenders

- Internal risks – public servants and contractors
- External risks – members of the public / benefit recipients

Australian Government
Australian Institute of Criminology



Organised cybercrime risks

Information attacks

- Attacks on government websites (e.g. Department of Prime Minister & Cabinet – DDoS attack against Internet filtering policies in Sept 2009)
- Extortion using denial of service attacks by Botnets
- Misappropriation of government information
- Loss of information from insecure outsourcing
- Electoral fraud and vote rigging (especially for e-voting)

Fraud against the Commonwealth

- AIC Report 2007-08 (45% of agencies reported 873,401 incidents)
- CDPP 2007-08 (4,055 individuals prosecuted for fraud - $84.4 million)
- AFP 2007-08 (2,178 finalised economic crime cases – $236.7 million)
- ANAO 2001-02 (11,162 fraud allegations reported by 47/106 agencies (44%); internal fraud $2.63 million, external fraud $90.7 million (min.)

Organised cybercrime risks for government

Unauthorised access to government premises / networks

- Access to disable security systems
- Embedded malicious code installed by corrupt insiders
- Displacement risks of violence to obtain access codes

Promoting and financing of terrorism

- Use of ICT to communicate and to disseminate propaganda
- Collection and transfer of funds by and to terrorist groups
- Use of ICT to plan and execute attacks e.g. *Lohdi case* (2006)
- Attacks aimed at disrupting ICT in target countries

Threats to national information infrastructure

- Disruption of supply chain management systems
- Attacks on financial agencies' networks
- Threats to energy resources and supply

Environmental crime prevention

Increasing the effort required to offend

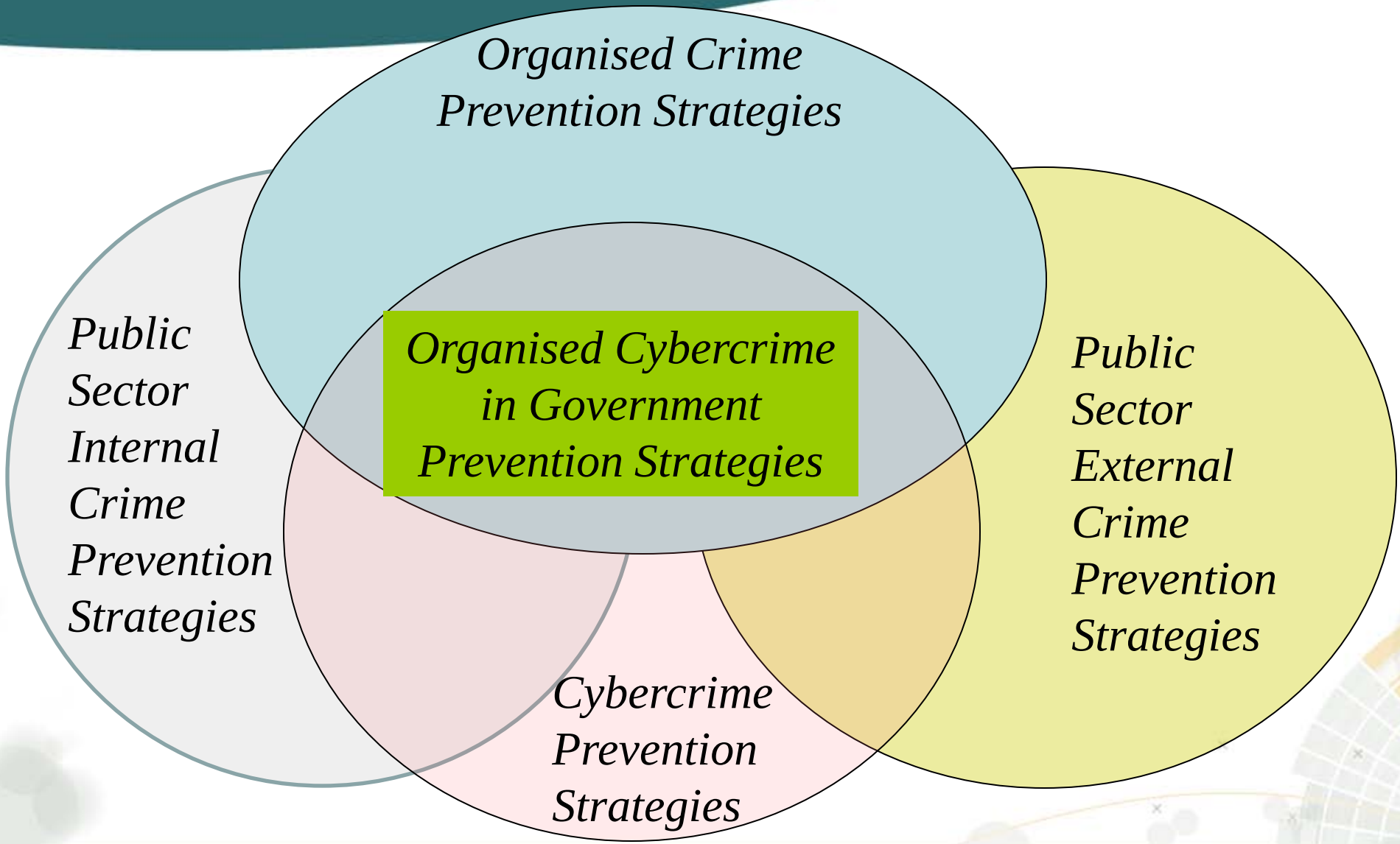
- Target hardening, access control, deflecting offenders, controlling facilitators

Increasing the risk of apprehension

- Entry-exist screening, formal surveillance, surveillance by employees, natural surveillance

Reducing the rewards of offending

- Target removal, identifying property, removing inducements, rule setting, confiscation of the proceeds of crime


Organised Crime Prevention Strategies
Public Sector Internal Crime Prevention Strategies
Organised Cybercrime in Government Prevention Strategies
Public Sector External Crime Prevention Strategies
Cybercrime Prevention Strategies

Responses

Interfering with organised crime networks

- Removing key figures that are essential for the functioning of the group
- Preventing key figures from communicating effectively
- Improving personal identification to enhance detection
- Monitoring of IT equipment and usage
- Increasing routine formal surveillance
- Using natural surveillance by group members
- Removing the status rewards of group membership
- Deterrence through prosecution and punishment
- Confiscation of the proceeds of crime

Cutting the ties

Rigid hierarchy

- Cutting out key leaders

Devolved hierarchy

- Removing regional leaders

Core criminal group

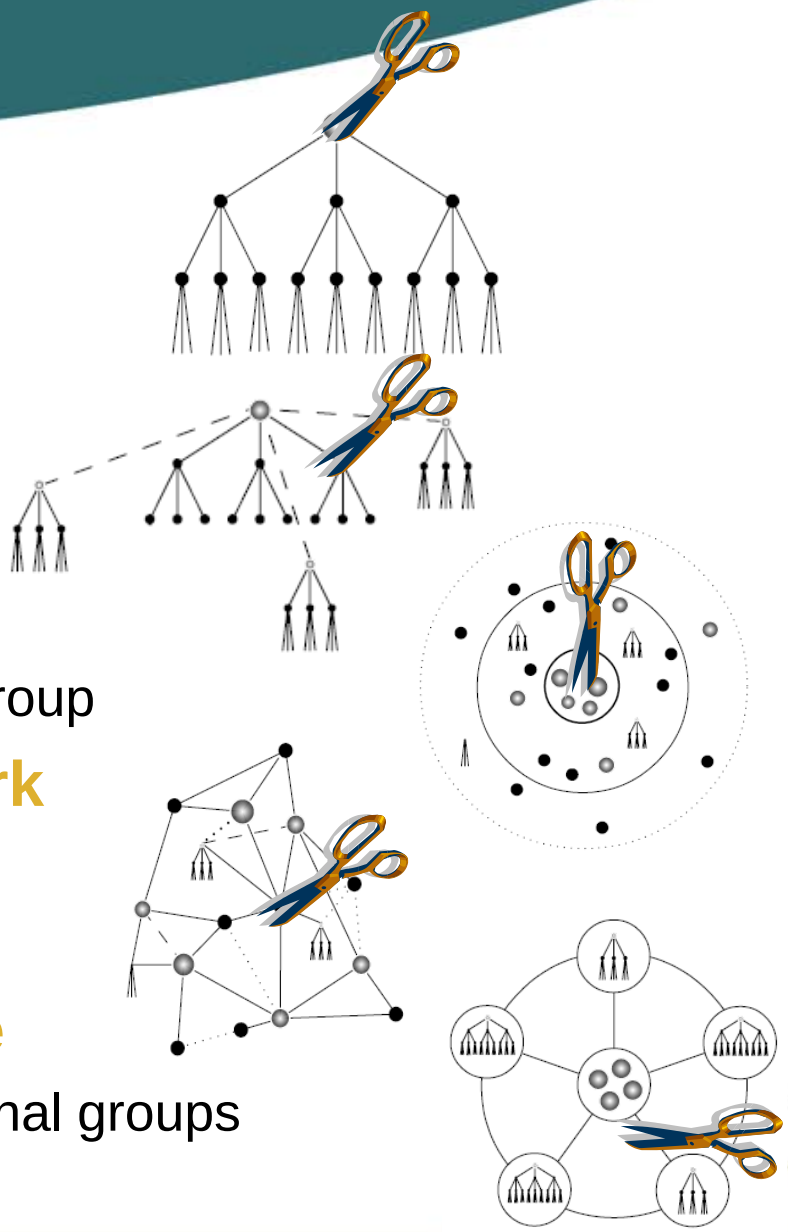
- Breaking up a small core group

Organised criminal network

- Destroying nodal players

Hierarchical conglomerate

- Cutting links between criminal groups



Responses

Information sharing

- Between and within law enforcement
- Between public sector agencies and law enforcement
- Between public sector and private sector (IT, banking etc)

Financial intelligence

- Effective reporting of suspect transactions
- Analysis of reported transactions
- Timely feedback to government agencies to enhance prevention

Telecommunications intelligence

- Capture and sharing of telecommunications intelligence
- Ability to share intelligence with law enforcement
- Global networking of intelligence data

Impediments

Geography

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

Identity

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

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