GREY NETWORKS

A New Look at an Old Risk

- "…if I don't want something to happen in Defence my tactic is to send it on whatever process we have designed, because that is an absolute guarantee that it will not succeed."

Air Marshal Geoff Brown,
Chief of Airforce, 2014

AGENDA

- Definition of Grey Networks
- Case Study 1
- Assessment
- Case Study 2
- How to Prevent, Detect and Respond to Grey Networks
- Conclusion

GREY NETWORKS DEFINED

GREY NETWORKS

- A group or system of interconnected people that use informal ties and employ operational security measures and/or clandestine techniques through varying degrees of overt, or more likely covert, activity to conduct activities to achieve legitimate purposes (Callan, 2016).
- Grey Networks are a facilitator of institutional corruption and dark (illicit) networks.
- Note: they operate legally and ethically!

NETWORK STRUCTURES

	Structure			
Network type	Actors & organisation	Ties	Topology	Participation
Bright Overt: efficiency as core outcome	Distribution of tasks among actors is transparent & directional; clear boundaries; clear structure; smaller size	Formal & informal; multiplex ties/exchanges	Dense connections; centralised; meshed under- layer of connection (sub-network)	Motivated by resources or professional norms & shared values; public interest
Dark Clandestine: Secrecy over effectiveness	Distribution of tasks & exchanges opaque & unidirectional; structure within organisation loose	Informal; unidirectional; single exchange	Loose connections; decentralised; dispersed layered cells	Motivated by self-interest; relies on existing inter- personal/organisational network

(Lauchs, Keast & Le 2011, p.9)

GREY NETWORK STRUCTURE

Structure				
Network type	Actors & organisation	Ties	Topology	Participation
Grey **Uncertain: Defensiveness over effectiveness**	Distribution of tasks among actors is opaque unclear boundaries clear structure: larger size	Formal & informal; multiplex ties/exchanges	Dense connections: centralised with meshed under-layer of connection (sub-network) in each major network. Loose connections: decentralised between differing networks.	Motivated by self-interest Relies on existing inter-personal/organisational network

HOW THEY FORM

- A team is formed containing competent individuals.
- Due to structure, culture, resourcing or leadership the team is incompetent (the individual team members are still competent).
- The team gains control of the information on its project or activities, and acts as a broker between its main organisation and any stakeholders
- As it begins to operate it realises it cannot achieve its goals or it has some form of failure due to its incompetence as a team.
- The team then uses it control of information to create a power imbalance to protect itself and the project.
- This power imbalance is the strategic influence that creates institutional corruption.
- This institutional corruption diverts the organisation from its primary goal

THE RISK

- Grey Networks:
  - blind organisations
  - corrupt other processes and ensure stakeholders compromise
  - allow the formation of illicit networks to form or at least the connection to do so

CASE STUDIES

CASE STUDY 1: MU 90 TORPEDO

- Mid-1990 – ADF Study said new light weight torpedo required as current torpedo not up to requirements.
- 1998: Phase 1 Replacement project approved for five combat platforms
- 2017: Project not complete. Of five platforms four are out of service and the final one is going out of service in 2020. ADF uses two light weight torpedo types, one for aircraft and one for ships.

BEGINNING OF THE PROBLEM

- Defence rushed into applying a project Alliance approach without due consideration or understanding, which led to many of the problems the project was suffering.
- JP 2070 had not followed the recommended procurement process for project alliances as described in Defence's recommended procurement guidelines for alliance contracting ('Guidance on Alliance Contracting in the DMO', version 1.5, 2001).
- There was a lack of full analysis and appreciation of the issues before deciding to accept an alliance approach.

(Australian National Audit Office 2009)

BEHIND THE PROBLEM

- Three distinct networks operating:
  - Project Team
  - Navy
  - The industry consortium

- The Project Team owned the relationship with industry and controlled the information flow to the Department and Navy
- The Project Team refused to give information to the ANAO
- The Department was ineffective or labile in its response to emerging threats
- ANAO was ineffective in its oversight and refused to flex its muscle

ASSESSMENT

- There was interconnected personnel or interconnected groups of personnel.
- The project team had greater power than the others through information control.
- The project team took unilateral action, without reference to advice, or outside the legitimate processes
- The level of interaction became ingrained and the response to emerging threats outside of the project team became limited and ineffective.

CASE STUDY 2: TIGER ARH

- Commenced in the late 1990's
- Designed to give the Australian Army an all-weather reconnaissance and fire support platform to ground troops
- De-risked the process by making the decision to purchase "off the Shelf"
- Project has delivered seven years later than planned, with 76 capability deficiencies, sixty of which are considered critical
- During this time, the Australian Army pilots responsible for flying the aircraft refused to fly in it for safety reasons
- The small size of the fleet has generated additional costs borne by the users.

BEGINNING OF THE PROBLEM

- The selection process for this aircraft did not follow its own tender evaluation plan
- The procurement requirement that the purchased aircraft should have commonality with other ADF equipment was not included
- The project did not develop or submit a source selection report, which should have occurred in accordance with extant Defence policies
- The project could not explain why this occurred.

(Australian National Audit Office 2005)

BEHIND THE PROBLEM

- Failure to consult on the first Australian built aircraft and delivered Aircraft Five without seeking clearance from Army
- A deliberate decision by the Defence Acquisition Organisation (DAO) not to advise the capability manager (and by extension it is assumed government) of information. (Australian Senate 2012, p.20)
- DAO preferred the information of the manufacturer to the advice provided by the in-house ARDU pre-contract report (Australian Senate 2012; Australian National Audit Office 2016)
- A lack of information being passed internally within Defence (Australian National Audit Office 2016)

THE PROJECT TEAM

- There was a drive to accept only information that suited the project team
- The project team did not hand over information to the capability owner leading to Army being unable to identify incoming risks.
- The project team took unilateral action, without reference to advice, or outside the legitimate processes
- The level of interaction became ingrained and unilateral action outside of the networks/groups is limited

HOW TO PREVENT DETECT AND RESPOND TO GREY NETWORKS

PREVENT

- The capability manager owns the project, not the project team
- Regular reporting and meetings, run by the capability manager
- Employ simple processes, and follow them
- Develop KPI that deliver the project not the politics

DETECT

- Red Flags:
  - Late or missing reports
  - Lack of timeliness
  - High number of external meetings and travel
  - Failure to attend meetings with capability manager
  - Deliverables aren't delivered, but you don't find out until its too late!
  - Capability managers can't talk to external stakeholders without "permission" and the project team involvement

RESPOND

- Zero tolerance to process failure (within reason)
- First failure requires immediate action
  - Review
  - Revise
  - Retrain
- Capability Manager deals with external success and failure

DEFEATING GREY NETWORKS

- Transparency
- Diffusion of accountability
  - No one party has control over information
  - The capability owner retains the funds
  - Stronger governance around reporting
  - Audit needs to look closely at reporting not performance
- Take action when the issue arises – zero tolerance to dumbness

CONCLUSION

- Grey Networks are not a new phenomenon
- They exist, and they are the bigger risk to an organisation that illicit networks – ask Enron
- They can be defeated, but it requires moral courage

QUESTIONS?