MOBILISATION REVIEW

Purpose

1. This report provides a high-level assessment of mobilisation planning in Defence and identifies the need to improve the mobilisation planning framework across Defence in response to significant changes in Australia's strategic outlook.

Background

2. Australia is a largely de-industrialised multi–cultural nation. It is highly connected to the global commons and has limited diversity in imports, exports and tax revenue. This situation leaves the nation exposed to major disruptions of global governance and supply, such as could be expected in the event of a major war or global catastrophe. Such disruption would require a national response.

3. ADDP 00.2 defines Mobilisation as 'The process of moving from the prepared state for a range of contingencies to being ready to execute a specific operation.' One useful approach to strategic consideration of mobilisation is that it has three broad components: military / Defence, economic (of which industry and infrastructure is a major part) and society.

4. Planning for mobilisation in response to a range of possible contingencies is a subset of preparedness management, which itself is a specialised form of risk management within the Department of Defence (Defence).

5. The geo-strategic environment is more uncertain than it has been for many decades and Defence needs to have confidence that its planning arrangements are appropriate for the contemporary context. Of particular concern, is the likely unconventional approach that could be taken by potential adversaries that could negate much of the benefits of conventional military planning. In particular, the level of security comfort that Australia's geography has previously given us has been noticeably reduced by the development of cyber and other capabilities that make national security borders very porous.

6. Consequently, in 2017 VCDF initiated a review of mobilisation architecture, the context in which it could occur, the framework for planning and action, and relevant policy and doctrine. The review is not attempting to propose the likely contingencies Defence will face in in the future.

7. This paper is a high level assessment of the state of mobilisation planning in Defence to inform subsequent mobilisation planning across Defence.

8. While considerable Defence mobilisation has occurred at lower levels since the 1998 lead up to Operation INTERFET, there has been limited consideration of formal planning for large scale (including national) mobilisation since the Vietnam era or the need to mobilise in less traditional ways.

9. Despite the extended period of ADF operations since the late 1990s, the mobilisation impact on the Australian economy and population has been limited to a narrow element of Defence industry and some employers of Defence reserves. There is, therefore, a need for a comprehensive review of mobilisation planning to better prepare Defence for an increasingly uncertain strategic outlook.

Data Gathering Process

10. In developing this report, information and perspectives were gained from the following sources:

a. senior personnel across Defence Groups, as listed in annex A;

b. US think tank personnel (CSBA, CSIS, CNAS, Eisenhower Institute);

c. extant legislation, doctrine, policy, procedures and guidance;

d. open source articles on mobilisation related issues;

e. foreign military internet websites;

f. ANU National Security College workshop 'Future Cyber War: How would Australia mobilise a response' held in November 2018, summary provided at annex B;

g. Engineers Australia Workshop on the effects of a collapse in global governance on the global supply chain held in February 2019, summary provided at annex C; and

h. Head National Resilience Task Force and Australian Vulnerability Profile Project members from, CSIRO and Emergency Management Australia.

OBSERVATIONS

General

11. Across Defence there are a number of discrete activities considering levels of mobilisation that would exceed recent Defence experience. However, most of these activities are being conducted in isolation. Related activities are occurring in VCDF Executive, Joint Capabilities Command, CASG, the Capability Managers, Defence Legal, DPG, SP&I Group, and E&IG.

12. There is a need for significantly improved whole of organisation arrangements to coordinate these efforts to maximise the benefit, adequately comprehend different aspects of an issue and more effectively use resources with a view to reducing the risk of nugatory or counter-productive work. Senior leaders have expressed concern over inadequate definition of accountabilities for planning mobilisation and managing some associated logistics issues.

13. s33(a)(ii)

14. The foregoing comments (and much of the Defence input and related initiatives) focus on traditional concepts of military mobilisation. However, the increasing prevalence of grey zone operations and hybrid warfare require Defence to reconsider the nature of attacks that Australia may have to respond to and how the Department may be tasked to respond. For example, the workshops conducted by the ANU National Security College and Engineers

Australia both highlighted a wide range of societal impacts that could arise from an action that does not resemble conventional warfare. Understanding the Australian economic, societal and military vulnerabilities against unconventional attacks is a key question that Defence needs to consider more thoroughly.

15. Furthermore, the concept of mobilisation has always implied authorities beyond peacetime / extant approvals. Increasingly, mobilisation is broader than just the ADF or the Department of Defence. While there are a number of Commonwealth mechanisms for related cross departmental coordination, there was a consistent view that they are not adequately supporting medium to long term planning, large scale crises or higher intensity operations; or the potential for unconventional threats to negatively impact Australian society.

Legislation

s4
2

s42

International Benchmarking

23. An initial study to compare and contrast mobilisation planning in Australia with that of other comparable nations has been conducted to identify gaps and opportunities in reviewing the Australian mobilisation framework. The countries examined were the United States, Canada, Poland, Sweden, New Zealand, Japan, Russia and China. They were chosen because they are either members of the Five Eyes Community with demographic and doctrinal similarities to Australia or because they have robust plans, and differing views of mobilisation, to deal with credible strategic threats.

24. The study identified two main approaches to mobilisation. Large states (including the United States, Russia and China) see mobilisation as a means to expand their military forces with a view to achieving strategic aims beyond their shores. By contrast, smaller countries, including Sweden, Poland and Japan, have increasingly emphasised the need to foster resilience against unconventional threats, including cyber warfare, economic risks, resource shortages, and natural disasters.

25. Smaller countries often focus on mobilisation for civil defence duties in local communities for a defined period of time. In these countries, mobilisation planning is a part of education and culture and, as a result, civilians are able to play their part in whole-of-government efforts against significant and unconventional threats. The approach of these countries provides a more robust preparation for circumstances where the civil population is affected at the same time as the military.

26. Australian mobilisation planning is currently based on a traditional approach more suited to a larger country with a large industrial base faced with conventional threats. Arguably, it should fall somewhere between the two extremes mentioned. Consequently, it should be reviewed to include community resilience against unconventional threats that now characterise Australia's strategic environment.

Expectations of Future Mobilisation

27. Future mobilisation arrangements must be able to better respond to both conventional and unconventional attacks.

28. Regardless of whether unconventional attacks relate to Australian agriculture, financial systems, communications or another aspect of society, a whole of government approach will be required. Even if a military kinetic response is not needed, Defence will be expected to support the response to major unconventional attacks that affect social cohesion. To do so, Defence must better understand a broader scope of national vulnerabilities than traditional preparedness and operations planning have provided.

29. The ADF may need to undertake coalition operations alongside countries with which it has not operated in the past. s33(a)(ii)

Personnel

31. s33(a)(ii)

There is a need to comprehend specialisation / trade priorities for reserve service in future conflicts as a selected call-out of reserves is considered a more likely scenario than a general call-out. In particular, tailored strategies may be required for critical specialisations.

32. Recognising the lack of experience in managing a significant call-out, HPC is investigating possible options for processing large numbers of SERCAT 3/5 to SERCAT 7 transfers. Further research is also required to determine how frequently a reservist can be mobilised. US military practice is for reserves to be engaged on one in six deployments / rotations. However, based on their current experience, there is a growing view that is too frequent.

33. There is also a need to critically assess if specialised roles are actually required in uniform. Civilians or contractors may be more practical. Other countries have taken novel approaches in regard to personnel management. In the United States, for example, the State Department has the authority to make someone a temporary government official if necessary to meet immediate government requirements. s42

Health

34. In contrast to other elements of the ADF, the overall health capability is not considered to be a major mobilisation concern. This assessment recognises that the ADF capability is a very small percentage of the overall Australian health capability and reserve medical personnel are already well integrated into deployed operations.

35. A key area of concern is the availability of pharmaceutical supplies. 90 percent of all Australian supplies are imported s33(a)(ii)

JHC has begun to investigate this issue more thoroughly.

36. Furthermore, the World Health Organisation (WHO) expects a significant pandemic to emanate from Asia in next 10 years. While the ADF health capability overall is considered adequate to meet expectations of support most likely to be requested (if at all), there is a possibility that other elements of the ADF could be requested to support civilian authorities with population, herd or crop control.

Logistics / Industry

37. The pervasiveness of logistics and concern about comprehension and awareness of supply chain vulnerabilities were apparent in almost every interview. The most commonly raised issue related to confidence in the supply of consumables in a contingency surge.

38. s33(a)(ii) . Of note there is recognition that contingency operations are significantly different from normal RTS activity and it is not feasible to simply scale up normal usage.

39. Other notable concerns included:

a. s33(a)(ii)

d. Coordination between VCDF Executive, Capability Managers, JOC, CASG, JLC, DIPD and E&IG needs to be improved as the lines of accountability are unclear.

e. s33(a)(ii)

40. A positive observation is the increased focus on surety of supply rather than just reserve stockholding levels. Such an approach recognises that alternative methods of manufacture / sources of supply may be possible in major conflict and can reduce the costs of acquiring and sustaining reserve stocks. s33(a)(ii)

41. The Sovereign Industrial Capability Assessment Framework provides a suitable basis for assessing industry capability priorities. As with many aspects of Preparedness, there are many varied, and sometimes conflicting, factors to be considered. How well the current sovereign capability priorities support mobilisation requirements merits further investigation.

Transportation

42. There are extant road transportation and sealift support panel arrangements in place, and one for rail will shortly be established. However, arrangements for contractor airlift are much less structured. s33(a)(ii)

43. s33(a)(ii)

Further investigation is required to explore options for having greater confidence in accessing logistics transport capacity at times when non-Australian owned options may be more difficult to access.

Society

44. Given Australia's connectivity to the global commons and our reliance on imported manufactured goods, the nation is exposed to major disruptions of global governance and supply that could significantly impact our society.

45. Mobilisation requires personnel, materiel and financial resources to be expended. Large scale mobilisation will require resources to come from the national economy, most likely at the expense of other areas of government funding, with subsequent impacts on the population. In higher end situations, the government would seek to motivate the population to support the national strategies requiring mobilisation. This support can be coerced, which is a short term and inefficient solution that simply creates civil unrest, or a longer term approach could be taken to pre-condition society, as described below. Clearly, mobilisation is not just a military or logistic planning exercise but one that also must include social issues and concerns. Frequently, there is a clash of ideas.[1]

46. In the contemporary era, the ideational battleground is likely to be contested as adversaries employ their own strategies to prevent such a national social mobilisation being

[1] Most of the material on social mobilisation is drawn from a paper titled 'Social Mobilisation in a Contested Environment', written by Dr (GPCAPT) Peter Layton from Griffith University.

successful. Strategies for and against social mobilisation will compete within an all-enveloping social context, an intangible, ideational 'field of battle'.

47. Adversary strategies have significantly improved with advances in information technology, big data and artificial intelligence. These developments allow groups and even individuals to be targeted for active manipulation. Three broad adversary strategy types are discernible: those that aim to: create societal disruption, manipulate existing grievances or try to change people's minds.

48. All three adversary strategies however, need to leverage off the target society to succeed. They all require the audience to be accessible and malleable; the defender in theory has the simpler task.

49. Both foreground and background measures can be taken to resist adversary counter-social mobilisation strategies. Arguably, they should be undertaken whether the environment is contested or not as they inform the population concerning government activities.

50. The foreground measures focus on building legitimacy and creating a strategic narrative. In this, Defence has real agency and choice in determining how these frameworks are fleshed out and implemented. Social mobilisation in time of conflict is unlikely to be successful without significant Defence involvement.

51. Timing is again an important issue. Ideally legitimacy will have been sought from the people and a strategic narrative delivered before adversary contestation strategies are activated. Playing catch-up will make adversary success more likely. Preparing the battlefield however, is a well-known political and military technique. This is an area where the Defence White Paper development process may be able to be adjusted to support.

52. The background measures aim to tilt the 'field of battle' and support the foreground measures of building legitimacy and devising a strategic narrative. They are more those where political leaders and perhaps other departments are better placed to be involved. As Defence has a strong self-interest in successful social mobilisation in times of crisis, it should develop and maintain an understanding of relevant Australian society attitudes so that it can recommend and support appropriate activities. An annual independent longitudinal study could be conducted for under $150,000 per year and, over a number of years, would build-up a valuable body of evidence for engaging with external stakeholders.

Key Assessments

53. s33(a)(ii) . The nature of unconventional warfare has changed significantly and needs to be better understood within Defence. s33(a)(ii)

55. Defence will not be expected to act in isolation and in most scenarios envisaged would not be the lead government department. However, Defence's size, operations planning and execution expertise means that it is likely to be engaged in any national response.

56. Considerable improvement is required across the full scope of Defence mobilisation planning. The broad nature of activities required will require coordination of and engagement from most Groups. Improved coordination across the Commonwealth is also necessary. An initial knowledge map of the more significant activities discovered is at annex E.

Way Forward

57. A program approach should be used to better understand requirements for mobilisation planning in response to either conventional or unconventional threats; coordinate efforts to maximise the benefit, ensure whole of Defence factors are considered and encourage the more efficient use of resources to reduce the risk of nugatory or counter-productive work.

58. These efforts should build on many current or planned activities with some new initiatives required. For many extant activities no change of scope is required to support the desired mobilisation outcomes, while some may require an additional minor element.

59. New study tasks should include assessment of national vulnerabilities, understanding and improving Australian social cohesion and improving Commonwealth government coordination. Once our understanding of how Defence may need to mobilise is clearer, consideration can be given to whether policy or doctrine changes are required.

Recommendation

60. s47C

Conclusion

62. Over the last 20 years there has been considerable conventional Defence mobilisation at the operational level, with valuable improvements in related policies, processes and procedures. However, since the Vietnam era there has been limited consideration of formal

planning for large scale (including national) mobilisation for more significant contingencies. Furthermore, there has been little consideration of mobilisation responses to unconventional attacks on both the ADF or Australian society.

63. Australia's strategic environment is more uncertain than it has been for many decades. The probability of a significant social or economic disruption, a regional operation requiring Australia to lead a multinational coalition or become engaged in a major power conflict is higher now than at any time in the last 60 years. Consequently, Defence needs to have confidence that its mobilisation framework is appropriate for the contemporary context with a better understanding of national vulnerabilities. Specifically, understanding the Australian economic, societal and military vulnerabilities against unconventional attacks is a key question that Defence needs to consider more thoroughly.

64. s33(a)(ii)
across Defence there is considerable diversity of activities contemplating aspects of mobilisation that would exceed recent Defence experience. Most activities, however, are being conducted in isolation and are focussed on responding to conventional threats. There is currently no comprehensive arrangement in place to coordinate these efforts to maximise the benefit, ensure whole of Defence factors are considered or encourage the more efficient use of resources to reduce the risk of nugatory or counter-productive work.

65. Further study with a program approach is required to determine priority areas for mobilisation planning. Considerations to include in such a review are: national vulnerabilities, legislation, command and control arrangements, global supply chain vulnerabilities, personnel planning, transportation capacity, infrastructure and community comprehension and support.

s47F

A.A. BRODERSEN CSC
AIRCDRE
Canberra

28 June 2019

Annexes

A. Senior Defence Officials Consulted
B. ANU NSC Cyber Workshop Summary
C. EA Workshop Summary
D. Mobilisation Related Legislation, Doctrine, Policy and Other Documents
E. Mobilisation Knowledge Map

Annex A

SENIOR DEFENCE OFFICIALS CONSULTED

CJC

DEPSEC CASG

DEPSEC E&I

CJHLTH

CJLOG

DDIO

HDL

HIW

HMSC

HMSP

HNC

HPC

ACAUST

COMAUSFLT

COMD FORCOM

JOC J5

DGWP

DGSP-AF

Director Critical Infrastructure

Director Industry Capability Analysis

Director Industry Strategic Plan

ACM Binskin

ANU NSC CYBER WORKSHOP SUMMARY

Future Cyber War: How would Australia mobilise a response?

1. In November 2018 the ANU National Security College Futures Hub held an interactive workshop on cyber mobilisation readiness with 27 participants from across federal and state government departments, industry and academia. The workshop report is summarised below.

2. The overarching learning was that, while Australia has a lot of plans, systems and relevant experience for managing crises and disasters, a cyber "war" situation is a qualitatively different type of emergency and we are not well set up to deal with it. This is linked to three attributes of a cyber war. First, scope: a cyber war will not be limited to a particular geography, business sector or segment of the community. Second, uncertainty: we will struggle to identify when it starts, how long it will last, and what will be affected next. Third, our vulnerability profile: adversaries will not just exploit weaknesses in computer systems; they will exploit vulnerabilities in society.

3. Another key learning was that "mobilisation" in the context of a cyber war will be a whole-of-nation endeavour. This is because first, many of the targets will be civilian businesses and individuals. Second, the resources needed to respond will be mostly privately held. Third, the centre of gravity is likely to be popular will and resilience.

4. As a result, contingency planning and preparedness cannot just occur inside defence or government silos. When it comes to mobilising for cyber war, a future government's role may be predominantly about coordinating and communicating, rather than directing or controlling. Further work is needed to clarify roles and responsibilities between states, federal agencies and other stakeholders, and to better understand and manage public expectations.

5. Attendees suggested that the following points merit further development and / or research.

- *Uncertainty about thresholds.* Identifying the point at which a single or series of incidents constituted a "cyber war", (i.e. requiring a major response).
- *Clarifying community expectations.* What does the community expect would happen in the event of a cyber war, and how can government manage or amend this expectation?
- *Cyber warfare pipeline.* There is not only a need to ensure we have a skilled cyber workforce, but also that mechanisms exist to quickly access capability in times of crisis.
- *Offensive / deterrence posture.* In a crisis situation, would Australia maintain a sufficient cyber capability and what would it look like?
- *Stress inoculation*. There is a need to prepare the population for cyber contingencies, to reduce the panic and uncertainty that is likely to emerge in the event of a cyber war.
- *Trust and social cohesion.* To reduce the attack surface for adversaries, there is a need to focus on building community trust and social cohesion.
- *Whole-of-nation vulnerability assessment.* Australia needs a clear picture of its vulnerability with input from across governments, businesses, and society.
- *Market mechanisms.* There is a need to ensure that we are using available market mechanisms to lift cybersecurity standards; particularly for small to medium enterprises.
- *Cultural change. To* lift national cyber hygiene, a major pivot is needed—similar to that involved in ensuring widespread adoption of OH&S or car safety.

EA WORKSHOP SUMMARY

Industry Responses in a Collapse of Global Governance

1. The Department of Defence engaged Engineers Australia to convene a workshop in February 2019 for senior engineers with deep industry experience to discuss national mobilisation issues. The workshop report is summarised below.

2. The workshop was attended by 17 engineers with high level expertise in the following sectors: construction; consulting; electricity generation and transmission; liquid fuel; health care; information telecommunications & media; space; manufacturing; mining; transport, postal and warehousing; and water and waste.

3. The workshop looked at the effects of a collapse in global governance, resulting in major disruption to the global supply chain. It sought to identify areas within each sector that would be affected, what those effects might be and how effects within one sector might affect others.

4. The workshop focussed on three areas:

a. immediate effects from one to seven days,

b. impacts if the situation lasts for three months, and

c. actions that could be taken prior to the event that would mitigate the effects identified.

5. The workshop delivered the overarching advice that, in the scenario provided, Australia would suffer massive upheaval over the following timeframes:

a. within one week - job losses, social unease and hoarding;

b. within a fortnight - stocks of imported supplies drawing down, major social infrastructure such as treated water would begin to fail and essential services such as health care would be degraded;

c. by two months - liquid fuel would be almost exhausted; and

d. by three months - there would be wide-spread unemployment, no transport capability, and services that rely on imported spares (such as electricity and telecommunications) would begin degrading significantly.

6. To overcome these challenges, the nation would require transformation in terms of the degree of personal responsibility for preparedness, management of industrial and social supplies to survive extended periods without access to global supply chains, and a review of governance to ensure federal, state and local governments can take legitimate control of essential services.

7. Overlaying all these issues, the workshop identified social cohesion and social mobilisation as the essential ingredients to surviving the scenario crisis.

PREPAREDNESS AND MOBILISATION RELATED DOCUMENTATION

Table D1: Legislation

Act	Purpose
Defence Act 1903	This act provides the legislative basis for the calling out of the reserves under Section 28, and the introduction of compulsory service under Section 60. It also provides for the control of railways, requisitioning of vehicles under Section 67 and use of civilian property under Section 68.
Liquid Fuels Emergency Act 1984	This act allows the Energy Minister to direct fuel corporations to maintain specific quantities of fuel in specified places in Australia under Section 12. Section 24 also allows the Minister to give directions regulating or prohibiting the sale of fuel.
Petroleum and Other Fuels Reporting Act 2017	This act requires the reporting of information relating to fuels and fuel-related products to the Commonwealth under Section 11.
Airports Act 1996	This act allows the Minister to direct an airport operator to provide, or give priority access to, specified forms of airport services for defence-related purposes under Section 250.
Australian National Railways Commission Sale Act 1997	This act provides that the Minister may, by written notice given to a person who manages or control a railway require that access, or priority access, be given for specified forms of defence-related purposes, under Schedule 5, Part 2, Section 1.
Qantas Sale Act 1992	This act requires that the facilities used by Qantas for the maintenance and housing of aircraft, catering, flight operations, training and administration be mostly located in Australia under Section 7(1)(h). It also prohibits Qantas from being incorporated outside Australia and requires an absolute majority of its board of directors to be Australian citizens under Section 7(1)(i) and Section 7(1)(k).
National Health Act 1953	This act provides that the Minister may, on behalf of the Commonwealth, may supply medical equipment to persons who require them, and can make modifications to a building, vehicle or equipment for the treatment of sick and disabled persons under Section 9A.
Telecommunications Act 1997	This act provides that a defence authority may give a carriage service provider a written notice requiring them to supply a specified carriage service for defence purposes of the management of natural disasters under Section 335.
Australian Broadcasting Corporation Act 1983	This act allows the Minister to direct the ABC to broadcast a particular matter if the Minister is of the opinion that it would be in the national interest to do so under Section 78.
Broadcasting Services Act 1992	The Minister for Foreign Affairs may suspend or cancel an international broadcasting licence under Section 121FL.
Control of Naval Waters Act 1918	This act provides that the Governor-General may make regulations for the control of naval waters under Section 4.
Biosecurity Act 2015	The Agriculture Minister may, in consultation with the Defence Minister, declare the ADF to be a national response agency for a biosecurity emergency under Section 452. Powers include entry to premises without warrant or consent under Section 470,
Lands Acquisition Act 1989	This act allows for an authorised person to examine land under Section 10, to occupy land temporarily under Section 11, and prescribes what it can do on that land under Section 12.
Corporations Act 2001	This act requires that, in the event of compulsory acquisition of property, the person acquiring the property pay compensation of a reasonable amount to the person from whom the property is being acquired under Section 1350.

Table D2: Military Doctrine

Document	Sponsor	Purpose
Executive Series: Preparedness and Mobilisation ADDP 00.2	Australian Defence Force Headquarters	Provides an overview of Australian mobilisation doctrine. It defines mobilisation, and breaks the mobilisation process down into four distinct phases from selective defence mobilisation to national mobilisation.
Personnel Series: Personnel ADDP 1.0	Defence People Group	Provides an overview of how personnel support ties into preparedness and mobilisation, and the factors that affect recruitment and retention of personnel.
Personnel Series: Health Support to Operations ADDP 1.2	Joint Health Command	Provides guidance for the provision of health support capability to operations, including command and control, coordination and planning requirements.
Logistics Series: Logistics Support to Capability ADDP 4.1	Joint Logistics Command	Provides an overview of how Defence's logistics capability supports preparedness and mobilisation planning, including the impact of preparedness and mobilisation on sustainment.
Doctrine and Training Series: Training ADDP 7.0	Australian Defence Force Headquarters	Provides an overview of Australian military training principles, aims and systems. It articulates training as a key input into individual and collective readiness, and the ability of the ADF to raise, train and sustain appropriate forces aligned to strategic direction.
ANP2420-4300 – Vol 1 – Navy Logistic Support	Navy	Provides guidance on Navy's explosive ordnance and fuel stockholdings, as well as supply chains.
Land Warfare Doctrine 1-2 – Health Support	Army	Provides guidance on the planning and conduct of health support to land operations.
Land Warfare Doctrine 4-0 – Supply	Army	Provides guidance on the provision on logistical support to the Army, including fuel and explosive ordnance.
Land Warfare Doctrine 4-1 – Supply Support	Army	Provides further context LWD 4-0 by setting out the principals for procurement, warehousing and stockholding.
Land Warfare Doctrine 7-0 – Training and Education	Army	Provides guidance on the planning, conduct and management of Army learning, training and/or education activities. It emphasises effective training as central to Army preparedness, force generation and force modernisation.
Australian Maritime Logistics Doctrine	Navy	Outlines Navy's enduring logistical principles intended to ensure Navy DEs are able to sustain operational effect(s) at optimum through-life cost. It articulates how engineering, maintenance and supply chain management practices interact to support the preparedness and sustainment of Navy assets/materiel.
ANP3702: Royal Australian Navy Training	Navy	Outlines Navy's training system and organisation as a mechanism to meet workforce capability requirements. Chapter 6 outlines the integration of training into the acquisition of new capability. Chapters 8 and 9 cover the planning and resourcing of Navy training to meet identified capability requirements, respectively.
AAP1005: Air Force Capability	Air Force	Provides guidance for RAAF CMs in delivering capability as part of the force-in-being and in planning for the delivery of new capabilities. This guidance covers the full capability

Management Manual		lifecycle, including the management and sustainment of enabling capabilities and materiel.
Manual of Air Force Education and Training (MAFET)	Air Force	Outlines RAAF policy on the management of education, training and assessment processes related to all Air Force-managed practices. It seeks to ensure RAAF personnel preparedness through individual and collective training.

Table D3: Defence Policy

Document	Sponsor	Purpose
Defence Planning Guidance	Strategic Policy Division	The overarching, classified strategic policy document that guides what Defence needs to achieve and how to achieve it, includes Australia's Military Strategy (AMS).
Defence Logistics Manual	Joint Logistics Command	Provides instructions on how reserve stock requirements are to be determined under Paragraph 2.5, and Chapter 1, Annex A.
Defence Health Manual (DHM)	Joint Health Command	Consolidates all extant Defence health policy into a single, unified document – including joint health procedures and practices, including recruitment of skilled personnel in Paragraph 3.10.
Defence Force Recruiting Strategic Plan	Defence Force Recruiting	Outlines DFR's approach to attracting, targeting and recruiting personnel to build, sustain and maximise ADF capability. The 2018 plan is particularly focused on addressing gaps in STEM-related capability streams to promote alignment between ADF personnel skills and the direction provided by the White Paper.
Defence Fuels Manual	Joint Capabilities Group	Provides for policy and procedural direction applicable to the Defence Fuel Supply Chain (DFSC), including liquid fuels, oils, lubricants and packaged products.
Military Personnel Manual (MILPERSMAN)	Defence People Group	Provides the administrative policy framework that applies to all Defence personnel. It includes guidance on the supply and management of personnel/workforces, as well as guidance regarding individual and collective training.

Table D4: Other

Document	Sponsor	Purpose
CDF Preparedness Directive	Australian Defence Force Headquarters	Sets Defence's preparedness requirements, including unit readiness and explosive ordnance requirements.
Defence Preparedness Assessment Summary	Australian Defence Force Headquarters	Reports on Defence's ability to meet CPD preparedness requirements in the context of the Quarterly Strategic Review, with a focus on identified deficiencies.
CASG Quarterly Performance Report	Capability Acquisition and Sustainment Group	Provides updates to senior stakeholders on the performance of CASG acquisition projects and sustainment activities, and provide an understanding of any emerging risks or issues to facilitate effective, efficient and coordinated remediation by Defence.

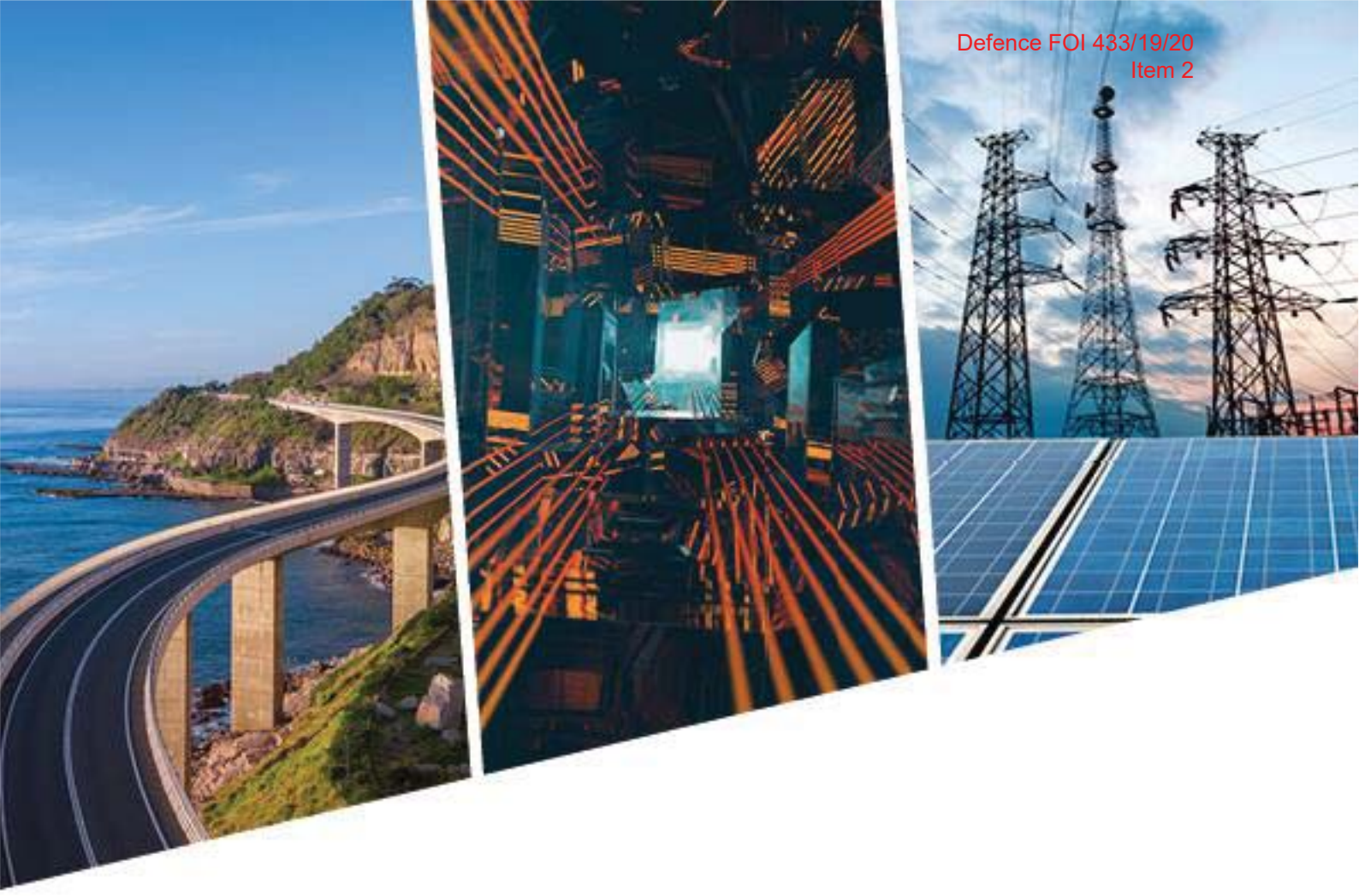
Annex E

E-1

Mobilisation Knowledge Map

This annex provides an overview of known activities relating to mobilisation in Defence and the wider Australian context. These activities include those with a focus on the resilience or vulnerability of supply chains and critical infrastructure. The knowledge map lists activities discovered during the Mobilisation Review – it is not exhaustive. There are many other activities which touch on aspects of preparedness and mobilisation that are not listed eg: the PADFA Review.

	Defence	Economic	Social
Environmental Analysis Risk and Vulnerability Assessment	Mobilisation Review (VCDF) Cyber Mobilisation Workshop (VCDFE/ANU) Collapse of Global Governance Workshop (VCDF/Engineers Australia) Global Supply Chain Study (VCDF/DST) s33(a)(ii) Supply Chain Illumination Activity (Navy/CASG) s33(a)(ii) SERCAT Preparedness Status Review (AHQ) s33(a)(ii) Review of Surge Recruitment Contracting (AHQ) Logistics Supply Chain Assurance Activities (CJC) Critical Infrastructure Nodal Assessments (SP&I)	Liquid Fuel Security Review (DoE) Future Transport Scenarios (Department of Transport)	Australian Vulnerability Profile (Home Affairs/Defence/DoE)
Policy and Strategy	DPG 2019- Task for VCDF to conduct mobilisation (SP&I) One Defence Energy Strategy (SP&I) Defence Industry Policy (SP&I) s42)	Declaration of Climate Emergency and Mobilisation (24 Australian jurisdictions- covering 20% of the Australian Population)	Social Cohesion Strategy (Department of Social Services)
Plans and Programs	Total Workforce Model (DPG) Supply Chain Illumination G&O for FSP 19 (CASG)		
Implementation	s47J Total Workforce System (DPG) Cyber Workforce Implementation (CJC/DPG) OP Supplementation Bids (VCDFE) Defence Fuel Transformation Program (CJC) Australian Health Security Centre (DFAT/Defence)	National Resilience Task Force (DoHA)	Movements mobilising for non-violent civil action in response to the Climate Emergency • Extinction Rebellion • Greenpeace • School Strike for Climate Change



ENGINEERS AUSTRALIA

CELEBRATING OUR CENTENARY

Industry Responses in a Collapse of Global Governance

Workshop report for the Department of Defence

February 2019

Engineers Australia
11 National Circuit, Barton ACT 2600
Tel: 02 6270 6555
Email: publicaffairs@engineersaustralia.org.au

www.engineersaustralia.org.au

Table of Contents

1. Introduction

1.1 Background

In 2018, the Department of Defence engaged Engineers Australia to convene a workshop for senior engineers with deep industry experience to discuss national mobilisation issues.

The workshop was held on 12 February 2019, at the Engineers Australia office in Melbourne. Seventeen expert engineers attended the workshop (plus Department of Defence project team members and Engineers Australia support staff). The engineers brought expertise from the following sectors:

- construction
- consulting
- electricity generation and transmission
- liquid fuel
- health care
- information telecommunications & media
- space
- manufacturing
- mining
- transport, postal and warehousing
- water and waste.

This report provides the findings of the workshop. It will inform further stages of work by the Preparedness and Mobilisation team at ADF Headquarters.

1.2 Workshop scenario

The workshop looked at the effects of a collapse in global governance, resulting in major disruption to the global supply chain. It sought to identify areas within each sector that would be affected, what those effects might be and how effects within one sector might affect others. They considered responses and preparatory methods of mitigation and resilience.

Detailed solutions to the issues identified were not developed.

The workshop focussed on three areas:

- Immediate effects from one to seven days
- Impacts if the situation lasts for three months, and
- Actions that could be taken prior to the event that would mitigate the effects identified.

1.3 Attendees

The workshop included 17 expert engineers. This number does not include the Department of Defence project team members and Engineers Australia support staff who assisted the workshop facilitation and discussion.

The workshop was conducted under the Chatham House Rule: *When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed*.[1]

[1] The Royal Institute of International Affairs, Chatham House Rule, Accessed 26 February, 2019. Available at: https://www.chathamhouse.org/chatham-house-rule.

1.3.1 Attendee list

Due to the use of the Chatham House Rule, a public version of this report (that omits section 1.3.1) has been provided for distribution beyond the Department of Defence. The 17 expert engineers who attended the workshop are listed below.

Workshop attendees

Name	Company
s47F	

2. Key insights

The workshop delivered the overarching advice that, in the scenario provided, Australia would suffer massive upheaval within one week due to job losses, social unease and hoarding.

Within a fortnight, due to stocks of imported supplies drawing down, major social infrastructure such as treated water would begin to fail and essential services such as health care would be degraded.

By the two-month mark liquid fuel would be almost exhausted, and by three months there would be wide-spread unemployment, no transport capability, and services that rely on imported spares (such as electricity and telecommunications) would begin degrading significantly.

To overcome these challenges, the nation would require transformation in terms of the degree of personal responsibility for preparedness, management of industrial and social supplies to survive extended periods without access to global supply chains, and a review of governance to ensure federal, state and local governments can take legitimate control of essential services.

Overlaying all these issues, the workshop identified social cohesion and social mobilisation as the essential ingredients to surviving the scenario crisis.

3. Findings and critical vulnerabilities

A range of critical vulnerabilities were identified for several sectors of industry.

3.1 Fuel security, power and transport

Limited fuel resources and an overarching power dependency will have a cascading effect on all sectors. There will be a clear and prompt effect on transport and freight which in turn affects the movement of goods and people. This is because most transport in Australia relies on liquid fuels, which is largely imported.

Without the ability to transport goods, there will be an effect on food security. The restricted ability to transport people will affect health care services and limit the ability to travel for work.

Emergency services will suffer, and rural and regional communities will be isolated. Some isolated networks are reliant on diesel fuel.

Of most concern is diesel as a fuel for generators that provide backup electricity systems. Random outages will have an influence on the edge of a network (suburbs) but, the greater the area affected, the greater the severity of the effects. For example, the effect of a mass power outage on a city the size of Melbourne would be catastrophic.

In the scenario with no international trade routes, liquid natural gas exports would stop, and the inability to export and import will have significant consequences. For example, most propane and butane is exported, so the excess that cannot be sold overseas would need to be stored within the gas storage and pipeline system, burned, or perhaps reinjected to the subsurface stores.

In addition, even though Australia has some domestic oil reserves, overseas-sourced crude is still required to enable Australian refineries to produce a wide spectrum of liquid fuels. Alternatively, the refineries could be re-calibrated to more effectively process the lighter Australian crude.

3.2 Electricity

Gas would continue to be available for gas-fired electricity generators. Coal, whilst still available, might not be able to be transported from mine to generator.

The workshop attendees were not too concerned with the electricity system in terms of supply but did note that system security would be at risk. This is because the ability to deal with normal maintenance issues will degrade over time as the necessary spare parts are exhausted.

3.3 Spare parts

Disruption to materials supply and specialist parts and equipment required for new projects and maintenance will affect all sectors. As stores diminish, projects would slow down and eventually halt. The cessation of operations would result in vast economic ramifications. There is the possibility of supply hoarding with subsequent negative influences on business-to-business collaboration.

'Just in time' logistics models will be unworkable in a situation whereby imports are halted, and if liquid fuel constraints affect domestic freight movements.

3.4 Health

The group noted that it estimated that 90-95% of specialist medical supplies are imported. Further work to verify that figure may be required.

A disruption to the supply of specialist pharmaceuticals will result in severe repercussions for public health. Specialised medicine supplies may be exhausted within days.

From an industry factors points of view, this could lead to lower productivity. Particularly affected will be the elderly and, if there is a disease outbreak, the unvaccinated.

Medical equipment and spare parts for maintenance form part of the critical health supply chain. Most are imported and the restriction of supply would create a steady degradation of medical support.

Health will also be greatly affected by disruptions to water and sewerage management, and waste disposal.

Waste collection services will be affected. Service standards may drop to ration fuel and electricity.

In terms of food supplies, they are expected to reduce within about 45 days.

3.5 Family and community

Clearly there would be an effect on non-essential travel and existing family arrangements such as education and other leisurely pursuits such as attendance at sporting events. The ability for intra-family care (such as adult children caring for elderly parents) would be disrupted.

3.6 Water

Water and wastewater are radio controlled standalone systems and therefore less vulnerable than other systems that rely on the internet and cloud data. It was noted that this is because water systems are often based on old infrastructure.

Mechanical supplies for workshops mean that the water sector could probably operate for more than 90 days.

However, the treatment of water relies on hundreds of tonnes of chemicals. Domestic supplies of the necessary chemicals would run out after about one week.

3.7 Telecommunications

Hardware, firmware, software and all spares come from overseas. Within 1-2 weeks, telecommunications outages (hardware, firmware and software) would occur with broad implications for data, particularly where not backed up and stored in the cloud.

At three months, software security will become an issue. It was also noted, however, that if the nation was targeted as part of a wider act of aggression (as opposed to the victim of a general global breakdown in supply chains), that the cyber security and telecommunications networks could be slowly infiltrated for months or years ahead of 'Day zero.' The infiltration could be so slow that it is either not identified, or the degree of threat builds imperceptibly.

The loss of international data, such as offshore commerce data facilities, will cause major social and economic disruptions.

Telecommunications are connected by international undersea cables and they regularly break. It was advised that it's not a matter of 'if' but 'when', and that ships are the essential tool in fixing lines that lie in international waters. If international shipping is stopped, satellites are relied on, but if they are also affected by the global political situation, there is a high risk that telecommunications will fail entirely.

Network stability may also be compromised, with the networked pushed beyond capacity.

3.8 Space

A space weather event that takes out power networks and GPS would have a significant effect. Loss of GPS affects the finance sector which relies on GPS-based timekeeping, and the transport and aviation sectors that rely on GPS navigation.

Examples of this occurring at a local level are the Montreal and Carrington space weather events. It was noted that space weather can have effects at a global scale, or very local scale.

3.9 Economic decline

The largest economic drivers are the export industries of mining and tourism, both of which will grind to a halt in the workshop scenario.

Job security will be diminished as projects slow down or stop. Major capital projects would see widespread layoffs after a week.

The result would be an economic downturn and price increases. It was expected that for many employers, especially those which operate on very small profit margins, layoffs of workers would begin within a week.

The financial system, including financial transactions, will be adversely affected by disruptions because they rely on GPS systems for things such as having an accurate time.

Shutting down the nation's export market would negatively affect export-oriented companies.

3.10 Civil infrastructure

The civil engineering sector has about 2-3 months of supplies. However, diesel and copper supplies will begin to be limited after about 2-3 weeks. Any repairs to infrastructure will be affected by limitations of stockpiles.

3.11 Mining

Mining exports will stop, so mines will quickly shut down operations—perhaps within two weeks. The benefit of this situation is that mine resources such as diesel would become unutilised and therefore free to fill gaps in supplies for other sectors.

Some domestic mining may continue, such as mineral sands and bauxite. Many mining systems utilise electricity rather than liquid fuels, which means that there is less chance for restriction to operations than in other sectors that rely on diesel and other liquid fuels.

The effect on the mining sector from low diesel fuel supplies was debated. Further research is required to determine the extent to which mine operations are dependent on diesel or electric energy sources.

3.12 Social order

With a decline in the availability and quality of goods, services and employment, a breakdown in social cohesion is likely. It was noted that 'Day 0', when global supply chains are cut, would likely be presaged by a long period of building tension and public awareness of the worsening situation. Hoarding of food, water and essential supplies by the public and industry is therefore expected.

It was noted that the governance structures of industry are not designed to cope with global disruptions. Instead, they are geared towards isolated and short-term events. Most industries are therefore unlikely to be well prepared for the workshop scenario, and their responses may be poor.

4. Timeline of effects

The timeline at Table 1 shows the major effects from before Day Zero to the three-month mark.

Table 1 Timeline of effects

Time	Event
Pre-Day 0	Cyber security and telecommunications infiltrated
Day 0	Public and industrial hoarding
	Specialised medicines shortage
Week 1	Water treatment systems begins to fail
	Export sectors affected
	Mass worker lay-offs begin
Week 2	Export mining operations cease
	Diesel shortages
	Copper shortages
	Standards for supply of goods & services declines
≈	
Month 1	Liquid fuel shortages affect logistics
	Food supplies begin to run out
Month 2	Civil construction supplies start to run out
	Liquid fuel supplies exhausted
	Freight and passenger transport services cease
Month 3	Employment scarce
	Social unrest
	Software security degraded
	Undersea communications cables degrade
	Water supply networks degrade
	Electricity supply & transmissions degrade

5. Responses and preparedness

The Workshop participants were asked to identify potential responses to the likely effects of the scenario. Options to help prepare for those responses were also provided. These are shown in Table 2.

Table 2 Responses and Preparedness

Responses	Preparedness
Liquid fuel shortages treated with rationing and the triage of distribution. Priority allocation for critical services such as transport, health and waste.	Ensure fuel reserves for 90 days, which is in line with the International Energy Agency stockholding obligations.
Hoarding by the public of fuel, food and medicines, and industrial hoarding of spare parts and specialist supplies, may require civil authorities to take over distribution and begin rationing.	Encourage societal self-sufficiency while society is connected and cohesive. Create policies that require people to take individual responsibility. For example, all households to hold at least one week's worth of supplies. Ensure adequate stores of strategic medical and industrial supplies. Increase local manufacturing capability. This includes small scale onshore parts manufacturing that could be scaled to meet high demands if required.
Low liquid fuel supplies can be ameliorated by increasing use of alternative energy sources.	Consider electrification of a dedicated proportion of the transport fleet, and more investment in alternative fuel production. Develop an integrated energy policy. Increase liquid fuel refining capacity.
ADF supports the government in development of a coordinated response.	Seek legitimacy for an increase to federal government powers to coordinate a national response. Create multi-government framework to make contingency plans at all levels of government.
Provide alternative and coordinated communication channels such as radio and town hall meetings.	Create a large scale sophisticated and consistent national dashboard for communications and plan for swift implementation. Maintain an independent communications system. Introduce the relevant issues to the public at an early stage to make it part of a national dialogue rather than suddenly inducing panic when the crisis reaches breaking point. Conduct an analysis of communications best practices from other countries. Create public awareness of the crisis communications plans through unofficial and official channels.
Local government will become a key coordinator of service provision and goods distribution at the local level.	The private sector has a key role in preparing for crisis events. Note that industry typically prepares for short term and localised issues rather than global long-term crises.
ADF will provide civil support, in part to keep the public in a positive frame of mind regarding the role of the state to managing the crises.	Ensure that the ADF is well informed, in advance, of its civil support role.
Accept a decline in standards and cost responsibility.	Create a plan for the degradation of services.

6. What to do: thinking with head or heart

The final workshop exercise was to identify a range of options for how to respond, and how to prepare. Each is listed below and expressed as a 'hashtag handle'.

All workshop participants then voted for each option that they thought was most important to address, but from two different perspectives:

- Thinking with one's head, and
- Thinking with one's heart.

The results are at Tables 3 and 4.

Table 3 Responses - #votewithyourhead #votewithyourheart

Responses	Head	Heart
#NationalMobilisation	5	0
#AccurateInformation	4	3
#Rationing	8	1
#SOMO (social mobilisation)	2	10
#CommsAreDown	1	0
#PoliticalCooperation	0	6

Table 4 Preparedness - #votewithyourhead #votewithyourheart

Responses	Head	Heart
#SupplyDependency	4	0
#SOCO (social cohesion)	2	9
#MultiGovernmentCoordination	2	1
#CommsRedundancy	0	0
#HeirarchyOfPriorities	3	2
#PersonalResponsibility	0	2
#MadeInAustralia (minimum essentials)	2	3
#PlannedPerformanceDegradation	0	0
#BeAlertNotAlarmed	0	2
#Legislate	0	0
#PoliticalCooperation	0	0
#EnergyStrategy	6	1
#CorporateRiskAnalysis	0	0
#Biz+	0	1

7. Recommendations and Challenges

The workshop did not make recommendations *per se*. However, a range of challenges and questions were identified and these a recommended for further investigation by the Department of Defence Preparedness and Mobilisation project team:

- To what extent will the political parties cooperate?
- How well will the general public cooperate with each other and the authorities?
- The very elderly are likely the only people who will have experienced a government-enforced degradation of services and liberties in periods like WW2. How will the younger generations react if this occurs in the modern age?
- It will be hard to prioritise without knowing the exact scenario to be encountered.

Similarly, several factors were identified as having a large effect on the ability for society to act cooperatively. These should also inform future work:

- Size of Australia
- Role of government and regulatory agencies
- Lack of government authority over the private sector (legislation may be needed to define the authority of government)
- Lack of social cohesion and getting people to act in collaboration as a community and not as self-interested individuals.
- Cost of making the necessary preparations, in terms of efforts like fuel conversion, adaptation of logistics models and storage of supplies.
- Preparing for the extreme events in the absence of indications that they are likely to occur.
- The challenge of issuing a consistent public message without being alarmist and thus causing social unease and unrest.


ENGINEERS
AUSTRALIA
100
CELEBRATING
OUR CENTENARY

ENGINEERS AUSTRALIA

CELEBRATING OUR CENTENARY

Industry Responses in a Collapse of Global Governance

Workshop report for attendees

February 2019

Engineers Australia
11 National Circuit, Barton ACT 2600
Tel: 02 6270 6555
Email: publicaffairs@engineersaustralia.org.au

www.engineersaustralia.org.au

Table of Contents

1. Introduction

1.1 Background

In 2018, the Department of Defence engaged Engineers Australia to convene a workshop for senior engineers with deep industry experience to discuss national mobilisation issues.

The workshop was held on 12 February 2019, at the Engineers Australia office in Melbourne. Seventeen expert engineers attended the workshop (plus Department of Defence project team members and Engineers Australia support staff). The engineers brought expertise from the following sectors:

- construction
- consulting
- electricity generation and transmission
- liquid fuel
- health care
- information telecommunications & media
- space
- manufacturing
- mining
- transport, postal and warehousing
- water and waste.

This report provides the findings of the workshop. It will inform further stages of work by the Preparedness and Mobilisation team at ADF Headquarters.

1.2 Workshop scenario

The workshop looked at the effects of a collapse in global governance, resulting in major disruption to the global supply chain. It sought to identify areas within each sector that would be affected, what those effects might be and how effects within one sector might affect others. They considered responses and preparatory methods of mitigation and resilience.

Detailed solutions to the issues identified were not developed.

The workshop focussed on three areas:

- Immediate effects from one to seven days
- Impacts if the situation lasts for three months, and
- Actions that could be taken prior to the event that would mitigate the effects identified.

1.3 Attendees

The workshop included 17 expert engineers. This number does not include the Department of Defence project team members and Engineers Australia support staff who assisted the workshop facilitation and discussion.

The workshop was conducted under the Chatham House Rule: *When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed*.[1]

[1] The Royal Institute of International Affairs, Chatham House Rule, Accessed 26 February, 2019. Available at: https://www.chathamhouse.org/chatham-house-rule.

2. Key insights

The workshop delivered the overarching advice that, in the scenario provided, Australia would suffer massive upheaval within one week due to job losses, social unease and hoarding.

Within a fortnight, due to stocks of imported supplies drawing down, major social infrastructure such as treated water would begin to fail and essential services such as health care would be degraded.

By the two-month mark liquid fuel would be almost exhausted, and by three months there would be wide-spread unemployment, no transport capability, and services that rely on imported spares (such as electricity and telecommunications) would begin degrading significantly.

To overcome these challenges, the nation would require transformation in terms of the degree of personal responsibility for preparedness, management of industrial and social supplies to survive extended periods without access to global supply chains, and a review of governance to ensure federal, state and local governments can take legitimate control of essential services.

Overlaying all these issues, the workshop identified social cohesion and social mobilisation as the essential ingredients to surviving the scenario crisis.

3. Findings and critical vulnerabilities

A range of critical vulnerabilities were identified for several sectors of industry.

3.1 Fuel security, power and transport

Limited fuel resources and an overarching power dependency will have a cascading effect on all sectors. There will be a clear and prompt effect on transport and freight which in turn affects the movement of goods and people. This is because most transport in Australia relies on liquid fuels, which is largely imported.

Without the ability to transport goods, there will be an effect on food security. The restricted ability to transport people will affect health care services and limit the ability to travel for work.

Emergency services will suffer, and rural and regional communities will be isolated. Some isolated networks are reliant on diesel fuel.

Of most concern is diesel as a fuel for generators that provide backup electricity systems. Random outages will have an influence on the edge of a network (suburbs) but, the greater the area affected, the greater the severity of the effects. For example, the effect of a mass power outage on a city the size of Melbourne would be catastrophic.

In the scenario with no international trade routes, liquid natural gas exports would stop, and the inability to export and import will have significant consequences. For example, most propane and butane is exported, so the excess that cannot be sold overseas would need to be stored within the gas storage and pipeline system, burned, or perhaps reinjected to the subsurface stores.

In addition, even though Australia has some domestic oil reserves, overseas-sourced crude is still required to enable Australian refineries to produce a wide spectrum of liquid fuels. Alternatively, the refineries could be re-calibrated to more effectively process the lighter Australian crude.

3.2 Electricity

Gas would continue to be available for gas-fired electricity generators. Coal, whilst still available, might not be able to be transported from mine to generator.

The workshop attendees were not too concerned with the electricity system in terms of supply but did note that system security would be at risk. This is because the ability to deal with normal maintenance issues will degrade over time as the necessary spare parts are exhausted.

3.3 Spare parts

Disruption to materials supply and specialist parts and equipment required for new projects and maintenance will affect all sectors. As stores diminish, projects would slow down and eventually halt. The cessation of operations would result in vast economic ramifications. There is the possibility of supply hoarding with subsequent negative influences on business-to-business collaboration.

'Just in time' logistics models will be unworkable in a situation whereby imports are halted, and if liquid fuel constraints affect domestic freight movements.

3.4 Health

The group noted that it estimated that 90-95% of specialist medical supplies are imported. Further work to verify that figure may be required.

A disruption to the supply of specialist pharmaceuticals will result in severe repercussions for public health. Specialised medicine supplies may be exhausted within days.

From an industry factors points of view, this could lead to lower productivity. Particularly affected will be the elderly and, if there is a disease outbreak, the unvaccinated.

Medical equipment and spare parts for maintenance form part of the critical health supply chain. Most are imported and the restriction of supply would create a steady degradation of medical support.

Health will also be greatly affected by disruptions to water and sewerage management, and waste disposal.

Waste collection services will be affected. Service standards may drop to ration fuel and electricity.

In terms of food supplies, they are expected to reduce within about 45 days.

3.5 Family and community

Clearly there would be an effect on non-essential travel and existing family arrangements such as education and other leisurely pursuits such as attendance at sporting events. The ability for intra-family care (such as adult children caring for elderly parents) would be disrupted.

3.6 Water

Water and wastewater are radio controlled standalone systems and therefore less vulnerable than other systems that rely on the internet and cloud data. It was noted that this is because water systems are often based on old infrastructure.

Mechanical supplies for workshops mean that the water sector could probably operate for more than 90 days.

However, the treatment of water relies on hundreds of tonnes of chemicals. Domestic supplies of the necessary chemicals would run out after about one week.

3.7 Telecommunications

Hardware, firmware, software and all spares come from overseas. Within 1-2 weeks, telecommunications outages (hardware, firmware and software) would occur with broad implications for data, particularly where not backed up and stored in the cloud.

At three months, software security will become an issue. It was also noted, however, that if the nation was targeted as part of a wider act of aggression (as opposed to the victim of a general global breakdown in supply chains), that the cyber security and telecommunications networks could be slowly infiltrated for months or years ahead of 'Day zero.' The infiltration could be so slow that it is either not identified, or the degree of threat builds imperceptibly.

The loss of international data, such as offshore commerce data facilities, will cause major social and economic disruptions.

Telecommunications are connected by international undersea cables and they regularly break. It was advised that it's not a matter of 'if' but 'when', and that ships are the essential tool in fixing lines that lie in international waters. If international shipping is stopped, satellites are relied on, but if they are also affected by the global political situation, there is a high risk that telecommunications will fail entirely.

Network stability may also be compromised, with the networked pushed beyond capacity.

3.8 Space

A space weather event that takes out power networks and GPS would have a significant effect. Loss of GPS affects the finance sector which relies on GPS-based timekeeping, and the transport and aviation sectors that rely on GPS navigation.

Examples of this occurring at a local level are the Montreal and Carrington space weather events. It was noted that space weather can have effects at a global scale, or very local scale.

3.9 Economic decline

The largest economic drivers are the export industries of mining and tourism, both of which will grind to a halt in the workshop scenario.

Job security will be diminished as projects slow down or stop. Major capital projects would see widespread layoffs after a week.

The result would be an economic downturn and price increases. It was expected that for many employers, especially those which operate on very small profit margins, layoffs of workers would begin within a week.

The financial system, including financial transactions, will be adversely affected by disruptions because they rely on GPS systems for things such as having an accurate time.

Shutting down the nation's export market would negatively affect export-oriented companies.

3.10 Civil infrastructure

The civil engineering sector has about 2-3 months of supplies. However, diesel and copper supplies will begin to be limited after about 2-3 weeks. Any repairs to infrastructure will be affected by limitations of stockpiles.

3.11 Mining

Mining exports will stop, so mines will quickly shut down operations—perhaps within two weeks. The benefit of this situation is that mine resources such as diesel would become unutilised and therefore free to fill gaps in supplies for other sectors.

Some domestic mining may continue, such as mineral sands and bauxite. Many mining systems utilise electricity rather than liquid fuels, which means that there is less chance for restriction to operations than in other sectors that rely on diesel and other liquid fuels.

The effect on the mining sector from low diesel fuel supplies was debated. Further research is required to determine the extent to which mine operations are dependent on diesel or electric energy sources.

3.12 Social order

With a decline in the availability and quality of goods, services and employment, a breakdown in social cohesion is likely. It was noted that 'Day 0', when global supply chains are cut, would likely be presaged by a long period of building tension and public awareness of the worsening situation. Hoarding of food, water and essential supplies by the public and industry is therefore expected.

It was noted that the governance structures of industry are not designed to cope with global disruptions. Instead, they are geared towards isolated and short-term events. Most industries are therefore unlikely to be well prepared for the workshop scenario, and their responses may be poor.

4. Timeline of effects

The timeline at Table 1 shows the major effects from before Day Zero to the three-month mark.

Table 1 Timeline of effects

Time	Event
Pre-Day 0	Cyber security and telecommunications infiltrated
Day 0	Public and industrial hoarding
	Specialised medicines shortage
Week 1	Water treatment systems begins to fail
	Export sectors affected
	Mass worker lay-offs begin
Week 2	Export mining operations cease
	Diesel shortages
	Copper shortages
	Standards for supply of goods & services declines
≈	
Month 1	Liquid fuel shortages affect logistics
	Food supplies begin to run out
Month 2	Civil construction supplies start to run out
	Liquid fuel supplies exhausted
	Freight and passenger transport services cease
Month 3	Employment scarce
	Social unrest
	Software security degraded
	Undersea communications cables degrade
	Water supply networks degrade
	Electricity supply & transmissions degrade

5. Responses and preparedness

The Workshop participants were asked to identify potential responses to the likely effects of the scenario. Options to help prepare for those responses were also provided. These are shown in Table 2.

Table 2 Responses and Preparedness

Responses	Preparedness
Liquid fuel shortages treated with rationing and the triage of distribution. Priority allocation for critical services such as transport, health and waste.	Ensure fuel reserves for 90 days, which is in line with the International Energy Agency stockholding obligations.
Hoarding by the public of fuel, food and medicines, and industrial hoarding of spare parts and specialist supplies, may require civil authorities to take over distribution and begin rationing.	Encourage societal self-sufficiency while society is connected and cohesive. Create policies that require people to take individual responsibility. For example, all households to hold at least one week's worth of supplies. Ensure adequate stores of strategic medical and industrial supplies. Increase local manufacturing capability. This includes small scale onshore parts manufacturing that could be scaled to meet high demands if required.
Low liquid fuel supplies can be ameliorated by increasing use of alternative energy sources.	Consider electrification of a dedicated proportion of the transport fleet, and more investment in alternative fuel production. Develop an integrated energy policy. Increase liquid fuel refining capacity.
ADF supports the government in development of a coordinated response.	Seek legitimacy for an increase to federal government powers to coordinate a national response. Create multi-government framework to make contingency plans at all levels of government.
Provide alternative and coordinated communication channels such as radio and town hall meetings.	Create a large scale sophisticated and consistent national dashboard for communications and plan for swift implementation. Maintain an independent communications system. Introduce the relevant issues to the public at an early stage to make it part of a national dialogue rather than suddenly inducing panic when the crisis reaches breaking point. Conduct an analysis of communications best practices from other countries. Create public awareness of the crisis communications plans through unofficial and official channels.
Local government will become a key coordinator of service provision and goods distribution at the local level.	The private sector has a key role in preparing for crisis events. Note that industry typically prepares for short term and localised issues rather than global long-term crises.
ADF will provide civil support, in part to keep the public in a positive frame of mind regarding the role of the state to managing the crises.	Ensure that the ADF is well informed, in advance, of its civil support role.
Accept a decline in standards and cost responsibility.	Create a plan for the degradation of services.

6. What to do: thinking with head or heart

The final workshop exercise was to identify a range of options for how to respond, and how to prepare. Each is listed below and expressed as a 'hashtag handle'.

All workshop participants then voted for each option that they thought was most important to address, but from two different perspectives:

- Thinking with one's head, and
- Thinking with one's heart.

The results are at Tables 3 and 4.

Table 3 Responses - #votewithyourhead #votewithyourheart

Responses	Head	Heart
#NationalMobilisation	5	0
#AccurateInformation	4	3
#Rationing	8	1
#SOMO (social mobilisation)	2	10
#CommsAreDown	1	0
#PoliticalCooperation	0	6

Table 4 Preparedness - #votewithyourhead #votewithyourheart

Responses	Head	Heart
#SupplyDependency	4	0
#SOCO (social cohesion)	2	9
#MultiGovernmentCoordination	2	1
#CommsRedundancy	0	0
#HeirarchyOfPriorities	3	2
#PersonalResponsibility	0	2
#MadeInAustralia (minimum essentials)	2	3
#PlannedPerformanceDegradation	0	0
#BeAlertNotAlarmed	0	2
#Legislate	0	0
#PoliticalCooperation	0	0
#EnergyStrategy	6	1
#CorporateRiskAnalysis	0	0
#Biz+	0	1

7. Recommendations and Challenges

The workshop did not make recommendations *per se*. However, a range of challenges and questions were identified and these a recommended for further investigation by the Department of Defence Preparedness and Mobilisation project team:

- To what extent will the political parties cooperate?
- How well will the general public cooperate with each other and the authorities?
- The very elderly are likely the only people who will have experienced a government-enforced degradation of services and liberties in periods like WW2. How will the younger generations react if this occurs in the modern age?
- It will be hard to prioritise without knowing the exact scenario to be encountered.

Similarly, several factors were identified as having a large effect on the ability for society to act cooperatively. These should also inform future work:

- Size of Australia
- Role of government and regulatory agencies
- Lack of government authority over the private sector (legislation may be needed to define the authority of government)
- Lack of social cohesion and getting people to act in collaboration as a community and not as self-interested individuals.
- Cost of making the necessary preparations, in terms of efforts like fuel conversion, adaptation of logistics models and storage of supplies.
- Preparing for the extreme events in the absence of indications that they are likely to occur.
- The challenge of issuing a consistent public message without being alarmist and thus causing social unease and unrest.


ENGINEERS
AUSTRALIA
100
CELEBRATING
OUR CENTENARY

Future Cyber War: How would Australia mobilise a response?

1. Overview

On 8 November, 2018 the National Security College Futures Hub held an interactive workshop on cyber mobilisation readiness with the participants listed at **Annex A**. This note summarises key findings and recommendations generated by attendees.

The overarching learning was that, while Australia has a lot of plans, systems and relevant experience for managing crises and disasters, a cyber "war" situation is a qualitatively different type of emergency and we are not well set up to deal with it. This is linked to three attributes of a cyber war. First, scope: a cyber war will not be limited to a particular geography, business sector or segment of the community. Second, uncertainty: we will struggle to identify when it starts, how long it will last, and what will be affected next. Third, our vulnerability profile: adversaries will not just exploit weaknesses in computer systems; they will exploit vulnerabilities in society.

Another key learning was that "mobilisation" in the context of a cyber war will be a whole-of-nation endeavour. This is because first, many of the targets will be civilian businesses and individuals. Second, the resources needed to respond will be mostly privately held. Third, the centre of gravity is likely to be popular will and resilience.

As a result, contingency planning and preparedness cannot just occur inside defence or government silos. When it comes to mobilising for cyber war, a future government's role may be predominantly about coordinating and communicating, rather than directing or controlling. Further work is needed to clarify roles and responsibilities between states, federal agencies and other stakeholders, and to better understand and manage public expectations.

2. Findings

Participants imagined that it was 2022, and a state adversary had launched a "cyber war" against Australia. They were separated into four groups, which produced the scenarios at **Annex B**. The below findings surfaced across multiple groups.

2.1 What are key vulnerabilities and potential targets?

- *Democracy.* In a democracy, public attitudes and opinion are a key target. In every scenario the hypothetical adversary used a cyber war to intimidate, distract, coerce, or otherwise control the Australian public, in order to ensure that economic, security, or foreign policy decisions were made in its favour.
- *Critical infrastructure.* Every scenario included attacks against CI, including energy, transport, hospitals and sanitation systems. Key findings included:
    - Adversaries will look for the "sweet spot" between system criticality and ease of attack. For example, successful attacks against financial institutions are difficult;

but attacking the systems that consumers use to interface with their bank—e.g. EFTPOS or apps—may be easier, and just as impactful.
    - Critical infrastructure supply chains are particularly vulnerable. Since the networks of CI providers may be comparatively well-defended, an adversary might target smaller, less visible providers or inputs. For example, by targeting the few laundromats in a state able to supply hospital-grade linen cleaning, an adversary could significantly impair hospital functions. Alternatively, disrupting RFID tracking for just a few major trucking companies could significantly impact food supply.
    - While an adversary may choose to target civilian communications networks, we should also prepare for situations in which they choose to leave communications networks intact, so that information operations and / or news of other attacks spread, generating fear, uncertainty, or mistrust.
- *Indo-Pacific connectivity.* Adversaries may attack offshore targets to impact Australia—for example shutting down energy trading in Australia to impact flow of fuels to Australia. Third-party targets will have different priorities for responding.

2.2 What would "cyber war" look like?

- *Lengthy pre-war phase.* This is likely to last months, if not years. It will involve intelligence gathering, reconnaissance, and testing of capabilities (e.g. via isolated acts of cyber sabotage). It may also involve information operations designed to undermine public resilience (e.g. by weakening trust in government, increasing tensions between segments of the community, or by using 'false flag' attacks to reduce public trust in attribution).
- *Identification and attribution problems.* "Day 0" of a cyber war will be difficult to identify. The opening salvos of a cyber war may be lost in the noise of day-to-day cyber incidents, or dismissed as criminal acts. Individual targets may be unaware that their experience forms evidence of a broader pattern of attacks and not report it, depriving cyber agencies of a full picture of events.
- *Attacks against trust and confidence.* Every imagined scenario had a dominant psychological / information warfare component. A hybrid of cyber and information attacks were used to exploit and deepen mistrust between sections of the community, levels of government, citizens and government, and Australia and its international partners. Most scenarios involved acts of deception including false flag attacks, deep fakes, and altering digital records.
- *Significant impact on civilian life.* In every scenario, targets were mostly civilian rather than military or governmental. Disruption of food and fuel supply chains was a common theme. Other scenarios targeted consumer banking, ticketing at major sports events, or "mum and dad" business networks, to increase public inconvenience and fears.

2.3 How would Australia respond to a cyber war?

Following on from the scenarios presented above, groups then generated a response plan. Common findings emerged across four categories: (a) pre-attack readiness; (b) mitigation and recovery; (c) resilience and public communications; and (d) counter-attack and deterrence.

Pre-attack readiness

- *Early warning systems are essential.* To solve for the "identification" problems observed above, systems and processes which enable anomalies to be identified and reported are essential. These would be enhanced by threat intelligence sharing by government to entities that are likely to be targeted, so that they can be alert and prepared for threats.
- *Allocation of roles and responsibilities.* Nearly all participants emphasised the critical importance of increased clarity about responsibilities and expectations. For example, significant harm and confusion will result if state governments are waiting for ASD to act, or individuals and communities are waiting for a military response when they could be taking action themselves.
- *Fail safes and fall backs.* Having safety options and contingencies inbuilt into infrastructure systems as well as "everyday" Internet-of-Things devices will be essential. For example, a smart metre should be able to be disconnected and turned into a "dumb metre" in the event of attack. Citizens should know how to establish mesh networks in the event of telecommunications disruptions.

Mitigation and recovery

- *Triage.* Any response would prioritize restoring systems which threaten civilian safety—e.g. disruptions to water, sanitation and food supply. Traditional emergency services, as well as federal and state law enforcement and health departments would play an important role.
- *Success will come from the bottom up.* All groups agreed that much of the capability to respond to an attack would come from individuals and communities—governments' role would be leveraging and coordinating this. One group spoke of the need to inculcate a cyber "civil defence" mentality, rather than relying on an emergency management approach. Others spoke of the need for citizens to have a "cyber plan," just as they may currently have a bushfire plan, for local "cyber emergency sheds," or for a "cyber reserve" model to build capability across communities.
- *Use industry to quickly scale capability.* Much of the cyber capability to respond to a massive cyberattack resides in the private sector. But there were concerns about whether industry would have the ability, or will, to support a national recovery effort.

Resilience and public communications

- *Trusted crisis communications.* Communications will be essential to maintaining trust, distributing information, and coordinating a response, but are likely to be challenged and contested. One group proposed a "showerhead strategy"—whereby core messages

would be tailored to different segments of the community, and communicated by trusted spokespersons.

- *Shared narrative.* Public resilience was identified by all groups as essential—since most of the cyber war scenarios were designed to undermine public resolve and trust. Being able to clearly identify the "bad guys," and creating a common purpose and narrative around resisting them, would increase resilience.

Counter-attack and deterrence

- *Digitally assured destruction?* A number of participants questioned whether Australia's offensive cyber capability was sufficient to deter a largescale cyberattack. Should Australia have a larger, and more obvious capability?

3. Recommendations

Attendees suggested that the following points merit further development and / or research.

- *Uncertainty about thresholds.* All groups struggled with identifying the point at which a single or series of incidents constituted a "cyber war" footing, and therefore triggered the need for a major response.
- *Clarifying community expectations.* What does "good" look like? What does the community expect would happen in the event of a cyber war, and how can government manage or amend this expectation?
- *Cyber warfare pipeline.* There is not only a need to ensure we have a skilled cyber workforce, but also that mechanisms exist to quickly access capability in times of crisis.
- *Offensive / deterrence posture.* In a crisis situation, especially if cut off from key partners, would Australia maintain a sufficient cyber capability? If Australia was to develop an offensive "sledgehammer" sufficient to deter or counter-attack potential adversaries, what would this look like? Is there evidence that this approach works? And are there escalation or stability risks if Australia was to adopt this path?
- *Stress inoculation*. There is a need to prepare the population for cyber contingencies, to reduce the panic and uncertainty that is likely to emerge in the event of a cyber war.
- *Trust and social cohesion.* To reduce the attack surface for adversaries using 'divide and conquer' tactics, there is a need to focus on building trust and social cohesion. This should be based on broad shared values, and may need processes such as truth and reconciliation commissions to be fully realised.
- *Whole-of-nation vulnerability assessment.* Australia does not have a clear picture of its vulnerability. An assessment would require coordination across governments, businesses, and civil society.
- *Market mechanisms.* There is a need to ensure that we are using available market mechanisms to lift cybersecurity standards. In particular, there is a cyber service gap in small and medium enterprises, yet these form the bulk of the economy.
- *Cultural change.* To lift national cyber hygiene, a major pivot is needed—similar to that involved in ensuring widespread adoption of OH&S or car safety. Could a reframing from cyber "security" to "safety" help? Should non-compliance penalties be increased?

Annex A—List of Attendees

Name	Company / Agency
Adam Henschke	National Security College
Andrew Beard	PM&C
Anker Brodersen	Department of Defence
Annie Brusic	PM&C
Arthur Horobin	Department of Health
Brad Fallen	National Security College
Catherine Bridges	National Security College
Cheryl Durrant	Department of Defence
Chris Davis	Department of Defence
Chris Farnham	National Security College
David Cullen	DPC, Vic
Greg Evans	Department of Defence
Greg Sadler	Critical Infrastructure Centre
Jerry Doganer	Department of Human Services
John Gill	Department of Defence
Katherine Mansted	National Security College
Kendra Morony	Australian Cyber Security Centre
Kieran Dale	NSW Finance Department
s47F	
Mark Colbran	AFP
s47F	
Roger Bradbury	National Security College
Sabiq Tan	Critical Infrastructure Centre
Sarah Norton	PM&C
Steve Seguna	Australian Cyber Security Centre

Annex B—"Cyber war 2022" scenarios

I. Intimidate

An adversary seeks to weaken the Australian government's resolve to oppose it, and limit Australia's ability to conduct its foreign policy in the region.

Pre-attack: Years of intelligence gathering, target acquisition, testing of cyber capabilities (perhaps against other countries), and information warfare (to erode trust between government and citizens, and between different segments of the community.)

Attack: "Hard and fast" simultaneous cyber attacks on day 1 maximize public impact. These include attacks against critical infrastructure–like the electricity grid and military networks–and important national systems, such as the food supply chain and incident response. Information operations maximize public fear and distrust in government, and reduce partners' willingness to come to Australia's aid.

II. Distract

An adversary uses a cyber war to keep the Australian public and government distracted while it achieves military objectives in the region.

Pre-attack: The adversary identifies and maps target vulnerabilities, and engages in "false flag" attacks to undermine community resilience and make attribution more politicized.

Attack: What seem at first to be isolated acts of cyber sabotage build over time into a coordinated attack. Targets include critical infrastructure supply chains and major public events (like ticketing for a Grand Final). The adversary makes attribution difficult–both technically and politically. The public quickly starts to feel that government/s are losing control of the response, and basic functions of government.

2022

III. Coerce

An adversary uses a lengthy cyber war to coerce the Australian people into being unwilling to contribute to a coalition effort in response to a regional crisis.

Attack: Multiple lines of attack are opened from day 1 to create a "compound emergency." Cyber attacks cause widespread financial disruption, underwriters withdraw support for fuel carrier ships, and the food supply chain is disrupted. The front widens into a year-long disruption, and confidence in the government's ability to respond wanes. Attacks against autonomous vehicles cause road accidents. Drones are redirected to cause bushfires. The public feels highly vulnerable and unwilling to oppose the adversary.

IV. Control

An adversary uses a cyber war to change policy and public opinion.

Attack: The attack builds over time. Targets are selected to exert economic pressure and create a public sense of chaos. Deep fakes and false flags undermine public trust. Attacks against food and fuel supply create a "hoarder mentality," compounding the crisis. A combination of cyber and information attacks are used to divide Australia internally, and from its allies. For example, public confidence falls when it appears that the PM received payments into her bank account after infrastructure projects commenced. Australia is cut off from its Five Eyes partners, and stops receiving valuable intelligence, after its partners conclude that it can no longer keep its systems protected. Just as the government seems unable to restore core civilian-facing systems, the adversary makes a public offer of support. Systems are restored. Public support for the adversary lifts dramatically, and its personnel and / or equipment remains in Australia to "help."

Global Change in Strategic Military Geography: Preparedness Impacts

Southern Lights Hypothetical Game Quick-Look Report

Prepared By: Joint Force Intelligence Analysis and Risk Directorate

Methodology

Participants

- *ADML (Rtd) Chris Barrie,* ANU (Facilitator)
- *AVM Neil Hart ,* HJCC
- *RADM Neil Morrisetti,* UK Climate Change Envoy
- *Mr Matt Ramage,* ASSP
- *Mr Joel Watson ,* FCO, UK
- *Dr Peter Dortmans,* Discipline Leader DSTO
- *COL Dennis Malone,* AHQ
- *Col Chris Stockton,* US DA
- *Ms Clare Young ,* Senior Futures Analyst, ONA
- *Ms Sheryl Boxall,* Senior Futures Analyst, NZDF
- *Mr Andrew Arnold,* VCDF S&T Advisor
- *CMDR Chris Aulmann,* FSR Team
- *Assistant Commissioner Andy Sims,* IDG, AFP
- *Mr Rob Bryson,* Australian Antarctic Division
- *Mr Laughlin Wilson ,* Strategic Futures, DIO
- *Mr John Lee,* Strategy Analyst

The purpose of the hypothetical was to discuss a series of events that could arise in a plausible 2030 context. The intent was to scope a spectrum of plausible scenarios and potential threats rather than confine discussion to one possible scenario.

The hypothetical game was set in 2030 scenario space. This scenario was developed from the research undertaken for the VCDFG Global Change and Strategic Military Geography: Preparedness Impacts Study. The hypothetical was structured around seven operational vignettes.

The vignettes were:

1. Nuclear Issues
2. Mass Migration
3. Pacific Relocation
4. Southern Ocean (SO) Disaster
5. Extreme Weather
6. Pandemic
7. Southern Ocean (SO) Eco-Terrorists

Participants provided comments verbally and also in response to structured questions.

Foresight for Deep Uncertainty

Scenario Setting

The scenario setting was developed using the INSPECT(S) model from the QUEST scenario development method, modified to include themes or topics of particular interest to Defence.

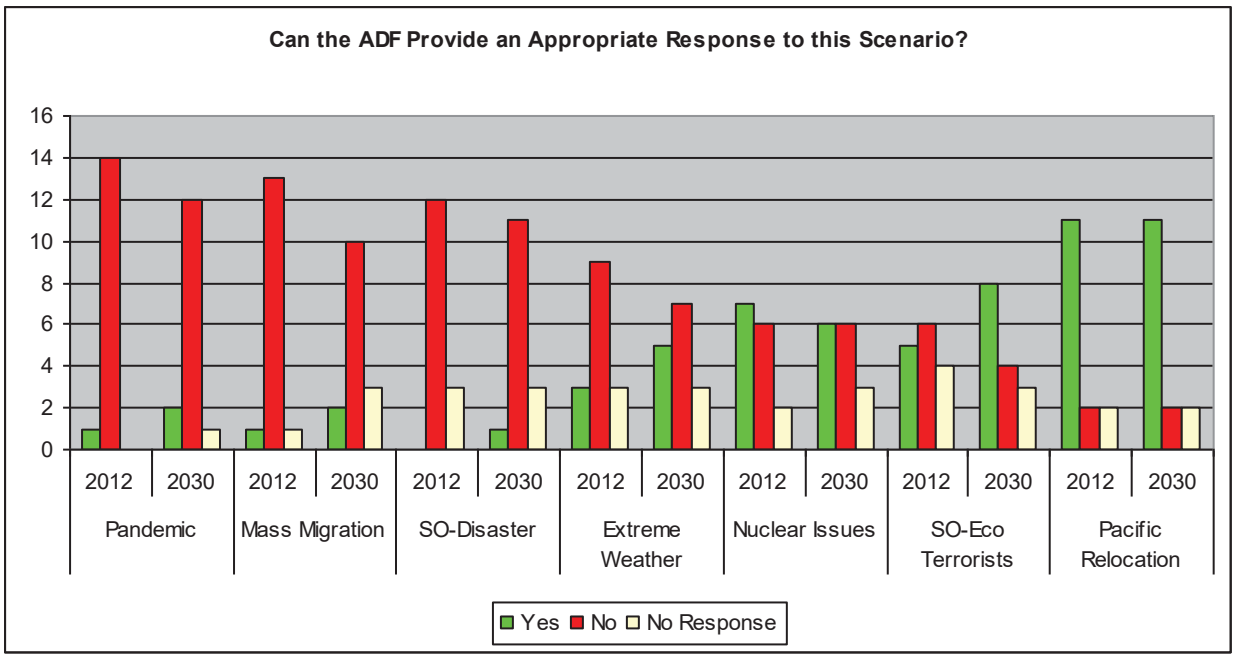
The INSPECT Model is:
I=Intellectual;
N=Nature;
S=Society;
P= Politics;
E=Economics;
C=Culture;
C=Cyberspace;
T = Technology;
S = Space.

In the scenario the effects of climate change have grown more serious, but stop short of the doomsday forecasts made by many. It assumes that agricultural production continues to expand, despite the challenges posed by climate change and high energy prices, but that it does not fully keep pace with population growth. The scenario (enclosure 1) peers into the future and sketches out a plausible "muddling through" world

The scenario is neither a "best case" nor a "worst case" scenario.

Defence Preparedness

Participants were asked could the ADF provide an appropriate response to each of the seven scenario vignettes for two timeframes: now (2012) and 2030. The table below summarises participants responses. Participants rated the ADF as least able to respond to a major pandemic in either timeframe. Mass migration issues, involving a <100 fold increase of arrivals on our northern borders and responding to a major disaster in Antarctica involving shipwreck within the Australian area of search and rescue responsibility also presented high difficulty for the ADF.

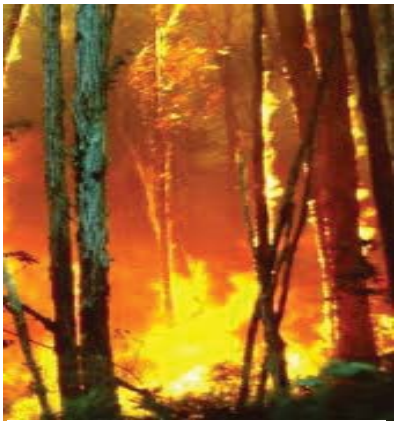


Participants assessed the ADF as capable of providing responses to the need to relocate pacific islanders in either timeframe. The ability to respond to eco-terrorism (piracy, sabotage) in the southern ocean (SO) and Antarctica was assessed as providing an issue for the ADF now but within it's capabilities in 2030. Participants were divided on the ADF's ability to respond to extreme weather (concurrent fire/storm events on AS mainland) and nuclear issues.

Key Themes from the Discussion

1.0 Scale and Concurrency. Participants thought that the ADF had capabilities that could effectively respond to any of the scenario vignettes. They argued that the difficulty faced by the ADF was created by the scale of the response needed (mass migration, pandemic) or the concurrent demands on ADF capabilities (mass migration, pandemic, SO disaster, extreme weather).

This raises the importance of explicitly addressing increase in the scale and potential concurrency of hazard driven events in future scenario planning. Like the national bushfire warning system which has had to add a new level of risk to cater for extreme fire events, Defence needs to make sure that planning adequately addresses risks of a similar extreme scale.



Fire events in Australia are becoming more severe.

2.0 Rise of Supranational Organisations and Global Tribes. Most participants felt that the future political and social environment would change in response to geo-morphological change. How it might change was uncertain.

The central position of the Westphalian State in global politics may or may not be eroded with the rise of corporations, global tribes and enhanced international and supranational bodies. Participants agreed that the uncertainty of the global and political landscape needed to be a factor in Defence planning. Concepts exploring how Defence might operate in these changed environments might be explored and intelligence assets would need to monitor developments. Defence might consider a more proactive rather than reactive approach to change. Understanding community and global values would become increasingly relevant to Defence planning.

"Security is like oxygen you tend not to notice it until you lose it."
Joseph Nye

"The Army is also a fragile organism and its capability must be painstakingly built up and nurtured."

General
David Morrison
October 26 2012

3.0 A Risk Based Contract with Government. Participants held mixed views on the role of Defence in responding to the vignettes. Overseas and non-Defence participants felt that there is clearly an expectation from Government that Defence will respond to national emergencies and disasters, regardless of stated policy. They argued that Defence must have a clear contract with Government covering Defence's expected contribution to HADR, DACC and DACP operations within a national and international context. They argued that this is an area where the ADF might display greater leadership in shaping the national security debate.

ADF participants also thought that Defence must think in terms of strategic risk and opportunity; not inputs and outputs. This must be presented in unambiguous language, not as sensationalist problems: with a full understanding of cost and risk. However there was a view that Defence must follow the thinking in the National Security Strategy and the National Security Risk Framework.

4.0 Preparedness and Resilience. There was considerable discussion on the need for Defence to ensure internal resilience to potential hazards and extreme weather events in order to have a secure footing for the range of potential responses. Participants flagged Defence infrastructure vulnerabilities, safety of Defence families, and the importance of Continuation of Defence Operations (CoDO) planning as areas where greater preparedness guidance and monitoring might be needed.

There was a general consensus that the concept of resilience needed to be embedded across the full spectrum of Defence processes including; strategy, operational plans, preparedness, capability plans, and monitoring and governance. It was suggested that the cost of resilience, and the risks of not having it, needed to be better understood in order to inform investment choices. Resilience might become a decision criterion for strategic choice.

5.0 Defence Global Leadership. The majority of participants, including overseas personnel, agreed that Defence can and should play a leading role in preparing for and mitigating, climate change impacts. Defence was seen as having the tools and the ability to think strategically and a culture of focussing on the future. Participants were adamant that Defence must be a leader not a follower, within its remit, and seek to collaborate more across Government, academia, industry and society. Participants also pointed to the utility of international Defence partnerships as a way of creating critical mass for action. Overseas participants noted that some parts of the military are already working together and that there is a lot happening within the five-eyes community. Participants felt that there needed to be more inter-operability and engagement at the strategic level around global security and climate change impacts.

6.0 Reputation and Change in Public Mood. Public perception was also viewed as changing, both in Australia and especially in the neighbourhood. For example, some prominent Indonesians are saying that democracy is not working for them because politicians tend to focus on elections and looking after the middle class. Defence has a very high status in Australian public opinion and an excellent reputation world-wide. Participants flagged that Defence needs to be conscious of opportunities to maintain this high regard. There was a concern that younger generations would become less supportive of the institutions of state, including Defence, if we take no action to address climate change.

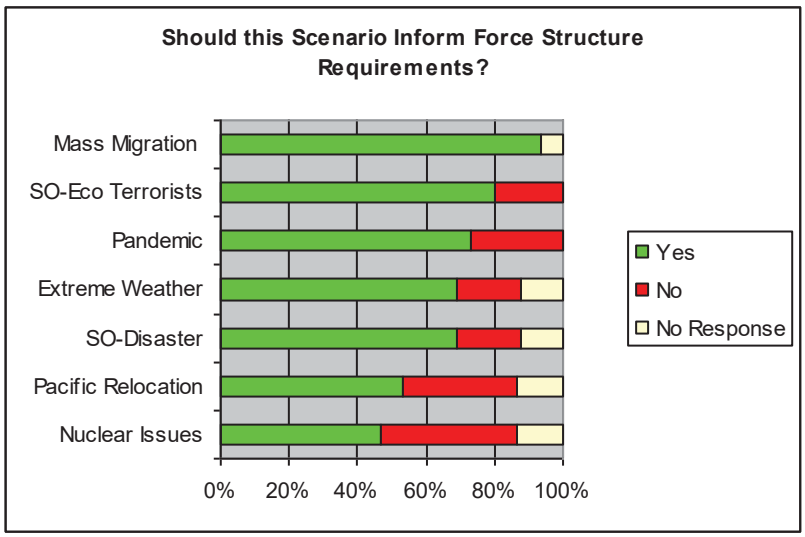
7.0 Other points. There was a common view amongst participants that Defence will have to face the bulk of these scenarios with current personnel, structure and kit. Defence's main opportunities for adaptation were in changing thinking, concepts and doctrine. "We are not going to have new capability or kit but we will be asked to do new things with the kit we have". Intellectual capital as the basis of military skill sets might emphasise appreciation of environment and adaptive planning and execution. New concepts were needed.

Participants viewed Tipping Points as a distinct and uncertain threat, given the difficulty of knowing when a tipping point had been passed. Tipping Points could come from the biophysical world (eg loss of Greenland ice sheet and consequent sea-level rise) or the socio-economic world (eg insurers and large institutional investors decide the costs of doing little or nothing about climate change outweigh the benefits of business as usual). Participants also discussed weak signals and how they might be used, along with discontinuities, to provide forewarning of abrupt or sudden change.

Scenario Relevance Assessment

Hypothetical participants were asked to assess whether the scenarios used should be considered in developing force structure requirements. The table opposite shows participants responses with the most relevant scenarios at the top.

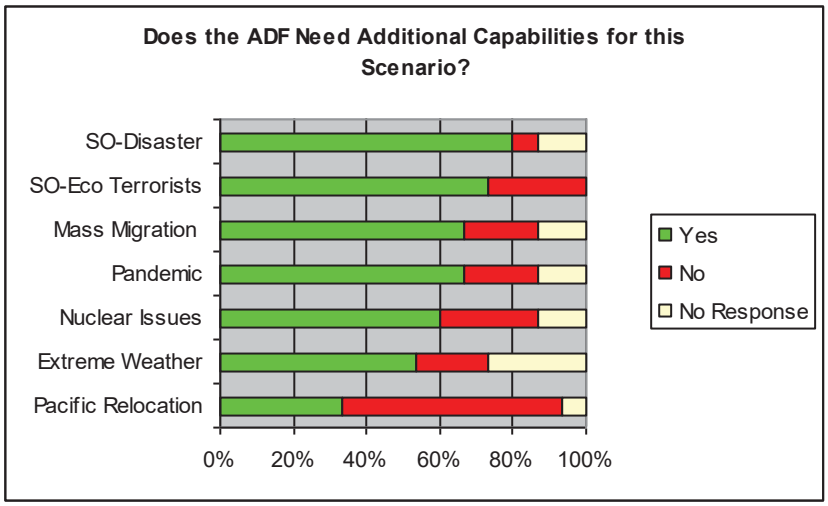
SO= Southern Ocean.



ADF Capability Assessment

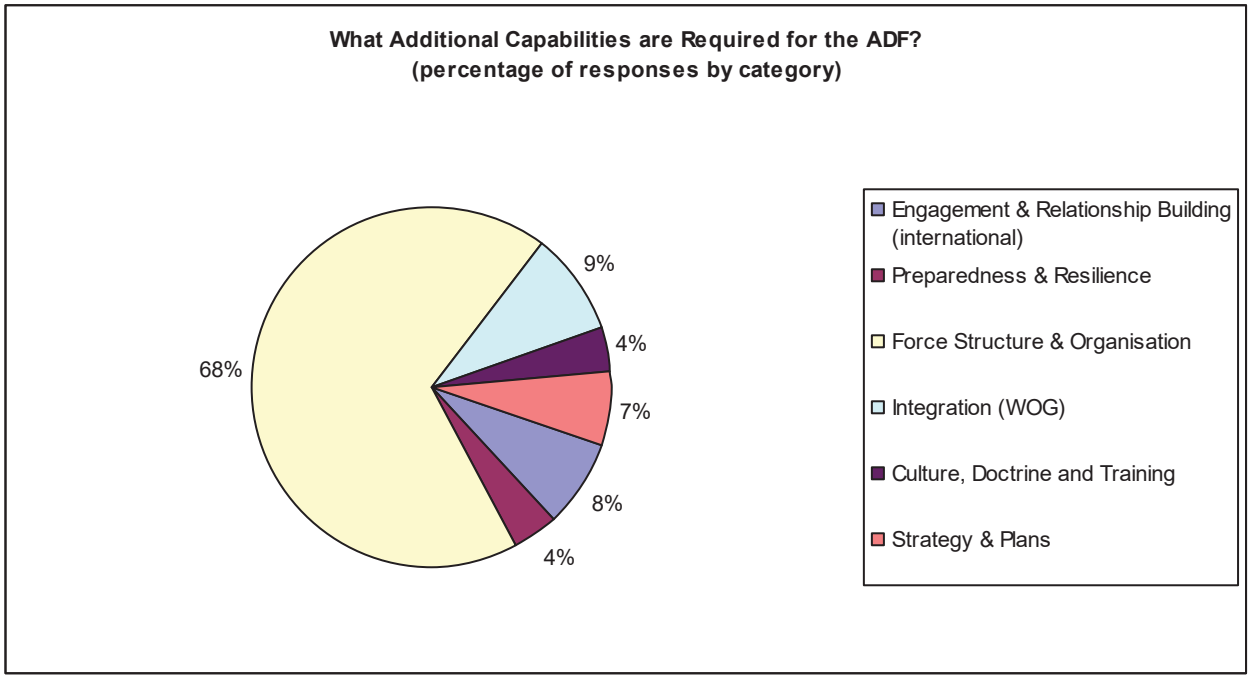
Hypothetical participants were asked whether the ADF would require additional capabilities to responds effectively to each scenario. The table opposite shows participant responses ordered from greatest to least capability need.

Of note the ADF was assessed as least capable with regard to the two Southern Ocean scenarios.



Capabilities to Consider

Participants were asked to suggest additional capabilities that may be needed by the ADF for each of the scenarios. The majority of responses (68%) proposed additional force structure requirements, while just under a third of responses suggested other capabilities such as improved relationship building, strategy, culture, doctrine, preparedness and whole-of-Government integration (including enhanced planning, training and exercising).



Force structure proposals which were suggested by multiple participants and/or for multiple scenarios included: enhanced health capabilities; enhanced maritime and airlift capabilities for southern ocean operations; enhanced maritime surveillance patrol and response capabilities, other ISTAR capabilities including early warning and threat detection and enhanced capabilities for C2 with other Government and coalition partners.

Conclusion-Key Actions For Defence

The following key conclusions and actions were identified by participants during the hypothetical game final session.

- Defence needs to be part of a common national assessment, risk and futures process, incorporating Government, science, industry and community organisations. A rich picture of future environments and risks is an essential start point for planning and monitoring.
- Defence needs to address the future challenge of balancing high end and low end warfighting capabilities. There must be common understanding between Government and Defence on expectations and risks.
- Defence needs to establish a firm economic argument for preventative and adaptive global change responses, and the new capabilities this might entail. The argument of fear is unlikely to be effective.
- Defence needs new thinking in order to address opportunities to mitigate global change impacts and develop responses to security impacts. These two problems are different and should not be confused.
- Defence must address the twin problems of slow acquisition cycles and inflexible budget agreements if it is to adapt with the speed and agility required. Organisational redesign may be required.
- Defence needs to display leadership both nationally and internationally. The sum of five eyes partners, acting in a collegiate manner, can do a lot, but only if Defence is prepared to act.
- Defence needs to develop improved forecasting techniques, using advanced statistical and dynamic models to complement existing point based forecasting and risk assessments.
- Resilience needs to be a central concept in organisational design, capability planning and CoDO planning.

Prepared By: Joint Force Intelligence Analysis and Risk Directorate



JFIAR