

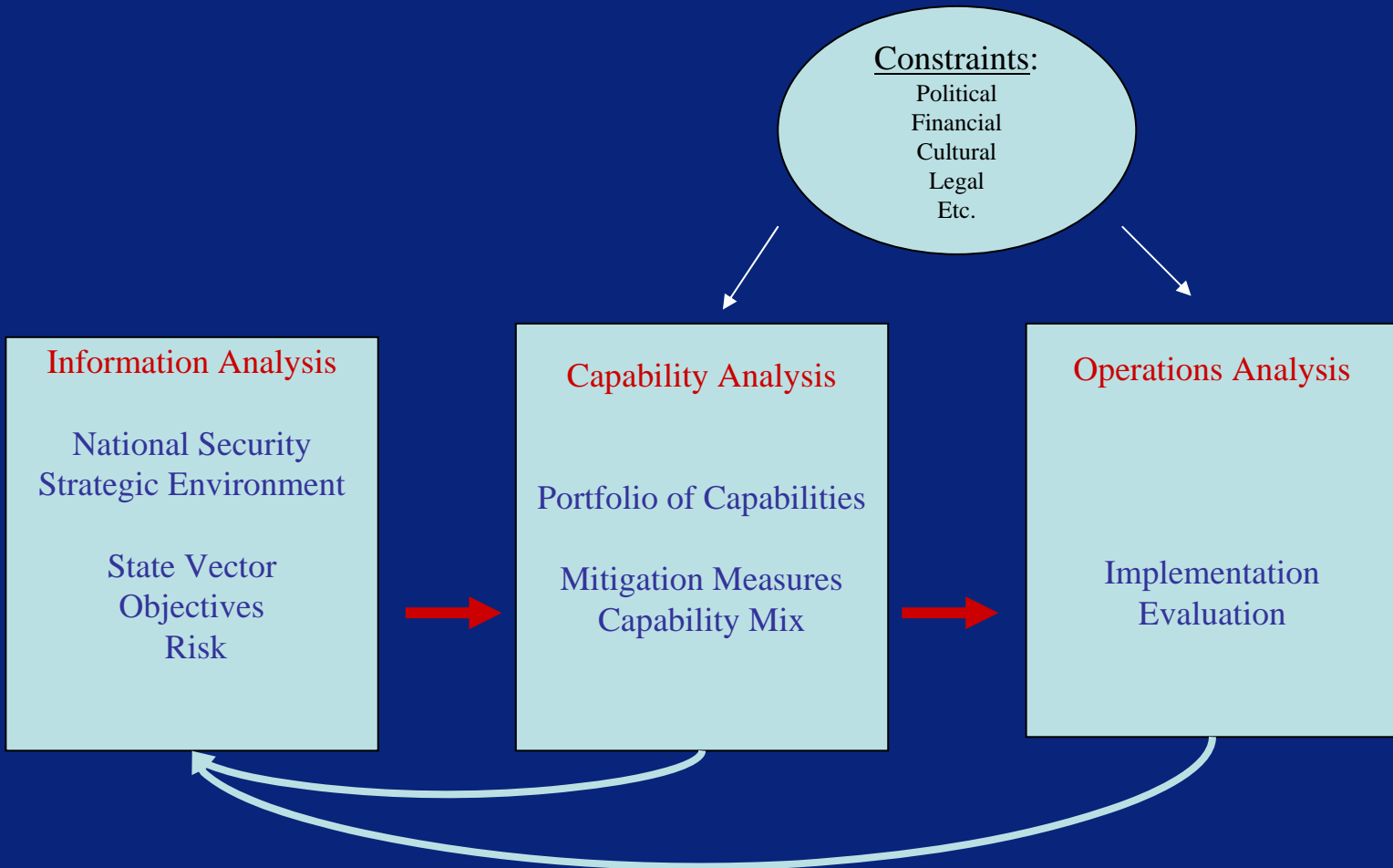
Metrics for National Security Capability Development (Dynamic Risk Models)

Alexei Filinkov and Ian Fuss



Australian Government
Department of Defence
Defence Science and
Technology Organisation

Dynamics and Levels of RM





Risk Management

- Establish Context & Identify Risk: **State Vector**
 - Domestic, regional and global components
 - Domestic: by CI/KR items (by type of threat, by agencies, etc.)
 - Principal components analysis
- Analyse & Quantify Risk: **Dynamics of State Vector**
 - Takes into account terrorist motives, capabilities and intents
 - mixture of Analytic, Deliberative and Practical methods
- Mitigate Risk: **Modified Dynamics of State Vector**
 - Agencies activities (e.g. Physical Security, I&S Operations), new technologies, policies, training & education, etc.
 - Can use Real Options approach to value, compare and prioritise various mitigation portfolios
- Monitor – Review – Communicate – Consult



State Vector

The State Vector can be arranged according to various categories such as

- CI/KR (Critical Infrastructure/Key Resources) items
- Types of threat
- Agencies
-
-



Critical Infrastructure/Key Resources Areas

1. Agriculture and Food
2. Defence Industrial Base
3. Energy
4. Public Health and Healthcare
5. National Monuments and Icons
6. Banking and Finance
7. Drinking Water and Water Treatment Systems
8. Chemical
9. Commercial Facilities
10. Dams, Emergency Services
11. Nuclear Reactors, Materials and Waste
12. Information Technology
13. Telecommunications
14. Postal and Shipping
15. Transportation Systems
16. Government Facilities

Source: National Infrastructure Protection Plan (NIPP) 2006,
Department of Homeland Security, USA

Structure of State Vector

Air Transport Example

Area 1 | Area 2 | ... | **Area 15** | Area 16

Area 15 : Transportation Systems

Sub-Area 15.1 | ... | **Sub-Area 15.j : Air Transportation Systems**

Sub-Area 15.j : Air Transportation Systems

Sub-Area 15.j.1 | ... | **Sub-Area 15.j.n : a CTFR airport**

Sub-Area 15.j.n : a CTFR airport

Physical Security | Information Security | Operational Security | etc. ... |



NSST's R&D Capability Framework identifies the following types of threat:

- Chemical
- Biological
- Radiological
- Nuclear
- Explosives
- Cyber
- Human
- Nature (all hazard)



Threat Level - Phase Space

Desirable Part



States that require some adjustments to the dynamics
of State Vector

States that require Emergency Measures
(caused by major incidents, catastrophic events, etc.)



Some Definitions

- **Objective**: our aim is to keep the State Vector in the desired part of the Phase Space
- By **Risk** we therefore understand the *possibility of not achieving this Objective at some time in the future (due to uncertainties and unknowns)*
- **Risk Mitigation Strategies** are designed to minimise this possibility



Phases

- **Pro-Active** (anticipate, prepare, prevent, protect)
- **Re-Active** (respond, recover, attribute)



Phase Space

Pro-Active

Desirable Part



Re-Active

States that require some adjustments to the dynamics
of State Vector

States that require Emergency Measures
(caused by major incidents, catastrophic events, etc.)

Re-Active
Emergency

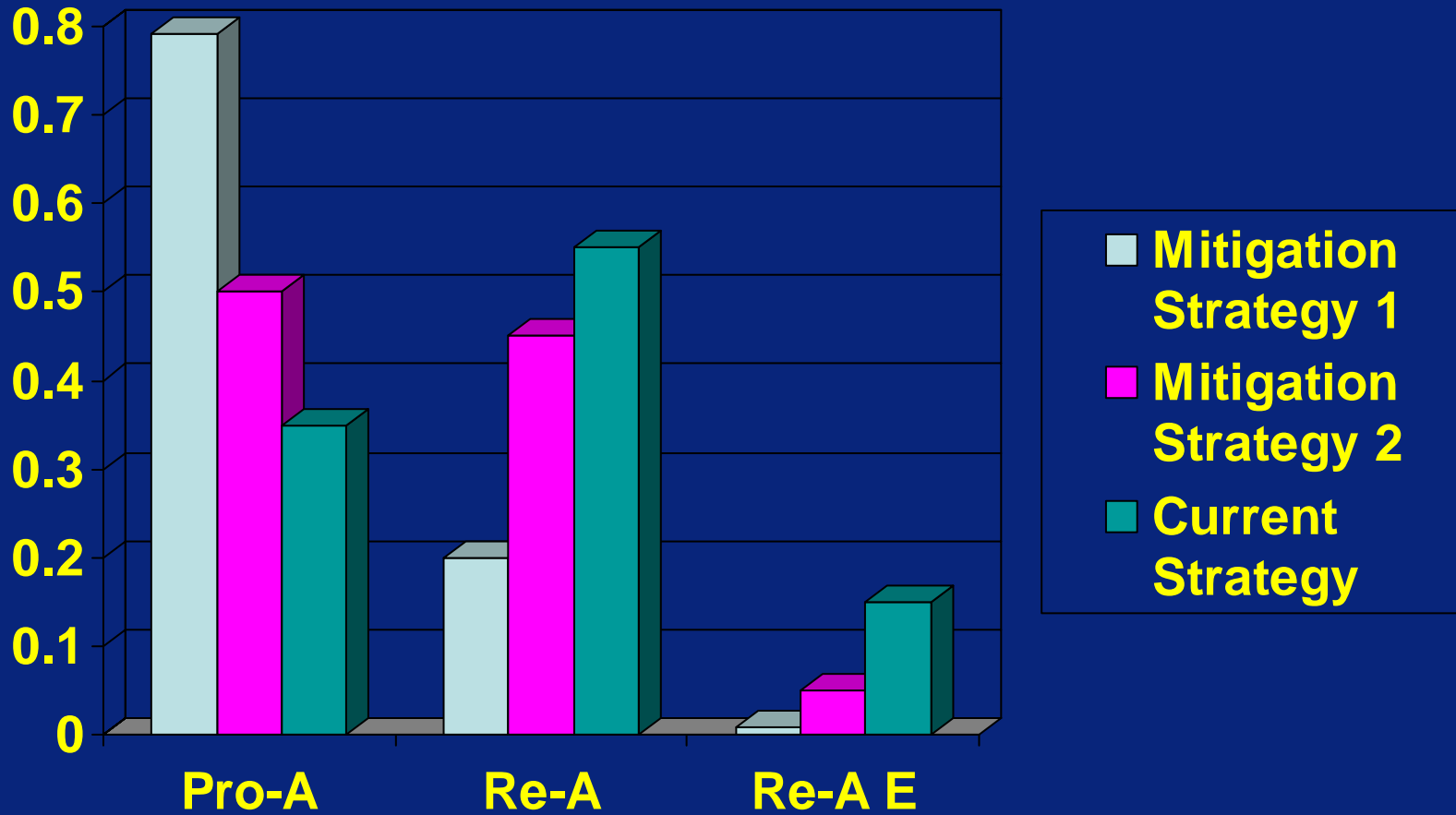


Dynamics of State Vector

1. *Dynamics* are driven by the National Security Strategic Environment and in particular they depend on
 - our Capabilities and Intent
 - Capabilities and Intent of adversaries
2. Understanding these Dynamics is associated with *evaluation* of our current Capabilities and hence it leads to the *analysis* of Capability Gaps and Capability Development
3. Note that by *capability* we mean not just equipment, but also personnel, training, doctrine, stockholding, etc.



E.G.



A simplified example of a probability distribution



Levels of RM

Our *Objective* is to stay in the Pro-Active area but we have to be ready to use Re-Active and Re-Active Emergency measures, which involves

- different time scale for specific Objectives
- different Mitigation Mixes and Strategies
- different Agencies



Levels of RM

When we choose a Mitigation Measure, we assume that the selected Capability Mix would deliver certain expected effects with a certain rate of success. This formulates specific *Objectives* for the Agencies that are involved in this Mix. Their Risk is that the expected effects are not delivered with the estimated rate of success. This Risk might be driven by various uncertainties and unknowns, such as human factors, financial and legal matters, adversaries' counter-measures, forces of Nature, etc. – RM continues!



Australian Government
Department of Defence
Defence Science and
Technology Organisation

Discussion/Questions



Risk in Australia

Risk Management Institution of Australasia Limited (RMIA),
the peak body for risk management practitioners

RMIA is committed to:

- Promoting and furthering the interests of risk management
- Providing a forum to exchange views and experiences
- Promoting educational activities and research
- Accrediting risk management education
- Co-operating with like-minded organisations
- Promoting the Certified Practicing Risk Manager designation

Members span a wide variety of industries and professions, including the corporate and government sectors. RMIA is a lead organisation in the development and promotion of the Risk Management Standard, AS/NZS 4360.



Risk in Australia

The Research Network for a Secure Australia (RNSA)

is a multi-disciplinary collaboration established to strengthen Australia's research capacity to enhance the protection of the nation's critical infrastructure from natural, human-caused, or accidental disasters, and terrorist acts.

RNSA will facilitate a knowledge-sharing network for research organisations, government and the private sector to develop research tools and methods to mitigate emerging safety and security issues relating to critical infrastructure. The network will integrate complementary, yet diverse research areas including physical and information infrastructure security, and surveillance and intelligent systems.



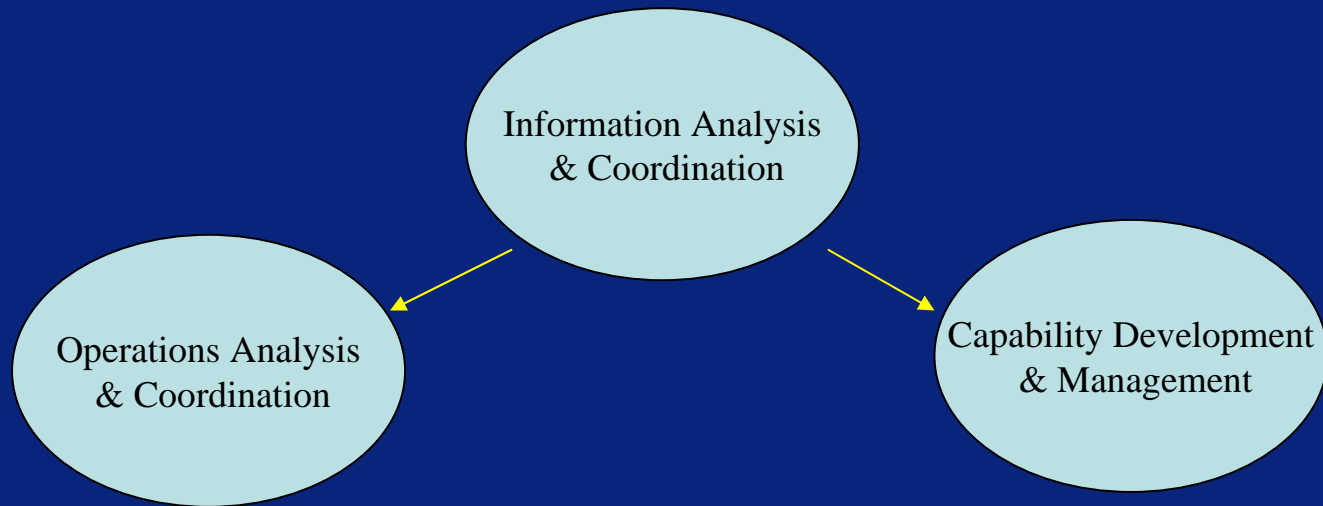
Risk in Australia

Australian Centre of Excellence for Risk Analysis

The Australian Centre of Excellence for Risk Analysis (ACERA) was established in the School of Botany at the University of Melbourne on March 1st, 2006, a result of a Federal Government election commitment. It will develop the practice of risk analysis by creating and testing methods, protocols, analytical tools and procedures.

National Security Framework

Functional Elements



Policy and Law
Coordination

Outreach, Education
& Public Relations

S&T Support and
Coordination



Information Analysis & Coordination

- **Function: identify, analyse and quantify risks**
 - **Receive /request/source** information from various sources, including intelligence, other government and non-government agencies, business partners, media, academia, BoM , etc.
 - **Analyse** information, populate the State Vector, determine it's dynamics and perform the Principal Components analysis
 - **Represent** information in a coherent and accessible form, adequately disseminate it
 - **Inform** the Operations Analysis group, collaborate and support their analysis of immediate , short-term and long-term mitigation measures
 - **Inform** the Capability Development group and support their analysis of current and future capabilities



Operations Analysis & Coordination

- **Function:** Analysis, prioritisation and coordination of mitigation measures
 - Analysis, valuation and prioritisation of mitigation measures (including effectiveness and cost):
 - Baseline everyday security
 - Response to specific and general threats
 - Response to catastrophic events
 - Coordinate efforts of federal and state agencies, industry partners, social and religious organisations, etc.



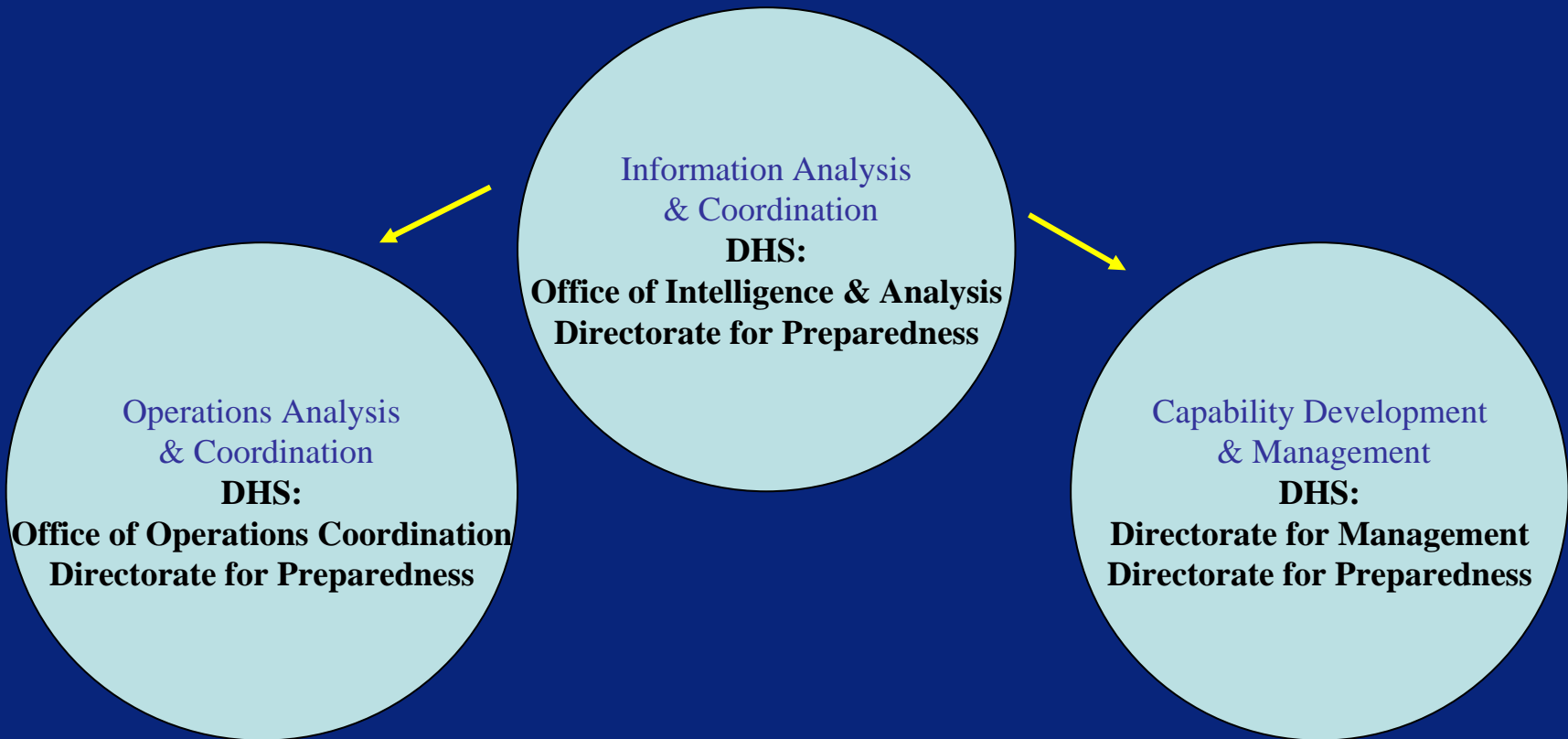
Capability Development & Management

- **Function:** analyse & manage current and future capabilities
 - **Identify** capability gaps and **plan** capability development according to dynamic analysis of strategic environment
 - **Analyse** all Fundamental Inputs to Capabilities (equipment, training, doctrine, stockholding, etc.)
 - **Form** and **manage** a Capability Portfolio that would allow timely deployment of dynamic and flexible capability mixers
 - **Sustainability** analysis



National Security Framework

US mapping





National Security Framework

US mapping

Policy and Law
Coordination
DHS:
Directorate for Policy

Outreach, Education
& Public Relations
DHS:
Office of Public Affairs
HS-Centers of Excellence

S&T Support and
Coordination
DHS:
Directorate for S&T
HS-Centers of Excellence

RAND
RMS
SANDIA



Risk Management approach to support decision making:

- Risk based resource allocation
among alternative classes of threats or targets
- Threat based investments and policies
based on identified threats and vulnerabilities, assess alternative mitigation measures against a class of threats
- Site or Asset specific investments
- Acting on pieces of intelligence