AFP
AUSTRALIAN FEDERAL POLICE

Radiation and National Security in Australia

Dr George Koperski

Australian CBRN Data Centre

35 ARPS Adelaide October 2010

Contents

- Malevolent use of radioactive material
- Radiation protection & source security nexus
- COAG national security strategy
- The Australian CBRN Data Centre
- Technical Intelligence process
- Summary

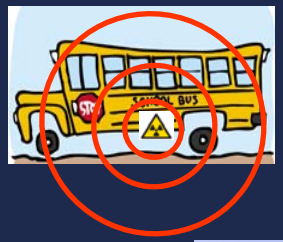
Malevolent Use of Radioactive Material

- Radiological Dispersal Device (RDD)

  Explosive

  Non-explosive

- Radiological Exposure



  Device (RED)

- Attack on facilities

- Targeted radiation poisoning

Radiation Protection & Source Security Nexus

Radiation Safety

Radiation

Protection

+

Source

Security

COAG National Security Strategy

- 2002 COAG agreed to national review of *regulation*, *reporting* & *security* re storage, sale & handling of hazmat (NH_4NO_3 , RBC)
- 2005 NCTC developed the four-pronged National CBRN Security Strategy to cover prevention, preparedness, response & recovery (PPRR) related to potential/actual misuse of the materials
- 2007 COAG agreed to recommendations of the *Report on the Regulation and Control of Radiological Material* to minimise risk of misuse of such material by terrorists
  - (R6) "Cradle to Grave" reg framework for security of rad sources
  - (R10) National radioactive source incident notification system
  - (R11) National radioactive source register
- ARPANSA - lead agency for implementing and co-ordinating the response to COAG 2007 Recommendations
- 2007 CoP for the Security of Radioactive Sources

The Australian CBRN Data Centre

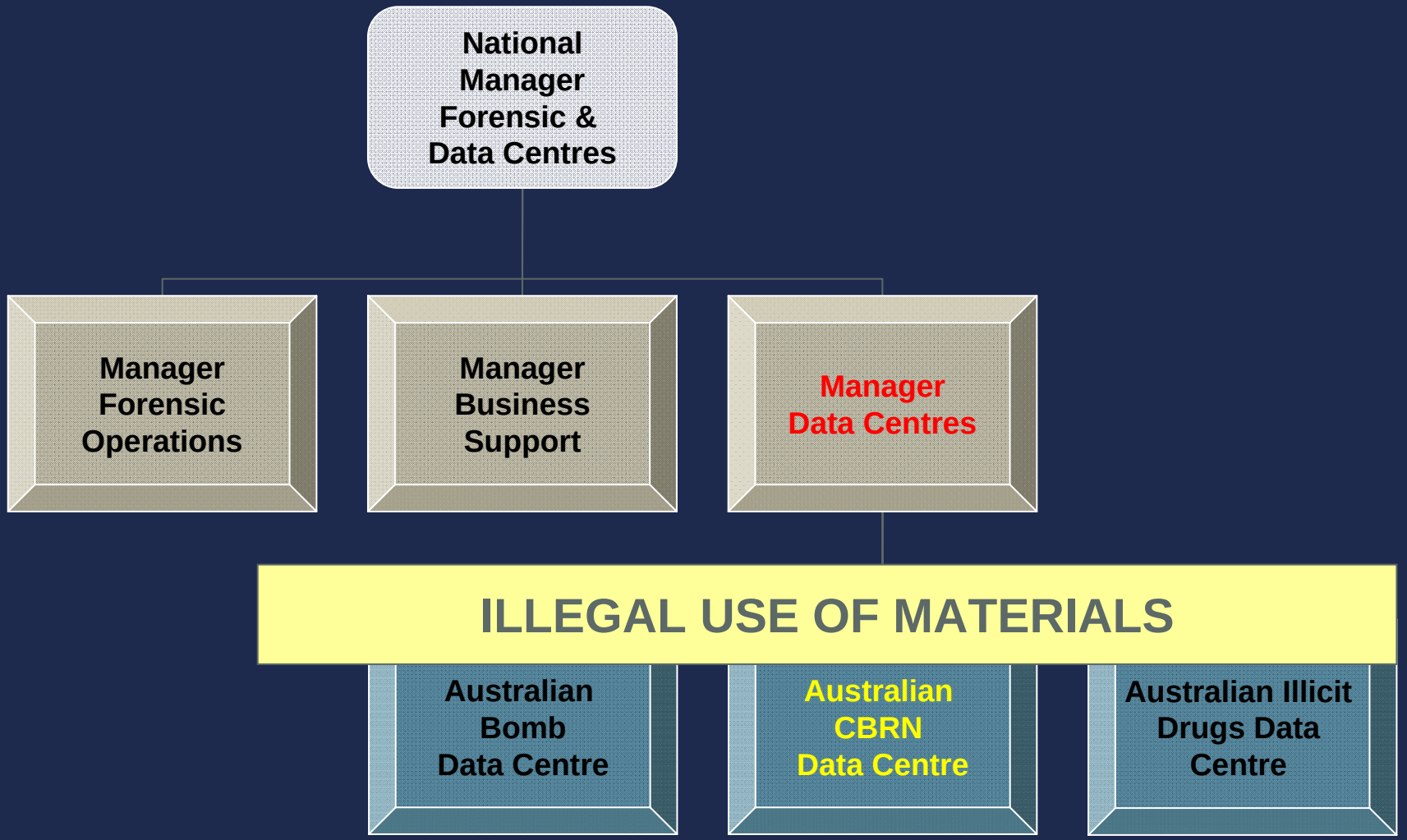
Opened 2 July 2007 by the Attorney General

The Australian CBRN Data Centre (ACBRNDC)

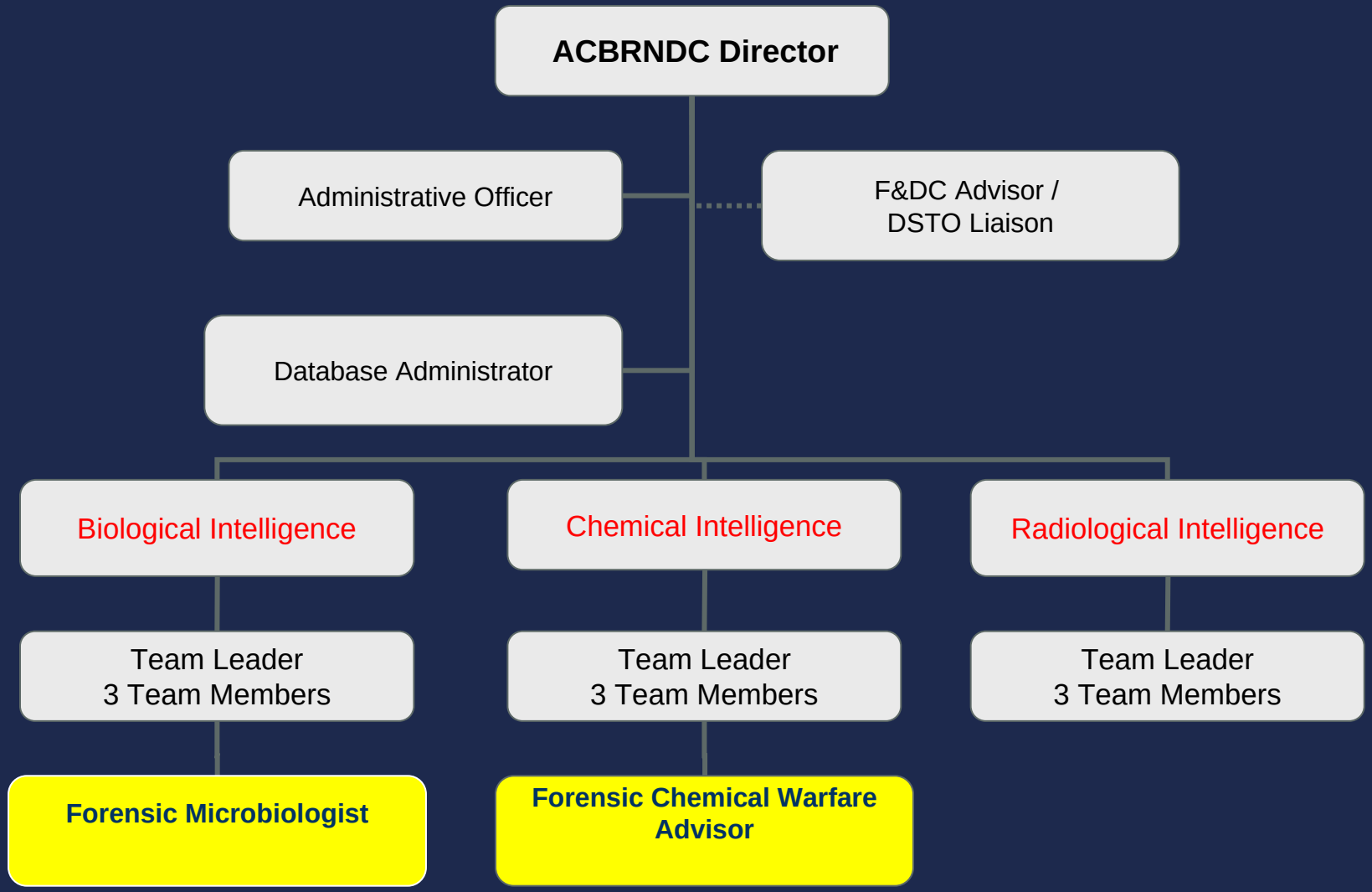
Mission Statement

Enhancing Australia's capability to prevent, prepare and respond to *malicious use* of chemical, biological, radiological and nuclear agents by providing *technical intelligence* products and services in order to *support* law enforcement and national security objectives

Forensic and Data Centres



The Australian CBRN Data Centre



ACBRNDC Stakeholders

ACBRNDC Data Inflow

- CBRN Incidents
- Theft of CBRN material
- Intelligence
- Terrorist literature
- Scientific literature
- Australian CBRN infrastructure

ACBRNDC Data Analysis

- New CBR agents
- New trends
- Links between events or agents
- Feasibility assessments
- Impact assessments
- Scenario evaluation
- Recipes evaluation

Products

- Warnings
- Intelligence assessments
- Policy advice
- Briefs
- Advice for preparedness

CBRN Terrorist / Intelligence Cycle

Technical & Forensic Intelligence

Forensic Investigation

INTERDICTION

Intelligence Indicators

disseminate

deploy

produce

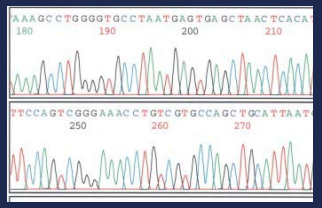
acquire

plan

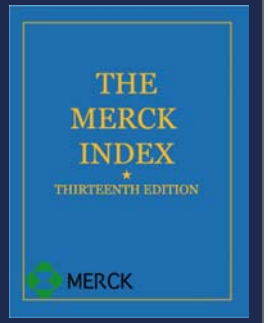
Terrorist Cell

Forensic Intelligence

Forensic evidence

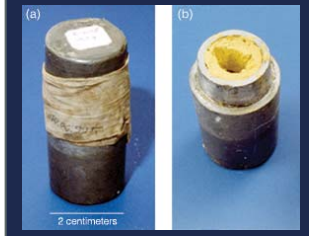


Technical Information



Analysis

Operational Intelligence



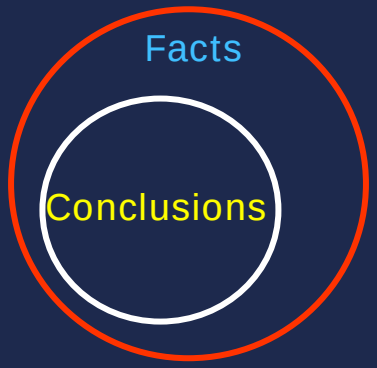
Forensic Intelligence products

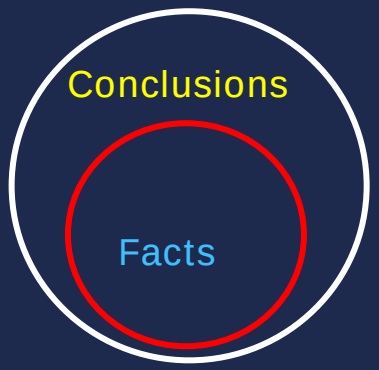
Technical Intelligence

- Technical Intelligence is the process of *adding value* to information through *analysis* in order to provide *insight* and to *influence decision* making

deductive *vs* *inductive*

reasoning





- Needs to be distinguished from Operational Intelligence

Intelligence *Indicators*

- Preparation often difficult to detect
- Terrorist intent almost never advertised
- Perpetrators unlikely to claim responsibility

Shoko Asahara

BUT

- Indicators of *planning*, *acquisition*, *production*, dissemination and behaviour maybe present

Bruce Ivins

Indicators of *Planning*

- Terrorist organisations recruiting from universities, laboratories, hospitals, industry




- Connections/interest with facilities holding R/N material
- Interest in R/N related infrastructure, materials and incidents
- Interest in extremist literature
- Recovery of periodicals, manuals

or web resources

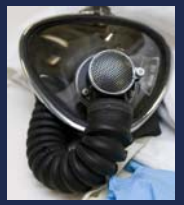
Indicators of *Acquisition*

- Diversion of R/N materials from supply chain
- Purchase of specialised componentry
- Purchase of materials known to be potentially dangerous
- Fraudulent acquisition from commercial suppliers
- Theft and illicit trafficking

Indicators of *Production*

- Modification of premises (e.g. taped windows, modification of ventilation systems)

- Unusual or suspicious possession of:
  - PPE
  - Lead bricks
  - Radiation detectors



- Recovery or evidence of acquisition of radiation sources & explosives

Indicators of *Dissemination*

- Presentation of people at health care facilities with
  - atypical symptoms
  - unusual lesions
- Discovery of people/areas radiologically contaminated

Suspicious behaviour

- Unusual or out of the ordinary behaviour in individual or a group
- Could come from an outsider or a trusted insider

- No definitive indicators of suspicious behaviour
  - based on observations, subjective judgement, circumstances, ‘gut feeling’ that something is wrong

Summary

- Clear potential exists for misuse of radioactive materials
- Contemporary *Radiation Safety* has two inseparable components: *radiation protection* and *security of radioactive material*
- COAG Recommendations form the basis for implementation of the security of radioactive material in Australia
- Interagency cooperation nationwide is the necessary condition of the implementation of radioactive material security
- Technical Intelligence (TI) assists the decision making process aimed at preventing, preparing for, and responding to malicious use of CBRN agents
- The role of the ACBRNDC is to provide TI products and services in support of law enforcement and national security objectives focused on malicious use of CBRN agents

QUESTIONS ?


Acquisition
Planning
Suspicious behaviour
CBRN Event
Dissemination

AFP

AUSTRALIAN FEDERAL POLICE

cbrndc@afp.gov.au