



ADF
Australian Defence Force

The Australian War College Shedden Papers 2025



The Australian War College (AWC)

The Australian War College (AWC) delivers world-class Joint Professional Military Education (JPME) focused on leadership, joint warfighting, operations and strategy through the delivery of a range of courses. Its courses have a strong practitioner focus that provides the knowledge, awareness and skills to operate at the highest levels of command and leadership.



The College delivers courses via a range of learning modes, both online, residential and a blend of the two, over periods from a year-long to short courses of several weeks. These modes of learning reflect the needs of modern Defence Forces, and modern pedagogy, and allow maximisation of access to PME across the enterprise. Many courses attract civilian university qualifications (or credits toward further study) from Masters to Graduate Certificate level.

The Defence and Strategic Studies Course (DSSC)

The DSSC is a year-long, full-time course for O-6 level officers from the ADF, the APS (both from Defence and from other Australian Government agencies) and selected allied and regional defence forces. It prepares officers and public service executives for key command and staff appointments where they are able to lead at the strategic levels of the organisation, including formation level command.

The DSSC provides military and government security professionals with the nuanced understanding of national security and strategy required to operate successfully in the increasingly complex and contested regional strategic environment. It also provides them with a series of analytical frameworks, tools and practical insights. Grounded in the National Defence Strategy, the DSSC emphasises the importance of deterrence, resilience, and force projection in an era of strategic competition, reducing warning times and grey-zone threats.

DSSC course members (CM) also critically engage with the interdependence of military, economic, and diplomatic instruments of power, examining how regional alliances, technological advancements, and the evolving nature of warfare shape security postures. Course members graduate with a Master of National Security and Strategy awarded by Deakin University. A capstone research unit required CMs to submit a thesis paper on a national security and strategy issue that aligns with Australian Defence senior leadership priorities.

Copyright

© Commonwealth of Australia 2026

This work is copyright. It may be downloaded, displayed, printed and reproduced in unaltered form, including the retention of this notice, for personal, non-commercial use or use for professional purposes. Apart from any use as permitted under the *Copyright Act 1968*, all other rights are reserved. To replicate all or part of this document for any purpose other than those stipulated above, contact the Editor via email at cdr.publications@defence.gov.au.

Disclaimer

This work is the sole opinion of the authors, and does not necessarily represent the views of The Australian War College, Australian Defence College or the Department of Defence. The Commonwealth of Australia will not be legally responsible in contract, tort or otherwise, for any statement made in this publication.

The Shedden Papers

The Shedden Papers are named after Sir Frederick Shedden KCMG, OBE who was Secretary of the Defence Department from 1937-1956, including the Second World War, the onset of the Cold War and Australia's commitment to the Korean War and the Malayan Emergency.

Sir Frederick Shedden's role went far beyond that of the traditional public servant. He was a central player in some of the most important events in Australian history. He was the key confidant of the Second World War Prime Ministers Robert Menzies and John Curtin, accompanying them in discussions with Prime Minister Winston Churchill and President Franklin Roosevelt. As secretary of the War Cabinet and the Advisory War Council, he was at the heart of the national defence effort when Australia was under threat of invasion. He became the trusted link between Curtin and American General Douglas MacArthur.

On the basis of his experiences during World War II, Sir Frederick Shedden had developed arrangements in the Defence Department which had laid the foundations for closer co-ordination and direction of defence policy and administration.

The Shedden Papers are produced by the Australian Defence College on behalf of the Commandant of the Australian War College. These papers represent the best capstone research papers of the previous year's Defence and Strategic Studies Course graduates and have been chosen for publication based on their scholarly attributes and the timeliness of their topic.

This page is intentionally blank

Foreword



Australia's strategic environment is evolving with speed and complexity that demands disciplined analysis, informed judgement and a cohesive national effort. The Indo-Pacific is now defined by intensifying strategic competition, rapid military modernisation, and persistent grey-zone coercion, making the region more contested and unpredictable than any time in recent decades.

In this context, the Shedden Papers provide a timely demonstration of the intellectual depth and professional acumen within Defence. This publication is not simply a compilation of academic work; it represents the considered thinking of experienced practitioners who already hold significant responsibilities across Defence and the national security enterprise and who will shape strategic decision-making in the years to come.

What distinguishes this year's collection is its strategic orientation. Contributors engage directly with the concepts, doctrine, and policy settings that underpin Defence's approach to force design, capability development, and integrated deterrence. Many papers highlight the imperative of coordinated, multi-agency action and the critical role of Australia's alliances and partnerships in strengthening our strategic posture. Authors adopt a global perspective recognising that Australia's security interests are deeply connected to developments well beyond our immediate region.

Collectively, these papers reinforce a fundamental truth for Defence leadership. Our advantage rests not only in advanced capabilities, but in the strategic literacy, intellectual agility, and judgement of our people. The ability to interrogate assumptions, synthesise complex information, and anticipate emerging risks is essential to Defence's ability to navigate uncertainty and maintain decision-making superiority.

I commend the authors for their rigorous and thoughtful contributions. I trust the insights contained within the Shedden Papers will support Defence's senior leaders in fostering a culture of critical inquiry, strengthening our strategic workforce, and preparing the next generation of Defence leaders for the challenges ahead.

A handwritten signature in black ink, appearing to read 'Lara Troy'.

Brigadier Lara Troy, CSC
Commandant, Australian War College

This page is intentionally blank

Contents

Foreword	5
How Can Small States Deter Cyberattacks? A Layered Approach to Deterring Grey Zone Threats in Cyberspace	11
About the Author	12
Abstract.....	13
Abbreviations and Acronyms.....	14
Chapter 1: Introduction.....	15
Chapter 2: Theoretical Framework	19
Chapter 3: Estonia	27
Chapter 4: Singapore	39
Chapter 5: Lessons for Small States	49
Chapter 6: Conclusion.....	57
Bibliography	60
Siloed Systems, Shared Stakes: Keeping the Nation’s Engine from Stalling	71
About the Author	72
Summary.....	73
Introduction	74
Chapter 1: How Market Logic Undermined Resilience.....	79
Chapter 2: Why Liquid Fuels Will Remain Important to National Capability	85
Chapter 3: The Review and Policy Package.....	92
Chapter 4: Finland and Japan’s Fuel Resilience Measures	97
Chapter 5: Stockpiles to Sovereignty, Low-Carbon Liquid Fuels as a Strategic Capability	101
Conclusion	107
Bibliography	111

What is the 'International Rules-based Order'? Does the use of this terminology advance Australia's foreign policy interests?

interests?	119
About the Author	120
Summary.....	121
Introduction	123
Chapter 1: The emergence of 'rules-based international order' terminology	127
Chapter 2: The 'rules-based international order' v. the 'liberal international order'	133
Chapter 3: When was the 'international rules-based order' created, and what does it comprise?.....	141
Chapter 4: The rules-based international order is 'under strain'.....	147
Chapter 5: What is the distinction between the 'order' and international law?	151
Chapter 6: Who is using 'rules-based order' terminology? Who is not?	157
Chapter 7: Implications for Australia's foreign policy	161
Conclusion	163
Bibliography	165

Autonomy and Artificial Intelligence in Hydrography: Royal

Australian Navy's Future Workforce	173
About the Author	174
Summary.....	175
Introduction	177
Chapter 1: The Evolving Landscape of RAN Hydrographic Capability	183
Chapter 2: The Strategic Dimensions Impacting Hydrography in the Indo-Pacific	191
Chapter 3: Autonomous Technologies and AI in Modern Hydrography	195
Chapter 4: Integrating Autonomy: A Comparative Analysis of RAN and Allied Experiences.....	199
Chapter 5: Workforce Transformation for an Autonomous Future: The Core Analysis.....	202

Chapter 6: The Supporting Ecosystem: Industry, Research, and Innovation .	209
Chapter 7: Policy, Doctrine, and Regulatory Alignment: Supporting the Transformation	213
Chapter 8: Conclusion: Navigating the Future	219
Bibliography	225
Case Studies in Strategy	235
About the Authors	237
Case Study 1: Lessons for students of strategy from economics – getting the economics of war wrong.....	238
Case Study 2: Ancient Carthage – Power and Strategy in the Punic Wars	247
Case Study 3: Having applied relevant theory and concepts to the Byzantine Empire, what are the most important lessons for students of strategy?	259



Image: Brian. Available at <https://cybercoversg.com/2025/strengthening-cyber-defenses-singapores-new-military-commands/>



How Can Small States Deter Cyberattacks? A Layered Approach to Deterring Grey Zone Threats in Cyberspace

Colonel Chen Bingqiang, Singapore Armed
Forces - Army



About the Author



Bingqiang Chen is an Army officer in the Singapore Armed Forces and has served in a variety of command and staff appointments over the past 25 years. He attended the Defence and Strategic Studies Course at the Australian War College in 2025 and graduated from the Goh Keng Swee Command and Staff College (Singapore) in 2015. He holds a Bachelor of Computer Engineering from Nanyang Technological University (Singapore)

and a Master of Science in Engineering Science from the Naval Postgraduate School (United States).

This paper reflects his personal views and does not represent those of the Singapore Armed Forces.

Abstract

This thesis asks: how can small states deter cyberattacks that sit in the grey zone between peace and war? It argues that small states cannot deter through scale or offence but by layering four mechanisms – punishment, denial, norms and entanglement – in ways that fit their strategic cultures. Using a comparative case study of Estonia and Singapore, the project assesses how each state combines denial, calibrated punishment, and norm- and interdependence-based strategies to raise costs, reduce gains, and narrow the payoff surface for hostile operations. The analysis adopts a realistic benchmark: deterrence is evidenced not by zero incidents, but by adversary restraint from large-scale, destructive, or politically significant attacks, and by rapid containment and recovery when incidents occur. Findings show denial-as-resilience is the foundation; norms and entanglement amplify its effects by widening coalitions and reputational costs; and punishment works best when proportionate, coalition-minded, and signalled clearly. Estonia demonstrates agenda-setting power through CCDCOE, the Tallinn Manual process, EU/NATO tools, and public attribution; Singapore emphasises institutional resilience, legal-regulatory instruments, economic entanglement, and diplomatic convening. The result is a tailored, layered cyber deterrence posture that small states can afford, sustain, and credibly signal.

Abbreviations and Acronyms

The detailed abbreviations and definitions used in the paper are listed in **Table 1**.

Table 1: List of Abbreviations and Definitions

Abbreviation	Definition
APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
CBM	Confidence Building Measure
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDU	Cyber Defence Unit
CERT-EE	Computer Emergency Response Team-Estonia
CIDeX	Critical Infrastructure Defence Exercise
CII	Critical Information Infrastructure
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CSA	Cyber Security Agency of Singapore
DDoS	Distributed Denial-of-Service
DIS	Digital and Intelligence Service
EDF	Estonian Defence Forces
EU	European Union
FOSS	Forum of Small States
GGE	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
GRU	Glavnoye Razvedyvatelnoye Upravlenie (Foreign military intelligence agency of Russia's General Staff)
GZ	Grey Zone
IHL	International Humanitarian Law
NATO	North Atlantic Treaty Organisation
OEWG	Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security
RIA	Estonia's Information System Authority
SAF	Singapore Armed Forces
SingCERT	Singapore Cyber Emergency Response Team
UN	United Nations

Chapter 1: Introduction

1.1 Background

Over the past two decades, cyberspace has become both a critical enabler of prosperity and an arena of contestation. The Internet and digital connectivity underpin global finance, communications, critical infrastructure, and national security. Yet the same interdependence generates great vulnerability. States and non-state actors exploit the digital domain to pursue political goals through operations below the threshold of armed attack. These *grey zone* (GZ) activities deliberately calibrate coercion, exploiting legal and political ambiguity to erode state capacity and will.¹

For small states, this environment poses acute challenges. Lacking the scale, offensive capacity, and redundancy of major powers, small states are disproportionately exposed to cyber threats.² Estonia's 2007 distributed denial-of-service campaign highlighted this vulnerability, when attacks linked to Russia significantly disrupted government, banking, and media networks.³ In Southeast Asia, Singapore has been a sustained target of advanced persistent threats (APTs).⁴ These cases illustrate that cyber coercion is no longer a theoretical risk but an everyday feature of international competition.

Classical deterrence theory, rooted in nuclear strategy, offers only partial guidance. Whereas nuclear deterrence sought total prevention through credible threats of retaliation, cyber deterrence is less absolute. Attribution difficulties, low barriers to entry, and the sheer frequency of malicious cyber activity complicate the translation of Cold War concepts to the digital age. As Joseph Nye argues, cyber deterrence should be conceived flexibly: raising costs and reducing gains through punishment, denial, entanglement, and norms.⁵ This layered approach is particularly relevant for small states, which cannot rely on scale or offence but can shape adversary behaviour through resilience, signalling, and multilateral posture.

¹ Hal Brands, 'Paradoxes of the Gray Zone', SSRN Scholarly Paper no. 2737593 (Social Science Research Network, 1 January 2016), 1, <https://doi.org/10.2139/ssrn.2737593>.

² Eugene E.G. Tan, 'A Small State Perspective on the Evolving Nature of Cyber Conflict: Lessons from Singapore', *PRISM* 8, no. 3 (2019): sect. Small States and Cyber Conflict.

³ Piret Pernik, *Cyber Deterrence: A Case Study on Estonia's Policies and Practice*, no. 8, Hybrid CoE Paper (European Centre of Excellence for Countering Hybrid Threats, 2021), 11, https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf.

⁴ K. Shanmugam, 'Opening Speech by Mr K Shanmugam, Coordinating Minister for National Security and Minister for Home Affairs, at CSA's 10th Anniversary Dinner', Cyber Security Agency of Singapore, 19 July 2025, sect. Advanced Persistent Threats, <https://www.csa.gov.sg/news-events/speeches/opening-speech-by-mr-k-shanmugam--coordinating-minister-for-national-security-and-minister-for-home-affairs-at-csa-10th-anniversary-dinner/>.

⁵ Joseph S. Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security* 41, no. 3 (2017): sect. The Problem of Attribution, https://doi.org/10.1162/isec_a_00266.

1.2 Puzzle Statement and Research Question

The core puzzle that animates this thesis is straightforward: how can small states deter cyberattacks in the GZ despite their structural disadvantages?

On the one hand, sceptics argue that deterrence in cyberspace is impossible, pointing to the persistent volume of intrusions and the limits of attribution.⁶ From this perspective, small states remain vulnerable, reliant on external security guarantees and unable to impose costs on adversaries. On the other hand, others suggest that deterrence in cyberspace can work – but in more modest and behavioural terms.⁷ Since 2007 Estonia has not again suffered a nationwide disruption, despite repeated Russian-linked campaigns.⁸ Similarly, Singapore has thus far avoided large-scale, destructive cyber incidents that undermined its national security.⁹ These outcomes raise an important question: if zero incidents are an unrealistic benchmark, what constitutes effective deterrence for small states?

This thesis contends that cyber deterrence should be assessed not by absence of all intrusions, but by whether adversaries refrain from large-scale, destructive, or politically decisive operations; and whether, when intrusions occur, the state can absorb, contain, and recover quickly. By this behavioural benchmark, deterrence in cyberspace is less about total prevention than about shaping adversary expectations and denying easy success.

Guided by this puzzle, the thesis asks: How can small states deter GZ cyberattacks, and what lessons can be drawn from the cases of Estonia and Singapore? This question has both theoretical and practical significance. Theoretically, it contributes to ongoing debates about the applicability of deterrence to cyberspace, in particular, for small states. Practically, it offers insights for policymakers in small states, who must craft strategies of survival and influence in a domain where asymmetry is acute.

1.3 Scope

This thesis examines how small states deter politically motivated GZ cyberattacks – specifically, computer network attack (CNA) and computer network exploitation (CNE).¹⁰ CNA aims to disrupt or destroy computer systems, networks, information or

⁶ Michael P. Fischerkeller and Richard J. Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', *Orbis* 61, no. 3 (2017): 381–93, <https://doi.org/10.1016/j.orbis.2017.05.003>.

⁷ Erica D. Borghard and Shawn W. Lonergan, 'Deterrence by Denial in Cyberspace', *Journal of Strategic Studies* 46, no. 3 (2023): 537, <https://doi.org/10.1080/01402390.2021.1944856>.

⁸ Information System Authority (RIA), *Cyber Security in Estonia 2023* (Republic of Estonia, Information System Authority (RIA), 2023), 9–10, <https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf>.

⁹ Tan, 'A Small State Perspective on the Evolving Nature of Cyber Conflict', 165.

¹⁰ In this thesis, the term “cyberattack” is used in a practical, non-legal sense as an umbrella term for hostile cyber operations, encompassing both CNA and CNE.

programmes, while CNE involves the covert exfiltration of confidential information.¹¹ Propaganda and disinformation campaigns are recognised as part of the broader threat in cyberspace, but lie outside the scope for this thesis. Purely profit-motivated crime is also excluded, unless directed, tolerated, or instrumentalised by state actors. Accordingly, it is limited to cyber operations with strategic intent or national-security implications. This delimitation reflects analytical tractability and the distinct legal-strategic challenges of GZ state activity.

1.4 Methodology and Case Selection

This thesis employs a comparative case study method. Case studies allow in-depth analysis of how theoretical concepts are applied in practice, and comparison between cases provides the basis for drawing more generalisable lessons. Estonia and Singapore are selected for three reasons.

First, both are small states: with populations under ten million, they fit the UN Forum of Small States' definition.¹² Both are highly digitalised, with economies and governance systems dependent on secure networks, making them especially exposed to cyber threats.

Second, both have been early movers in shaping cyber policy. Estonia's 2007 crisis catalysed the development of whole-of-society resilience, international legal works such as the Tallinn Manuals, and institution-building including NATO's Cooperative Cyber Defence Centre of Excellence.¹³ Singapore has invested in a centralised Cyber Security Agency, a statutory framework through the Cybersecurity Act, and regional and UN cyber diplomacy.¹⁴

Third, the cases offer variation in strategic culture and geopolitical context. Estonia is a member of the North Atlantic Treaty Organisation (NATO) and the European Union (EU) confronting persistent pressure from Russia, and anchors deterrence in collective defence and norm entrepreneurship.¹⁵ Singapore, by contrast, is a non-aligned, trade dependent hub in a multipolar Asia, balancing major powers.¹⁶ This variation allows

¹¹ The boundary between exploitation and attack is thin. Common to both is the intrusion of a computer system, network, and programme. Once access is established, a collection can be re-tasked to encrypt, disrupt, or destroy with only minor code changes. For more information on CNA and CNE, see: Rhea Siers, 'Cybersecurity', in *Security Studies*, 4th edn, by Paul D Williams and Matt McDonald (Routledge, 2023), sect. Introduction: cyber terminology and typology, <https://doi.org/10.4324/9781003247821-44>.

¹² Andrea Ó Súilleabháin, *Small States at the United Nations: Diverse Perspectives, Shared Opportunities* (International Peace Institute, 2014), 3, https://www.ipinst.org/wp-content/uploads/publications/ipi_e_pub_small_states_at_un.pdf; 'Country Comparisons - Population', The World Factbook, accessed 17 September 2025, <https://www.cia.gov/the-world-factbook/field/population/country-comparison/>.

¹³ Pernik, *Cyber Deterrence*.

¹⁴ Tan, 'A Small State Perspective on the Evolving Nature of Cyber Conflict'.

¹⁵ Pernik, *Cyber Deterrence*.

¹⁶ Tan, 'A Small State Perspective on the Evolving Nature of Cyber Conflict'.

assessment of how small states adapt cyber deterrence strategies to distinct environments.

The empirical material for this study draws on a wide range of primary and secondary sources: government strategies, laws, and speeches; reports from NATO, Association of Southeast Asia Nations (ASEAN), and the UN; scholarly analyses; and policy documents. Given the sensitivity of cyber incidents, open-source data are partial, but sufficient to trace patterns of state practice and outcomes.

Case-Selection Caveat

Both Estonia and Singapore are relatively wealthy,¹⁷ institutionally capable small states with high levels of digitalisation and governance capacity,¹⁸ and strong defensive cyber capabilities.¹⁹ This selection enables in-depth analysis of advanced small-state approaches to cyber deterrence, but it also constrains generalisability. The lessons are most directly applicable to small states with comparable resources and institutional strength and will require adaptation for poorer, fragile, or conflict-affected contexts.

1.5 Structure of the Thesis

The thesis proceeds in six chapters. Chapter 2 lays out key definitions and the theoretical framework. Chapters 3 and 4 present the case studies of Estonia and Singapore respectively, examining their deterrence posture and assessing their efficacy. Chapter 5 then compares the two cases, identifying common strategies and divergences. Chapter 6 synthesises findings, evaluates the viability of the layered deterrence framework for small states, and sets out limitations and generalisability, outlines implications for policy, practice, and future research.

¹⁷ Based on Global Finance Magazine's ranking of countries by Gross Domestic Product–Purchasing Power Parity (GDP-PPP) per capita, Estonia is ranked 47th, while Singapore tops the list of the world's richest countries. See: Luca Ventura, 'Richest Countries in the World 2025', *Global Finance Magazine*, 3 September 2025, <https://gfmag.com/data/richest-countries-in-the-world/>.

¹⁸ 'Press Release | Digital Transformation Accelerates, but Gaps Underscore Need for New Framework to Advance Use of Technologies in Governments', *United Nations Sustainable Development*, 17 September 2024, <https://www.un.org/sustainabledevelopment/blog/2024/09/press-release-e-government-survey/>.

¹⁹ The National Cyber Security Index (NCSI), developed by the e-Governance Academy (eGA), an Estonia-based think tank, measures national preparedness to prevent cyber threats and respond effectively to cyber incidents. According to the latest NCSI scores, Estonia ranks 4th and Singapore 18th. See: 'National Cyber Security Index: Ranking', NCSI, accessed 17 September 2025, <https://ncsi.ega.ee/ncsi-index/?order=rank>.

Chapter 2: Theoretical Framework

2.1 Introduction

This chapter establishes the theoretical foundation for the thesis. It does three things. First, it sets a clear definitional baseline for “small states” and outlines recurrent behavioural traits associated with smallness (Section 2.2).²⁰ Second, it explains why cyberspace is a privileged arena for GZ competition and why classical deterrence logic maps only partially onto this domain (Sections 2.3–2.5). Third, it introduces Joseph Nye’s four mechanisms—punishment, denial, norms and entanglement—as the organising framework for cyber deterrence and shows how they apply to small states (Section 2.6).

Throughout, the chapter advances the thesis argument: small states deter by layering mechanisms in ways consistent with their strategic cultures – anchoring deterrence in resilience (denial), clear signalling (including proportionate punishment and attribution), and a multilateral posture (norms and entanglement). This framework sets the criteria and vocabulary used in the Estonia and Singapore case studies.

2.2 Defining Small States and Behavioural Traits

There is no consensus definition of a “small state”. Different authors deploy varying measures – population size, territory, GDP, or power.²¹ Even one of the most common measures – population size – is operationalised at different cut-offs.²² Further, **relative** size also matters, since smallness is frequently understood as relational.²³ For definitional clarity in this thesis, however, we adopt a pragmatic baseline: the UN Forum of Small States (FOSS) convention defining small states as those with a population

²⁰ Andrea Ó Súilleabháin, *Small States at the United Nations*, 3.

²¹ Jeanne Hey, ed., *Small States in World Politics : Explaining Foreign Policy Behavior* (Lynne Rienner, 2003), 2, deakin.b2023628, <https://research.ebsco.com/linkprocessor/plink?id=cbcffc5a-30f1-3d14-b114-ddbd7ca7c137>.

²² Population thresholds for “small states” vary across organisations and studies. The World Bank uses ≤1.5 million; and the UN Forum of Small States is open to members with <10 million at the time of joining. In empirical work, common cut-offs include ≤3 million (e.g., Armstrong et al. 1998), and ≤5 million (e.g., Armstrong & Read 2006). See: ‘Overview’, Text/HTML, World Bank, accessed 16 September 2025, <https://www.worldbank.org/en/country/smallstates/overview>; Andrea Ó Súilleabháin, *Small States at the United Nations*; H. Armstrong et al., ‘A Comparison of the Economic Performance of Different Micro-States, and between Micro-States and Larger Countries’, *World Development* 26, no. 4 (1998): 641, [https://doi.org/10.1016/S0305-750X\(98\)00006-0](https://doi.org/10.1016/S0305-750X(98)00006-0); Harvey Armstrong and Robert Read, ‘Geographical “handicaps” and Small States: Some Implications for the Pacific from a Global Perspective’, *Asia Pacific Viewpoint* 47, no. 1 (2006): 79, <https://doi.org/10.1111/j.1467-8373.2006.00294.x>.

²³ Živilė Marija Vaicekauskaitė, ‘Security Strategies of Small States in a Changing World’, *Journal on Baltic Security* 3, no. 2 (2017): 9, <https://doi.org/10.1515/jobs-2017-0006>.

under 10 million.²⁴ This places both Estonia and Singapore within scope while preserving comparability.

Beyond size, small states tend to exhibit recurring behavioural traits shaped by external exposure: adaptiveness and niche specialisation; a propensity to seek influence through membership in international organisations; selective alliance participation for hard-security guarantees; a strong preference for a rules-based order and legalism;²⁵ coalition-building and network diplomacy; and heightened attention to reputation and signalling.²⁶ In cyberspace specifically, these patterns translate into emphasis on public–private cooperation, capacity-building with partners, advocacy for international norms, and participation in regional or functional arrangements that enable information-sharing and collective response.²⁷

2.3 Grey Zone and Cyberspace

The GZ describes the ambiguous space between peace and war, where actors pursue strategic objectives through coercive or disruptive means without crossing thresholds that would trigger conventional military responses. GZ threats span a wide spectrum, including disinformation campaigns, economic coercion, cyberattacks, and political interference.²⁸ In this sense, the concept can be seen as a modern evolution of George Kennan's 1948 notion of political warfare: "the use of all the means at a nation's command, short of war, to achieve its national objectives,"²⁹ albeit manifesting in a more interconnected and technologically advanced world.

Cyberspace has become an especially potent arena of GZ competition. Its inherent attributes – speed, global reach, anonymity and low cost of entry – make it an attractive environment for state actors to conduct GZ operations covertly and with plausible deniability. In cyberspace, GZ threats span a continuum to impose costs and shape behaviour. These include: (1) low-end nuisance activity: website defacements, phishing, and distributed denial-of-service (DDoS); (2) mid-range coercion: stealthy espionage and supply-chain compromises; and (3) high-end disruptive or destructive operations: pre-positioning in critical infrastructure, data-wiping campaigns, and cyber-physical attacks on industrial control systems.

The 2020 SolarWinds cyber-espionage campaign illustrates the GZ dynamics. Exploiting a trusted supply-chain, a Russian state-linked group compromised the update mechanism of a widely used IT management platform, gaining access to U.S. government and private-sector networks. For months, the operation remained

²⁴ Andrea Ó Súilleabháin, *Small States at the United Nations*, 3.

²⁵ Vaicekauskaitė, 'Security Strategies of Small States in a Changing World', 9.

²⁶ Vaicekauskaitė, 'Security Strategies of Small States in a Changing World'.

²⁷ Marius Kristiansen and Njaal Hoem, 'Small Players in a Limitless Domain: Cyber Deterrence as Small State Strategy', *Comparative Strategy* 41, no. 1 (2022): sect. Cyber-deterrence strategy, <https://doi.org/10.1080/01495933.2021.2017740>.

²⁸ Brands, 'Paradoxes of the Gray Zone', 1.

²⁹ George F. Kennan, 'Historical Documents - Office of the Historian', U.S. Office of the Historian, 4 May 1948, <https://history.state.gov/historicaldocuments/frus1945-50Intel/d269>.

undetected and yielded significant intelligence benefits. Because the exploit caused no physical damage, it remained below the legal and political threshold of armed conflict, enabling the perpetrators to extract strategic gains while avoiding escalation.³⁰

2.4 Classical Deterrence Theory

Deterrence aims to prevent hostile action by convincing an adversary that the costs of acting will outweigh any possible benefits. Though the idea is ancient, it was most fully developed during the Cold War in the context of nuclear strategy. Thomas Schelling described deterrence as “to prevent from action by fear of consequences,”³¹ while Glenn Snyder conceptualised it as an adversary’s cost-gain calculation.³² The logic of deterrence is fundamentally psychological: it seeks to shape the perceptions of adversaries rather than their capabilities alone.

Two primary mechanisms underpin classical deterrence. The first is punishment, which threatens severe consequences after aggression to raise the perceived costs. The second is denial, which reduces the likelihood of an attack’s success, thereby lowering the perceived benefits. Over time, scholars distilled effective deterrence into the “three Cs”: capability, credibility, and communication. First, the deterring state must possess the capability to punish or deny. Second, this capability must be credible, meaning that the adversary believes the state has the willingness to act. Third, the threat must be communicated clearly and unambiguously.³³ A failure in any of these dimensions undermines deterrence as a whole.³⁴

2.5 Challenges of Classical Deterrence in Cyberspace

Classical deterrence, developed in the context of nuclear strategy, struggles to map neatly onto the dynamics of cyberspace, where both punishment and denial face particular difficulties. The very features that make cyberspace attractive for GZ activity

³⁰ Marcus Willett, ‘Lessons of the SolarWinds Hack.’, *Survival* (0039-6338) 63, no. 2 (2021): 8–13, 157382767, <https://doi.org/10.1080/00396338.2021.1906001>.

³¹ Thomas C. Schelling 1921-2016, author. and Anne-Marie Slaughter, *Arms and Influence / by Thomas C. Schelling ; with a New Introduction by Anne-Marie Slaughter.*, Veritas paperback edition. (Yale University Press, 2020), 71, deakin.b4348287, <https://research.ebsco.com/linkprocessor/plink?id=aa500363-cb53-37a5-a63a-9b513c836277>.

³² Glenn H. (Glenn Herald) Snyder 1924-2013., *Deterrence and Defense: Toward a Theory of National Security* (Princeton University Press, 1961), 10, deakin.b3376548, <https://research.ebsco.com/linkprocessor/plink?id=5bd036b2-3de4-340b-80f3-96b7e11d2605>.

³³ Robert P. Haffa, ‘The Future of Conventional Deterrence: Strategies for Great Power Competition’, *Strategic Studies Quarterly* 12, no. 4 (2018): 96–97; Robert Peters et al., ‘Deterrence in the 21st Century: Integrating Nuclear and Conventional Force’, *Strategic Studies Quarterly* 12, no. 4 (2018): 17.

³⁴ Justin Lynch and Emma Morrison, *Through AI-Enabled Detection and Attribution*, The Kissinger Center Papers (John Hopkins School of Advanced International Studies, 2023), 1, <https://mediahost.sais-jhu.edu/saismedia/media/web/files/kissinger/deterrence-through-ai-enabled-detection-attribution-v2.pdf>.

– speed, anonymity, and the limited visibility of effects – also undermine the applicability of classical deterrence logic.

Challenges in Punishment

Deterrence by punishment is especially constrained in cyberspace because of two interrelated problems.

Attribution. Cyberattacks are often routed through multiple jurisdictions, using proxy servers, botnets, or compromised infrastructure to conceal their origin. Even when attribution is technically feasible, forensic investigation is time-consuming,³⁵ and political leaders may hesitate to assign blame publicly without near-certainty – both to avoid escalation due to flawed evidence and to protect sensitive intelligence sources.³⁶ This uncertainty undermines the credibility of punishment, since retaliation requires confidence in identifying the responsible actor.

Proportionality. Cyber operations such as espionage, data theft, or service disruption often lack the visibility or immediacy of conventional attacks. Their impacts are diffuse and incremental, raising doubts about whether they warrant a forceful response. Retaliation with military force would often appear disproportionate, while the use of offensive cyber capabilities is further constrained by their one-use nature, as such tools lose value once exposed.³⁷ This dynamic further undermines the credibility of punishment.

Challenges in Denial

Denial strategies also confront distinctive obstacles in cyberspace:

Accessibility of cyberattack tools. Unlike nuclear deterrence, where possession of a second-strike capability offers a credible deterrent effect, no defensive posture in cyberspace can ensure a zero-incident environment. The accessibility of cyberattack tools and the array of exploitation methods – such as phishing, insider threats, and supply-chain compromises – within a highly networked environment make perfect prevention impossible.³⁸

As these challenges demonstrate, the two central pillars of classical deterrence – punishment and denial – are difficult to apply effectively in cyberspace.

³⁵ William F. III Lynn, 'Defending a New Domain - The Pentagon's Cyberstrategy', *Foreign Affairs* 89, no. 5 (2010): 99, edshol.hein.journals.fora89.79.

³⁶ Sico van der Meer, 'Deterrence of Cyber-Attacks in International Relations: Denial, Retaliation and Signaling', *International Affairs Forum* 2 (2017): 87–88.

³⁷ Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009), 102–3, 304894, <https://research.ebsco.com/linkprocessor/plink?id=32d30978-3bb9-3fa2-be80-7e1256a68a1d>.

³⁸ Nye, 'Deterrence and Dissuasion in Cyberspace', 50.

2.6 Cyber Deterrence and Small States

Given the above limitations, a zero-incident standard for cyber deterrence is both unrealistic and unhelpful. Scholars and practitioners argue that deterrence can still operate in cyberspace, but it cannot be measured by the mere absence of hostile activity. A more realistic benchmark is whether adversaries refrain from conducting large-scale, destructive, or politically significant cyberattacks. In this sense, cyber deterrence is less about preventing every intrusion than about shaping adversary behaviour: raising perceived costs, reducing likely gains, and denying easy success.³⁹

Applied to small states, three scope conditions shape the choice and weight of mechanisms: limited unilateral punishment capacity; priority on denial and whole-of-society resilience; and leverage through norms and entanglement.

Joseph Nye provides a particularly useful framework for cyber deterrence, identifying four mechanisms to influence adversary decision-making by raising costs and reducing benefits through punishment, denial, entanglement, and norms. Each represents a distinct way of influencing adversary decision-making, and together they capture the range of options available to mount deterrence in cyberspace – particularly useful for deterring GZ threats in cyberspace.⁴⁰ This thesis adopts Nye's framework for GZ threats in cyberspace and applies it to small states.

For small states the relevance and applicability of these mechanisms vary. Limited military and economic power constrain their ability to wield punishment credibly. The salience of denial and resilience is further heightened for those with high digital dependence. Norms and entanglement, meanwhile, offer pathways for small states to leverage interdependence and legitimacy to offset material weakness by raising reputational and collateral costs.

The following subsections examine each of these mechanisms in turn. For each, the discussion first outlines the general logic of deterrence and then considers its specific implications for small states.

Punishment

Punishment seeks to deter by threatening retaliation severe enough to outweigh the benefits of aggression. In cyberspace, while this logic continues to be constrained by attribution challenges and proportionality dilemmas, it still has a role. Where attribution is strong, states may impose costs through cyber countermeasures, economic sanctions, diplomatic expulsions, or even military signalling.⁴¹

For small states, punishment is often the least accessible deterrence mechanism. Their limited offensive cyber capabilities and modest economic or military leverage undermine the credibility of unilateral retaliation. While measures such as criminal prosecution,

³⁹ Nye, 'Deterrence and Dissuasion in Cyberspace', 54–55.

⁴⁰ Nye, 'Deterrence and Dissuasion in Cyberspace', sect. Four Means of Deterrence and Dissuasion.

⁴¹ Nye, 'Deterrence and Dissuasion in Cyberspace', 55–56.

targeted sanctions, or diplomatic expulsions are available, they are rarely decisive on their own. Consequently, punishment tends to play a supplementary rather than central role in small-state deterrence, though its effectiveness can be enhanced through collective attribution and multilateral action with larger powers or international organisations.

Denial

Denial focuses on reducing the adversary's likelihood of success. This includes hardening digital infrastructure, increasing redundancy, improving incident response, and raising societal awareness. Denial does not depend on retaliatory capacity. A well-prepared target that can absorb and recover swiftly from an attack raises the cost and denies the aggressor their intended outcome.⁴²

For small states, denial assumes heightened importance. Because they cannot rely on



Image: Silicon UK. Available at <https://www.silicon.co.uk/workspace/council-cyber-attack-331750>

punishment to credibly deter, their primary imperative is to frustrate adversaries' strategic objectives by reducing the effectiveness of attacks. This extends beyond technical safeguards to include political and societal resilience: the ability of state institutions and population to adapt and continue functioning despite disruption. In this sense, denial provides small states with a practical and credible foundation for deterrence, signalling that cyber

operations will not yield the destabilisation or leverage that aggressors seek.

Entanglement

Entanglement deters by leveraging interdependence to complicate decision-making. When states are bound together through economic, political, or institutional linkages, an attack on one risks producing costs for the attacker as well as the victim. Interdependence can also generate caution, as leaders hold back from aggression for fear of wider repercussions. In cyberspace, the logic of entanglement is amplified because digital operations can produce cascading effects across interconnected networks, including those on which the attacker itself relies.⁴³

For small states, entanglement is both constrained and conditional. Often lacking the economic or strategic weight to generate interdependence on their own, their deterrent value from entanglement may rest more on embedding themselves in alliances, regional institutions, and global markets. By integrating into these wider networks, small states

⁴² Nye, 'Deterrence and Dissuasion in Cyberspace', 56–58.

⁴³ Nye, 'Deterrence and Dissuasion in Cyberspace', 58–60.

can indirectly raise the costs of aggression, since attacks risk cascading effects across systems that also affect larger stakeholders. This prospect of wider consequences can induce caution in potential adversaries, enhancing the small state's security despite its limited independent means.

Norms

Finally, norms provide deterrence through shared expectations about responsible behaviour. Normative deterrence does not rely on direct threats, but on reputational and diplomatic costs for violators. Active participation in international forums, consistent signalling of norms, and public attribution of violations can enhance the reputational risks for aggressors, particularly those who value their global standing. Norms are not absolute constraints, but they raise the political and diplomatic price of irresponsible behaviour in cyberspace.⁴⁴

For small states, norms function as a strategic multiplier. Because they cannot rely on material power, small states can amplify their influence by positioning themselves as norm entrepreneurs or trusted participants in global cyber governance. By championing responsible behaviour, they can enhance the reputational and diplomatic costs faced by aggressors, and build coalitions that enable collective responses. While norms cannot prevent all hostile activity, they create political space that small states can leverage to reinforce deterrence and compensate for their limited hard power.

Taken together, these four mechanisms offer small states a spectrum of tools to influence adversary decision-making despite their structural vulnerabilities. While Nye introduced them as distinct logics of deterrence, subsequent scholarship has highlighted the value of layering them to create cumulative effects.⁴⁵ Building on this insight, this thesis adapts the layered posture:

- (1) Norms – shaping expectations of responsible behaviour to promote cyber stability;
- (2) Entanglement – embedding the small state within wider networks so that any attack risks broader consequences;
- (3) Denial – building defences and resilience to frustrate attacks and deny adversaries their intended outcomes; and
- (4) Punishment – imposing costs to reinforce norms and deter future violations.

⁴⁴ Nye, 'Deterrence and Dissuasion in Cyberspace', 60–62.

⁴⁵ Brandon Valeriano and Benjamin Jensen, 'Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report', *13th International Conference on Cyber Conflict: Going Viral – Proceedings*, NATO Cooperative Cyber Defence Centre of Excellence, 2021, 189–214, <https://ccdcoe.org/uploads/2018/10/Art-01-Achieving-Cyberdeterrence-and-the-Ability-of-Small-States-to-Hold-Large-States-at-Risk.pdf>.

(Note: In this schema, denial is primarily *inward-facing*; while norms, entanglement and punishment are *outward-facing*.)

The case studies that follow assess how Estonia and Singapore have operationalised these mechanisms in practice, and how a layered posture enhances cyber deterrence.

2.7 Summary

This chapter set the theoretical foundation for the thesis by (1) fixing a pragmatic definition of *small states* (population under 10 million) and sketching recurrent behavioural traits; (2) explaining why cyberspace intensifies grey-zone competition; and (3) showing how classical deterrence travels only partially into this domain due to attribution frictions, proportionality dilemmas, and the ubiquity of low-cost attack tools.

In response, the chapter adopted Nye's four mechanisms – punishment, denial, norms and entanglement – as a coherent toolkit for cyber deterrence and argued for a layered posture: inward-facing resilience and rapid recovery (denial) complemented by outward-facing levers (norms, entanglement, and, where credible, punishment). For small states, layering frustrates adversaries' objectives, raises reputational and collateral costs through institutions and partnerships, and communicates resolve without material overreach.

The next chapters apply this framework to Estonia and Singapore, tracing how each state layers mechanisms in line with strategic culture and digital dependence, and drawing comparative lessons for small states seeking to deter grey-zone threats in cyberspace.

Chapter 3: Estonia

3.1 Introduction

Estonia's experience with cyber coercion has become emblematic of how small states can respond to and deter GZ threats in cyberspace. A pioneer in e-governance and digital innovation, Estonia was among the earliest victims of politically motivated cyber operations in 2007, when large-scale attacks targeted its critical networks.⁴⁶ Its response has shaped a distinctive deterrence posture, anchored in technical hardening and population-level digital resilience that offers valuable lessons for small states seeking to defend themselves against hostile cyber activity. This case study examines Estonia's layered approach to cyber deterrence, applying Joseph Nye's framework of punishment, denial, norms, and entanglement to assess its effectiveness in addressing the persistent and evolving threats it faces.

3.2 Background, Strategic Context and Threat Landscape

Following its independence from the Soviet Union in 1991, Estonia rapidly embraced digital transformation as a means to enhance public administration, reduce corruption, and project modernity. Central to this transformation was the development of a comprehensive e-governance ecosystem, including digital ID cards, e-voting, and paperless cabinet meetings, making Estonia one of the most digitised societies in the world by the early 2000s.⁴⁷ In 2004, Estonia joined NATO and the EU, anchoring its security and economic orientation firmly within the Euro-Atlantic community. These political and digital integrations, however, heightened Estonia's visibility and vulnerability in the increasingly contested cyberspace.

In April 2007, Estonia suffered a series of coordinated DDoS attacks targeting government ministries, banks, and media outlets. The attacks, widely attributed to actors linked to Russia, were triggered by a dispute over the relocation of a Soviet-era war memorial in Tallinn. Although the attacks, which lasted over three weeks, caused no physical destruction, they severely disrupted critical services.⁴⁸ More significantly, they exposed the fragility of Estonia's cyber infrastructure and demonstrated how cyberspace could be weaponised to achieve geopolitical goals below the threshold of armed conflict.⁴⁹

⁴⁶ Matthew Crandall and Collin Allan, 'Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms', *Contemporary Security Policy* 36, no. 2 (2015): 351, edscl.2-52.0-84937643444, <https://doi.org/10.1080/13523260.2015.1061765>.

⁴⁷ Victor I. Espinosa and Antonia Pino, 'E-Government as a Development Strategy: The Case of Estonia.', *International Journal of Public Administration* 48, no. 2 (2025): 86–91, 182024438, <https://doi.org/10.1080/01900692.2024.2316128>; Estonian Business and Innovation Agency, 'e-Estonia Story', e-Estonia, accessed 2 August 2025, <https://e-estonia.com/story/>.

⁴⁸ 'Hybrid Threats: 2007 Cyber Attacks on Estonia', NATO Strategic Communications Centre of Excellence, 6 June 2019, <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>.

⁴⁹ Crandall and Allan, 'Small States and Big Ideas', 351.

The incident marked a turning point in Estonia's strategic outlook. Recognising that digital vulnerabilities could be exploited to exert political pressure, Estonia began building a comprehensive national cyber defence posture, integrating technological hardening, institutional preparedness, and international cooperation. The inaugural Cyber Security Strategy, the first of its kind globally, was published in 2008 and laid the foundation for a systematic and forward-looking approach to national cybersecurity.⁵⁰ Over successive updates, Estonia has refined and expanded its efforts, and today boasts one of the most mature and adaptive cybersecurity architectures among small states.⁵¹

Today, regional tensions persist and Estonia continues to face persistent threats – from phishing campaigns and espionage operations to politically motivated disruptions.⁵² That said, since the 2007 cyberattacks, no large-scale cyber incident has significantly impacted its networks – an outcome often viewed in Tallinn as evidence of an effective deterrence posture.⁵³

3.3 Normative Deterrence

The 2007 cyberattack exposed the lack of legal clarity surrounding cyberattacks and their consequences. For Estonia, this vulnerability posed an existential risk to its highly digitised society, prompting the recognition that long-term security would depend on embedding its defence within a predictable, rules-based international order.⁵⁴ In the aftermath, Estonia pursued norm-entrepreneurship to convert legal ambiguity into strategic leverage for a small state: it pre-positions coalitions for faster coordinated response, raises expected reputational costs for visible disruption, and secures agenda-setting influence disproportionate to size.

⁵⁰ Josh Gold, 'Estonia as an international cybersecurity leader', e-Estonia, 21 August 2019, <https://e-estonia.com/estonia-as-an-international-cybersecurity-leader/>; International Institute for Strategic Studies, *Chapter 5: "Estonia" — in Cyber Capabilities and National Power*, Volume 2, IISS Research Paper (International Institute for Strategic Studies, 2023), 30, https://www.iiss.org/globalassets/media-library---content-migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_05-estonia.pdf.

⁵¹ The ITU Global Cybersecurity Index (GCI) is an international benchmark that measures countries' commitment to cybersecurity across legal, technical, organisational, capacity-building, and cooperative dimensions. Since its inception in 2015, Estonia has consistently ranked among the world's top five. In the 2024 edition, the ranking methodology changed, and Estonia was classified in Tier 1 — the highest tier. See: 'Global Cybersecurity Index 2024', International Telecommunication Union (ITU), 1 June 2024, <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>.

⁵² Information System Authority (RIA), *Cyber Security in Estonia 2025* (Republic of Estonia, Information System Authority (RIA), 2025), 8–41, <https://ria.ee/sites/default/files/documents/2025-02/Cyber-security-in-Estonia-2025.pdf>.

⁵³ Information System Authority (RIA), *Cyber Security in Estonia 2023*, 8–12.

⁵⁴ Crandall and Allan, 'Small States and Big Ideas', 351–52.

Strategically, Estonia seeks to shape the *rulebook* because rules shape others' choices. It supported the Tallinn Manual process – an independent academic project hosted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. The project explores how existing principles of international law, such as sovereignty, non-intervention, and the use of force can apply in cyberspace. Although non-binding, the Tallinn Manual has been widely cited in international legal and policy discourse, providing reference points for states and organisations responding to GZ cyberattacks.⁵⁵ Anchoring the project at CCDCOE places Estonia at the centre of doctrinal debate and gives allies a shared interpretive baseline – lowering coordination costs when responses are considered and increasing the plausibility of collective action.⁵⁶

Estonia pursues normative activism multilaterally to translate legal argument into political practice, creating a shared understanding of rules, thresholds, and consequences in cyberspace. At the UN level, Estonia has participated actively in the GGE and OEWG processes to embed the view that existing international law applies online.⁵⁷ In June 2021, while serving as the UNSC's rotating president, Estonia chaired the first-ever formal UNSC open debate on cybersecurity, socialising major powers to the applicability of International Humanitarian Law (IHL) in cyberspace and expectations of responsible-state behaviour.⁵⁸ At the EU level, Estonia helped to develop the Cyber Diplomacy Toolbox in 2017, institutionalising a framework for coordinated responses to

⁵⁵ Tallinn Manual and Tallinn Manual 2.0 were published in 2013 and 2017 respectively. Works for Tallinn Manual 3.0 is ongoing. See: International Institute for Strategic Studies, *Chapter 5: "Estonia" — in Cyber Capabilities and National Power*, 37.

⁵⁶ Josh Gold, 'How Estonia Uses Cybersecurity to Strengthen Its Position in NATO', *ICDS*, 27 May 2019, <https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/>.

⁵⁷ GGE is shorthand for Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and OEWG is shorthand for Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Estonia joined selected countries the UN GGE in 2009 and helped to shape international norms and principles for responsible state behaviour in cyberspace. The UN GGE last met in 2021. Thereafter, the UN shifted its primary forum for discussing cybersecurity to the OEWG which involved all UN member states. See: 'Developments in the Field of Information and Telecommunications in the Context of International Security', United Nations Office for Disarmament Affairs (UNODA), accessed 8 August 2025, <https://disarmament.unoda.org/ict-security/>; 'Open-Ended Working Group on Information and Communication Technologies (2021)', UN Office for Disarmament Affairs (UNODA), accessed 8 August 2025, <https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021>.

⁵⁸ Estonia was elected and took on the role of a non-permanent member of the UNSC from 1 January 2020 to 31 December 2021. See: Government Communication Unit, 'Estonia Hosted the First-Ever Formal Meeting on Cybersecurity in the History of the UN Security Council', Republic of Estonia - Government (Valitsus), 29 June 2021, <https://www.valitsus.ee/en/news/estonia-hosted-first-ever-formal-meeting-cybersecurity-history-un-security-council>.

malicious cyber activity.⁵⁹ Estonia has also been active in pushing for a coherent EU cyber diplomacy posture – to treat cyber stability as a foreign policy priority.⁶⁰

The shared understanding of norms enables public attribution – a mechanism that imposes diplomatic and reputational costs on offenders and creates focal points for coordinated response. In turn, Estonia uses public attribution as a norm-building tool, socialising expectations and clarifying thresholds — signalling that irresponsible cyber behaviour will be publicly identified and censured.⁶¹ Estonia employs attribution on a spectrum, ranging from cautious references to “pro-actors (e.g., pro-Russian groups)” to explicit identification of responsible states or entities. It also engages in collective attribution to amplify the normative signals while sharing political risks. For instance, in 2018, Estonia joined the U.K., U.S., and Australia in attributing the *NotPetya* cyberattacks to Russian state-linked actors.⁶² In 2019, Estonia established its public attribution guidelines,⁶³ and in 2024, made its first unilateral public attribution, naming Russia’s GRU for the 2020 cyber espionage campaign targeting Estonian ministries.⁶⁴

Net effect: shared norms enable public attribution and coordinated signalling that raise reputational costs and reduce the friction of collective responses. The limits of norms are clear: norms are non-binding and consensus-dependent; major-power convergence

⁵⁹ ‘Cybersecurity Cooperation – Regional Activities’, Republic of Estonia - Ministry of Foreign Affairs (Välisministeerium), accessed 7 August 2025, <https://vm.ee/en/activity/digital-and-cyber-diplomacy/cybersecurity-cooperation>.

⁶⁰ Xinchuchu Gao, ‘Challenges and Opportunities: Estonia’s Role in Shaping EU Cybersecurity Policy’, in *Small States in EU Policy-Making*, 1st edn, by Anna-Lena Högenauer and Matúš Mišík (Routledge, 2024), 169, <https://doi.org/10.4324/9781003380641-12>; Council of the European Union (General Secretariat), ‘Council Conclusions on the Development of the European Union’s Cyber Posture’, Council of the European Union, 23 May 2022, 12–14, <https://www.consilium.europa.eu/media/56358/st09364-en22.pdf>.

⁶¹ Pernik, *Cyber Deterrence*, 16.

⁶² Marietje SCHAAKE, ‘Question for Written Answer E-001005/2018 to the Council: “Attribution of the NotPetya Attack”’, European Parliament, 19 February 2018, https://www.europarl.europa.eu/doceo/document/E-8-2018-001005_EN.html; Sandra Kamilova, ‘Foreign Minister Mikser Condemns Russia for NotPetya Attacks against Ukraine’, Välisministeerium, 15 February 2018, <https://vm.ee/en/news/foreign-minister-mikser-condemns-notpetya-attacks-against-ukraine>.

⁶³ Information System Authority (RIA), *Cyber Security in Estonia 2020* (Republic of Estonia, Information System Authority (RIA), 2020), 23–24, <https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2020.pdf>.

⁶⁴ GRU is shorthand for Glavnoye Razvedyvatelnoye Upravlenie – the Foreign military intelligence agency of Russia’s General Staff. The public attribution was made possible by supporting evidence from U.S. and other partners. See: Public Relations Department, ‘Estonia Names Russia’s Military Intelligence in a First-Ever Attribution of Cyberattacks’, Republic of Estonia, Ministry of Foreign Affairs (Välisministeerium), 5 September 2024, <https://vm.ee/en/news/estonia-names-russias-military-intelligence-first-ever-attribution-cyberattacks>; Stefan Soesanto, ‘Inside the Fourth EU Cyber Sanctions Package’, Lawfare, 23 March 2025, <https://www.lawfaremedia.org/article/inside-the-fourth-eu-cyber-sanctions-package>.

on the applicability of IHL in cyberspace remains contested;⁶⁵ and naming-and-shaming exerts little leverage, especially over reputation-insensitive states (e.g., North Korea).⁶⁶ Hence, Estonia treats norms as a force-multiplier that is most effective when layered with denial (to blunt operational gains) and entanglement (to raise political risk). In 3Cs terms, norms contribute communication and credibility by socialising expectations and enabling coalition signalling.

3.4 Deterrence by Entanglement

Estonia's most consequential entanglement is politico-security. This is manifested in its membership in NATO and EU. As a member of NATO and the EU, Estonia is embedded within their decision frameworks, and this raises the expected costs and risks of coercive cyber operations: an attacker must consider not only Estonia's response but also how the collective entities will react. With NATO, under Article 5 of the North Atlantic Treaty, a cyberattack judged to be sufficiently grave could trigger collective defence response from the Alliance.⁶⁷ With the EU, the Cyber Diplomacy Toolbox binds members into coordinated signalling and potential sanctions for cyberattacks.⁶⁸ This kind of entanglement differs from economic or technical interdependence, which Estonia has only in limited ways. Its deterrent value lies in the political reality that Estonia's networks, institutions, and infrastructure are not defended in isolation but are bound into the wider NATO and EU frameworks.

Net effect: entanglement raises baseline political risk for attackers by binding Estonia into NATO/EU decision frameworks. Two caveats temper the effect: first, collective-action thresholds are politically constructed and responses are subject to intra-alliance/intra-union bargaining;⁶⁹ second, cyber escalation ladders, if they exist, are opaque and

⁶⁵ Ann Väljataga, 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly', NATO Cooperative Cyber Defence Centre of Excellence, accessed 2 September 2025, <https://ccdcoe.org/incyber-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/>.

⁶⁶ Fergus Hanson, 'Naming and Shaming the Unshameable', *The Strategist*, 17 April 2018, <https://www.aspistrategist.org.au/naming-shaming-unshameable/>; Tan, 'A Small State Perspective on the Evolving Nature of Cyber Conflict', 162.

⁶⁷ Article 5 of the North Atlantic Treaty enshrines the principle of collective defence: an armed attack against one Ally is considered an attack against all, obligating members to assist the attacked party, including the potential use of armed force. The Brussels Summit communiqué of 14 June 2021 affirmed that cyberattacks of significant consequence could trigger Article 5. See: NATO, 'Collective Defence and Article 5', NATO, 4 July 2023, https://www.nato.int/cps/en/natohq/topics_110496.htm; NATO, 'Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021', North Atlantic Treaty Organization (NATO), 14 June 2021, para. 32, https://www.nato.int/cps/en/natohq/news_185000.htm.

⁶⁸ Republic of Estonia - Ministry of Foreign Affairs (Välisministeerium), 'Cybersecurity Cooperation – Regional Activities'.

⁶⁹ Eric S. Edelman et al., 'NATO's Decision Process Has an Achilles' Heel', *Atlantic Council*, 12 March 2024, <https://www.atlanticcouncil.org/blogs/new-atlanticist/natos-decision-process-has-an-achilles-heel/>; 'The EU Sanctions Process Explained',

adversaries may probe below perceived thresholds. Taken together, entanglement is best understood as a credible backstop and uncertainty multiplier, most potent when paired with rapid attribution and a resilient defence, and when communicated in advance. In 3Cs terms, entanglement primarily bolsters credibility *ex ante* by raising perceived coalition risks.

3.5 Deterrence by Denial

Denial is Estonia's most dependable pillar because it reduces the expected payoff of attacks regardless of attribution. It works by compressing attacker dwell time, compartmentalising failure, and assuring continuity of critical functions across technology, institutions, and society.⁷⁰

Technically, Estonia engineers continuity into state functions. Its Cybersecurity Act obliges Critical Information Infrastructure (CII) operators to meet baseline security requirements. Its digital system architecture is designed to minimise single points of failure and to allow the isolation of compromised nodes without paralysing national functions.⁷¹ “Data embassies” provide sovereign, off-site replicas of critical government databases hosted in foreign countries.⁷²



Image: Cyber Command - Estonian Defence Forces

Institutionally, Estonian institutions translate design into operational effect. The Information System Authority (RIA) leads national cyber strategy implementation, provides guidance across both public and private sectors, and organises exercises to

rehearse cross-sector cyber crisis management.⁷³ Its operational arm, CERT-EE, is responsible for detecting, analysing, and responding to cyberattacks targeting

Council of the European Union, accessed 7 September 2025, <https://www.consilium.europa.eu/en/infographics/the-eu-sanctions-process-explained/>.

⁷⁰ Nye, ‘Deterrence and Dissuasion in Cyberspace’, sect. Denial.

⁷¹ Harvard Ash Center, ‘E-Stonia: One Small Country’s Digital Government Is Having a Big Impact’, *Innovations in Government*, 15 April 2021, <https://medium.com/innovations-in-government/e-stonia-one-small-countrys-digital-government-is-having-a-big-impact-a33e30983c0b>; Estonian Business and Innovation Agency, ‘X-Road’, e-Estonia, 10 June 2024, <https://e-estonia.com/solutions/interoperability-services/x-road/>.

⁷² The agreement between Estonia and Luxembourg for the world’s first data embassy was signed in 2017. See: Estonian Business and Innovation Agency, ‘Data Embassy’, e-Estonia, 7 June 2024, <https://e-estonia.com/solutions/e-governance/data-embassy/>.

⁷³ Republic of Estonia, Information System Authority (RIA), *Cybersecurity Strategy 2024–2030: Cyber-Conscious Estonia* (Republic of Estonia, Information System Authority (RIA), 2024), 33–34, https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf; ‘Tasks and Structure of the Authority’, Republic of Estonia, Information System Authority (RIA), accessed 5 August 2025, <https://www.ria.ee/en/authority-news-and-contact/authority-and-management/tasks-and-structure-authority>.

government networks and critical infrastructure.⁷⁴ The military networks are protected by the Estonian Defence Forces' (EDF's) Cyber Command, which also works with public- and private-sector partners in Estonia to strengthen inter-agency coordination and operational readiness.⁷⁵

Societally, a whole-of-society approach increases capacity and reduces cognitive attack surfaces. Estonia treats every citizen, organisation, and sector as a contributor to national security.⁷⁶ It invests in population-level resilience: digital competence and cyber hygiene are embedded from school curricula through to adult learning.⁷⁷ The RIA issues public advisories, runs national awareness campaigns, and offers free cyber hygiene courses, and public-sector organisations conduct regular staff awareness training and exercises.⁷⁸ This broad-based literacy shrinks the attack surface for phishing and social engineering, raises baseline security, and shortens detection-to-reporting timelines during incidents.⁷⁹

Estonia's whole-of-society approach also includes the Cyber Defence Unit (CDU) – the cyber-arm of the Estonian Defence League – a volunteer reserve. Comprising cybersecurity professionals and individuals with expertise in information security from the private and public sectors,⁸⁰ the CDU contributes technical expertise for threat analysis, supports awareness through training and exercises, and provides surge support to state authorities during major incidents.⁸¹ This mobilises private-sector talent,

⁷⁴ CERT-EE is shorthand for Computer Emergency Response Team – Estonia. See: Information System Authority (RIA), 'Monitoring Cyberspace and Impeding Incidents', Republic of Estonia, Information System Authority (RIA), accessed 5 August 2025, <https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee>.

⁷⁵ Information System Authority (RIA), *Cyber Security in Estonia 2020*, 34–35.

⁷⁶ Government of the Republic of Estonia, 'National Security Concept of Estonia', February 2023, https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf.

⁷⁷ Information System Authority (RIA), 'Prevention Efforts for All Generations', Information System Authority (RIA), accessed 24 August 2025, <https://www.ria.ee/en/prevention-efforts-all-generations>; Petra Holm, 'Estonia's approach to cyber security: a model for Europe', e-Estonia, 19 March 2025, <https://e-estonia.com/estonias-cyber-security-model-for-europe/>.

⁷⁸ On the RIA website, cybersecurity reports are published daily, monthly, quarterly and annually. The annual reports capture key community outreach programmes, watch areas for safer cyberspace and how the general public can contribute to a safer cyberspace. See: Information System Authority (RIA), *Cyber Security in Estonia 2020*, 40; 'Situation in the Cyberspace', Republic of Estonia, Information System Authority (RIA), accessed 7 August 2025, <https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/situation-cyberspace>.

⁷⁹ Lionel Oh, 'Exploring Policy Conditions for Cyber Deterrence: A Case Study of Estonia', *The Cornell International Affairs Review* XII, no. 2 (2019): 141–42.

⁸⁰ The Estonia Defence League is a voluntary, paramilitary organisation that operates under the Ministry of Defence. See: 'Estonian Defence Forces', Estonian Defence Forces, 30 July 2025, <https://mil.ee/en/defence-forces/>.

⁸¹ The Cyber Defence Unit is sometimes referred to as Cyber Unit or Cyber Defence League. For information on the league and the CDU, see: 'Frequently Asked Questions - Cyber Unit', Estonian Defence League, accessed 5 August 2025, <https://www.kaitseliit.ee/en/frequently-asked-questions>; Republic of Estonia, Information System Authority (RIA), *Cybersecurity Strategy 2024–2030*, 35; Sharon L. Cardash et al., 'Estonia's Cyber Defence League: A Model for the United States?',

shortens response timelines, and raises the perceived probability of rapid remediation.

Collectively, these choices function as strong deterrent signalling: they lower the attacker's expected gains, increase operational costs, and curtail windows of advantage.

Internationally, collaboration deepens defensive depth and increases discovery risk for adversaries. As host of the NATO CCDCOE, Estonia contributes to NATO's cyber doctrine development, capability building, and strategic coordination.⁸² It hosts and participates in major cyber exercises such as *Locked Shields* and *Cyber Coalition*. These exercises simulate complex cyberattack scenarios, test incident response capabilities, build trust among participating states, and foster interoperability across national systems and international partners.⁸³ In 2020, the Cyber Command also conducted joint operations with the US Cyber National Mission Force to perform threat hunting on EDF's networks.⁸⁴ Estonia's participation in multinational cyber threat intelligence-sharing networks further enhances early warning capacity and defensive depth beyond national borders. For adversaries, this raises the likelihood of prompt detection and multi-vector countermeasures.

Net effect: denial supplies capability, exercises establish credibility, and transparent messaging completes the loop; together they make cyberattacks low-payoff and short-lived. That said, two limits matter: first, high-end attacks such as APT-class intrusions can still succeed – denial constrains effects rather than eliminates them;⁸⁵ second, resilience must be visible – measured, exercised, and communicated – to shape adversary expectations. Estonia addresses these by investing in layered safeguards and publicising standards, drills, and after-action learning to demonstrate recoverability. In 3Cs terms, denial provides *capability* and demonstrated *credibility*, while transparent public messaging supplies *communication*.

3.6 Deterrence by Punishment

In Estonia's model, punishment functions as an amplifier: it converts attribution into legal and coalitional instruments that raise cumulative costs and strengthen the credibility of

Studies in Conflict & Terrorism 36, no. 9 (2013): 778–80, 89890772, <https://doi.org/10.1080/1057610X.2013.813273>.

⁸² 'About Us', NATO Cooperative Cyber Defence Centre of Excellence, accessed 6 August 2025, <https://ccdcoe.org/about-us/>.

⁸³ 'Locked Shields', NATO Cooperative Cyber Defence Centre of Excellence, accessed 6 August 2025, <https://ccdcoe.org/exercises/locked-shields/>; 'Exercise Cyber Coalition 2020', Supreme Headquarters Allied Powers Europe (SHAPE), 14 November 2020, <https://shape.nato.int/news-archive/2020/exercise-cyber-coalition-2020.aspx>.

⁸⁴ 'Hunt Forward Estonia: Estonia, US Strengthen Partnership in Cyber Domain with Joint Operation', U.S. Cyber Command, 3 December 2020, <https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/>.

⁸⁵ APTs are well-resourced, human-directed intrusion teams that infiltrate networks quietly and over long periods to steal data, position for disruption, or gain strategic advantage. See: Kurt Baker, 'What Is an Advanced Persistent Threat (APT)?', CrowdStrike, 4 March 2025, <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/>.

the broader deterrence posture. As a small state, Estonia has limited ability to impose direct economic or military costs on adversaries. While Estonia is assessed to possess offensive cyber capabilities, little is publicly disclosed and these are assessed to be limited.⁸⁶ Accordingly, punishment is modest in means and targeted in effect. In practice, this takes three main forms: coordinated sanctions with the EU, unilateral legal actions, and the prosecution of cybercrime.

The EU sanctions regime is central here: by aligning on joint attributions for major incidents, Estonia helped move the Union from statements to designations. For example, in the 2020 collective attribution of WannaCry, NotPetya, Operation Cloud Hopper, and the attempted cyberattack on the Organisation for the Prohibition of Chemical Weapons to state-linked actors in North Korea, China, and Russia, the EU imposed travel bans and asset freezes on six individuals and three entities responsible for or facilitating these operations.⁸⁷ For a small state, this converts normative success into punitive scale: while Estonia cannot meaningfully sanction a major adversary alone, the EU market – the world's second-largest – can.⁸⁸

National measures fill gaps where collective action is slow or politically constrained. In September 2024, Estonia undertook unilateral attribution of a Russian GRU operation and issued international arrest warrants for three suspected GRU officers for the 2020 cyber espionage campaign against its ministries.⁸⁹ While the material impact of such measures is limited – targets may not travel to jurisdictions where enforcement is feasible – the legal and reputational costs are real, constraining mobility and signalling that state-sponsored operators are not invisible. Domestic criminal law and cooperation with other law-enforcement agencies, such as Europol, further enable investigations and prosecutions against non-state or proxy actors, where criminal justice can be more immediate than geopolitics.⁹⁰ Granted, many perpetrators may remain beyond the reach of Estonian jurisdiction, yet its willingness to pursue cross-border legal action increases the risks for those who might otherwise act with impunity.

⁸⁶ International Institute for Strategic Studies, *Chapter 5: "Estonia" — in Cyber Capabilities and National Power*, 38.

⁸⁷ This was the EU's first ever sanctions against cyberattack. The shift from '*naming and shaming*' to punitive actions was also enabled by the adoption of the Cyber Diplomacy Toolbox in 2017. See: 'EU Imposes the First Ever Sanctions against Cyber-Attacks', European External Action Service (EEAS), 30 July 2020, https://www.eeas.europa.eu/delegations/china/eu-imposes-first-ever-sanctions-against-cyber-attacks_en?s=166; Sasha Erskine, 'The EU Tiptoes into Cyber Sanctions Regimes', Royal United Services Institute (RUSI), 12 August 2025, <https://www.rusi.orghttps://www.rusi.org>.

⁸⁸ In 2024, the three largest economies in the world are United States, European Union and China. See: 'World Economic Outlook (April 2025) - GDP, Current Prices', International Monetary Fund, accessed 13 August 2025, <https://www.imf.org/external/datamapper/NGDPD@WEO/USA/CHN/EU>.

⁸⁹ Public Relations Department, 'Estonia Names Russia's Military Intelligence in a First-Ever Attribution of Cyberattacks'.

⁹⁰ See §206, 207, 213, 217, and §216¹ in: 'Penal Code', Riigi Teataja, accessed 24 August 2025, <https://www.riigiteataja.ee/en/eli/522012015002/consolidate>; ERR News, 'Police Apprehend Suspects in Cyberattacks against Estonia', ERR News, 29 September 2020, <https://news.err.ee/1140977/police-apprehend-suspects-in-cyberattacks-against-estonia>.

These actions demonstrate Estonia's resolve to impose consequences for hostile activity and provide a bridge until coalition responses can be mobilised. Indeed, in January 2025, almost five months after Estonia's unilateral attribution and issuance of arrest warrants, the Council of the EU added three GRU officers to its cyber-sanctions list,⁹¹ illustrating that collective measures may arrive after a lag because consensus-building and legal designation procedures take time.

Net effect: punishment adds cumulative costs, raises operational security burdens, and publicly reinforces attribution credibility. That said, trade-offs remain: first, overuse of symbolic designations can dull impact; second, slow EU consensus can create response-time asymmetries that adversaries exploit;⁹² and third, unilateral actions carry diplomatic risk.⁹³ Estonia mitigates these by nesting punishment within a layered approach: deny benefits first, frame violations normatively, entangle politically, and punish where feasible – preferably with allies. In 3Cs terms, punishment contributes credibility and communication when capability is thin.

3.7 Assessment – Effectiveness of Cyber Deterrence

Applying the behavioural benchmark set out in Chapter 2 – Section 2.6, Estonia's layered cyber deterrence posture is assessed on whether it has (1) dissuaded large-scale, destructive, or politically decisive cyber operations and (2) reduced routine hostile activity to marginal returns, recognising that a zero-incident standard is neither realistic nor informative in a GZ environment with contested attribution.

Where Deterrence Worked

Since the 2007 DDoS campaign, Estonia has not suffered a system-wide disruption of comparable scale. Repeated waves of politically motivated activity have been contained at the tactical level and have not produced strategic effects. In 2022, for instance, pro-Russian hacktivists mounted intense DDoS campaigns; services were interrupted in places but restored swiftly, and officials noted that impacts were “mostly not even noticed by the average user.”⁹⁴ The campaign lasted only a few days – suggesting that the attackers may have curtailed their efforts once it became clear that their objectives could not be achieved. A subsequent campaign in 2024, described as the “largest cyberattack to date” was similarly reported to “have no visible impact” beyond brief

⁹¹ ‘Cyber-Attacks: Three Individuals Added to EU Sanctions List for Malicious Cyber Activities against Estonia’, Council of the European Union, 27 January 2025, <https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia/>.

⁹² Annegret Bendiek and Matthias Schulze, ‘Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW’, *SWP Research Paper*, Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, 2021, 7–9, <https://doi.org/10.18449/2021RP11>.

⁹³ Torbjørn Pedersen, ‘A Small State's Cyber Posture: Deterrence by Punishment and Beyond’, *Scandinavian Journal of Military Studies* 6, no. 1 (2023): 64, <https://doi.org/10.31374/sjms.191>.

⁹⁴ Information System Authority (RIA), *Cyber Security in Estonia 2023*, 10.

disruptions.⁹⁵ The inability of these operations to coerce policy change or erode public confidence points to the strength of Estonia's denial posture: layered resilience, broad public cyber hygiene, rehearsed incident management, and rapid recovery have raised the cost and lowered the payoff of disruptive cyber activity.

Normative and entanglement mechanisms have reinforced these outcomes rather than substituting for denial. Estonia's sustained norm entrepreneurship has helped consolidate shared expectations about responsible behaviour in cyberspace and increased reputational costs for violators. Concurrently, alliance entanglement – above all NATO's political-security umbrella – adds uncertainty for aggressors about potential collective consequences should a cyber incident escalate. Even without Article 5 being invoked for cyber, the possibility of alliance involvement acts as a brake on more ambitious operations.

Where Deterrence Remains Limited

Estonia continues to face persistent lower-level intrusions – espionage, phishing, ransomware, and harassment – reflecting the challenge of deterring GZ tactics that sit below collective-response thresholds. The 2020 espionage campaign, which Estonia attributed in 2024 to Russia's GRU, indicates that sophisticated actors can still penetrate networks.⁹⁶ While Estonia responded with arrest warrants and legal measures, such actions carry primarily reputational and legal risks for perpetrators; their coercive bite is modest.

Punishment, moreover, is structurally constrained for a small state. EU cyber sanctions provide scale and credibility but are consensus-driven and often slow.⁹⁷ The almost five-month gap between Estonia's September 2024 unilateral attribution and the Council of the EU's January 2025 listings of three GRU officers for malicious cyber activities against Estonia in 2020 further illustrates this.⁹⁸ This time lag limits the immediacy of punishment's effect, even as eventual listings add cumulative costs.

Summary

In sum, Estonia's cyber deterrence strategy has constrained adversaries rather than eliminated hostile activity. It has worked in the sense that despite persistent coercive disruption activities, they have failed to achieve strategic outcomes and that the expected returns on large-scale operations against Estonia appear diminished and short-lived. The most reliable pillar is denial – a deliberately cultivated resilience that turns attacks into tactical nuisances. Norms amplify this by shaping expectations and imposing reputational costs, while entanglement provides a credible backstop that

⁹⁵ ERR News, 'RIA: Estonia's State Institutions Hit by Largest Cyberattack to Date', ERR, 12 March 2024, <https://news.err.ee/1609278921/ria-estonia-s-state-institutions-hit-by-largest-cyberattack-to-date>.

⁹⁶ Public Relations Department, 'Estonia Names Russia's Military Intelligence in a First-Ever Attribution of Cyberattacks'.

⁹⁷ Bendiek and Schulze, 'Attribution', 7–9.

⁹⁸ Council of the European Union, 'Cyber-Attacks'; Council of the European Union, 'Cyber-Attacks'.

complicates adversaries' risk calculus. Punishment contributes but remains the least decisive tool given scale limitations and multilateral politics.

Looking ahead, Chapter 4 will apply the same framework to Singapore to assess its deterrence posture.

Chapter 4: Singapore

4.1 Introduction

As one of the world's most digitally competitive countries,⁹⁹ Singapore's experience with persistent cyberattacks underscores the challenges faced by small, highly connected states in safeguarding national security. As a global hub in several respects,¹⁰⁰ Singapore's CII supports essential services ranging from finance and energy to healthcare and transport,¹⁰¹ making it a high-value target for both state-linked and criminal actors.¹⁰² While no single incident has triggered a wholesale strategic shift, incidents and targeted campaigns over the years – such as the 2018 SingHealth data breach affecting 1.5 million citizens – have reinforced the view that GZ cyberattacks are a constant feature of Singapore's security landscape.¹⁰³ These incidents are assessed not simply as technical disruptions but as potential enablers of strategic coercion, capable of eroding public trust and undermining the functioning of the state.

This case study examines Singapore's approach to cyber deterrence, applying Joseph Nye's framework of punishment, denial, norms, and entanglement to assess its effectiveness in reducing the strategic utility of hostile cyber activity.

4.2 Background, Strategic Context and Threat Landscape

Singapore has long pursued an ambitious national digitisation agenda, beginning with the National Computerisation Plan in 1980 and advancing through successive national IT masterplans. This sustained transformation has deeply embedded technology across government, economy, and society, making the city-state one of the most digitally integrated economies in the world.¹⁰⁴ Against this backdrop, Singapore's economic

⁹⁹ *IMD World Digital Competitiveness Ranking 2024* (Institute for Management Development, 2024), 60, <https://imd.widen.net/s/xvhldkrrkw/20241111-wcc-digital-report-2024-wip>.

¹⁰⁰ 'Singapore Boosts Maritime, Aviation Hub Role as Cargo Flows Shift and Supply Chain Risks Rise', Economic Development Board (EDB) Singapore, 20 December 2024, <https://www.edb.gov.sg/en/business-insights/insights/singapore-boosts-maritime-aviation-hub-role-as-cargo-flows-shift-and-supply-chain-risks-rise.html>.

¹⁰¹ CII are defined from 11 critical sectors – Aviation, Banking & Finance, Energy, Government, Healthcare, Infocomm, Land Transport, Maritime, Media, Security & Emergency Services, and Water. See: Cyber Security Agency (CSA), *Singapore Cybersecurity Strategy 2021* (Cyber Security Agency of Singapore, 2021), 17, <https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf>; Shanmugam, 'Opening Speech by Mr K Shanmugam, Coordinating Minister for National Security and Minister for Home Affairs, at CSA's 10th Anniversary Dinner', sect. Annex 1.

¹⁰² Shanmugam, 'Opening Speech by Mr K Shanmugam, Coordinating Minister for National Security and Minister for Home Affairs, at CSA's 10th Anniversary Dinner'.

¹⁰³ Sashi Jayakumar, 'Commentary: Singapore Is Going from Cybersecurity to Cybermaturity', Channel News Asia, 5 June 2025, <https://www.channelnewsasia.com/commentary/cybersecurity-attack-scam-ransomware-hackers-ai-5165536>.

¹⁰⁴ 'Singapore Ranks as World's 12th Tech City, with Room to Grow as Tech-Savvy Generation Enter Job Market', Economic Development Board (EDB) Singapore, 24

profile and geographic position amplify its exposure to cyberattacks.¹⁰⁵ As a global hub for trade, finance, logistics, and advanced manufacturing, the city-state's critical systems are deeply integrated with digital technologies. It is also a regional data centre hub, supporting the storage and processing of vast amounts of commercial and cross-border data.¹⁰⁶ The government's Smart Nation agenda has accelerated the digitalisation of governance, public services, and everyday life, enhancing efficiencies but also expanding potential vulnerabilities.¹⁰⁷

Over the past decade, several high-profile incidents have highlighted the vulnerabilities of Singapore's digital domain. These include the 2014 cyberattack on the Ministry of Foreign Affairs and the 2018 SingHealth breach.¹⁰⁸ More recently, in July 2025, the government raised the alarm over APTs mounting covert campaigns against government systems and CII, with objectives that include espionage, theft of sensitive information, and potential disruption of essential services.¹⁰⁹ Alongside these higher-end threats, Singapore-based organisations were also subject to ransomware, social engineering scams, and cloud misconfiguration exploits. In 2023, more than eight in ten organisations reported at least one cybersecurity incident, with most incidents resulting in operational disruption, reputational harm, or data loss.¹¹⁰

Regionally, Singapore operates in a competitive and evolving security environment shaped by several dynamics. The intensifying technological competition between the United States and China extends into cyberspace. Within ASEAN, cyber capabilities remain uneven, with some members possessing advanced defences while others lag

October 2022, <https://www.edb.gov.sg/en/business-insights/insights/singapore-ranks-as-world-s-12th-tech-city-with-room-to-grow-as-tech-savvy-generation-enter-job-market.html>.

¹⁰⁵ Louise Marie Hurel, 'What Singapore's First Public Cyber Attribution Tells Us', Royal United Services Institute (RUSI), 30 July 2025, <https://www.rusi.org/explore-our-research/publications/commentary/what-singapores-first-public-cyber-attribution-tells-us>.

¹⁰⁶ 'Charting Green Growth for Data Centres in SG', Infocomm Media Development Authority, 30 May 2024, <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/charting-green-growth-for-data-centres-in-sg>.

¹⁰⁷ Singapore Ministry of Digital Development and Information, *Smart Nation 2.0 - A Thriving Digital Future for All* (MDDI, 2024), 4–9, <https://file.go.gov.sg/smartnation2-report.pdf>.

¹⁰⁸ Jayakumar, 'Commentary'.

¹⁰⁹ Sarah Koh, 'Suspected Advanced Persistent Threat Attacks Must Be Reported under S'pore's Amended Cybersecurity Act', *The Straits Times* (Singapore), 29 July 2025, <https://www.straitstimes.com/tech/suspected-advanced-attacks-must-be-reported-under-singapores-amended-cybersecurity-act>.

¹¹⁰ Cyber Security Agency (CSA), 'CSA Releases Key Findings from Singapore Cybersecurity Health Report 2023', Cyber Security Agency of Singapore, 28 March 2024, <https://www.csa.gov.sg/news-events/press-releases/csa-releases-key-findings-from-singapore-cybersecurity-health-report-2023/>; Cyber Security Agency (CSA), 'Singapore Cybersecurity Health Report', Cyber Security Agency of Singapore, 2024, <https://isomer-user-content.by.gov.sg/36/1051bace-6be7-4c59-934a-e43c952a32ed/csa-singapore-cybersecurity-health-report-2023.pdf>.

behind, creating vulnerabilities for collective resilience.¹¹¹ At the same time, cyber tools are increasingly used as instruments of interstate competition — for espionage, political influence, or disruption — adding volatility to the regional security landscape.¹¹² As a highly connected economy dependent on secure trade flows, cross-border data transfers, and international investment, Singapore has strong incentives to maintain a stable and rules-based digital environment.

4.3 Normative Deterrence

As a small state with limited capacity to unilaterally shape the strategic environment, Singapore treats norms as strategic leverage grounded in diplomacy. It operationalises this by leading UN rule-making, translating and socialising norms in ASEAN, and issuing calibrated public statements that cue coordinated responses to violations.

Internationally, Singapore exercises procedural leadership by shaping agendas and outcomes in UN processes. As chair of the 6th UN GGE, it brokered consensus reaffirming the applicability of international law in cyberspace and the 11 voluntary norms of responsible state behaviour.¹¹³ Leading the 2nd OEWG,¹¹⁴ it advanced confidence- and capacity-building measures and secured agreement to establish the *Global Mechanism* – a permanent UN forum for rules-based dialogue on state behaviour in cyberspace – setting the stage for future normative development by all UN members.¹¹⁵ These roles embed Singapore as a rules broker with recognised

¹¹¹ Julia Brock, 'ASEAN's Cyber Initiatives: A Select List', Centre for Strategic Studies & International Studies (CSIS), 16 July 2024, <https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list>.

¹¹² Callistus Francis Azubuike, 'Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks', *Nnamdi Azikiwe Journal of Political Science* 8, no. 3 (2023): sect. Introduction.

¹¹³ The norms were first established in the 4th UN GGE. However, the 5th UN GGE failed to reach consensus due to divisions over the application of international humanitarian law in cyberspace, undermining the UN's progress toward a common normative framework. With this backdrop the reaffirmation of voluntary norms and consensus at the 6th GGE's consensus was particularly significant. See: United Nations Secretariat, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/50 (United Nations, 2021), 26, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf; Våljataga, 'Back to Square One?'

¹¹⁴ Following the conclusion of the 6th UN GGE in 2021, the UN shifted discussions on responsible state behaviour in cyberspace to the OEWG which involved all UN member. See: United Nations Office for Disarmament Affairs (UNODA), 'UN GGE'.

¹¹⁵ Global Mechanism is shorthand for "Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs." Unlike the GGEs and OEWGs, which are ad hoc and mandate-limited processes, the Global Mechanism is intended as a standing institutional forum under the UN, providing continuity and inclusivity in discussions on responsible state behaviour in cyberspace. See: United Nations Secretariat, *Compendium of Statements in Explanation of Position on the Adoption of the Final Report of the Open-Ended Working Group*, A/80/257 (United Nations, 2025), <https://docs.un.org/en/A/AC.292/2025/INF/5>; Pavlina Pavlova and Christopher Painter, 'The UN's Permanent Process on Cybersecurity Faces an Uphill Battle', *Lawfare*,

legitimacy, furnishing both a vocabulary and a venue for collective signalling when norms are breached.

Regionally, Singapore converts principle into practice. Through the ASEAN Ministerial Conference on Cybersecurity, it championed the implementation of the 2015 UN GGE-established voluntary norms of responsible state behaviour and the accompanying confidence-building measures (CBMs).¹¹⁶ With Malaysia, it co-developed the ASEAN Norms Implementation Checklist, mapping concrete steps across policy, legal, operational, technical, and diplomatic pillars, and prioritising CBMs such as designated points-of-contact networks, shared incident taxonomies and reporting templates, crisis-communication protocols, voluntary transparency on national policies, and regular joint exercises. Through the ASEAN-Singapore Cybersecurity Centre of Excellence and the ASEAN Regional CERT, Singapore hosts regional training and capacity-building programmes, including ASEAN CERT Incident Drills, and provides a dedicated venue for in-person cyber exercises, workshops, and CERT-to-CERT cooperation that rehearse these CBMs in practice. These initiatives facilitate timely information-sharing and coordination among ASEAN Member States and align regional practice with evolving international expectations.¹¹⁷ More importantly, they socialise ASEAN members into shared expectations of acceptable behaviour, raising the reputational costs of violation and thereby discouraging norm-breaking.

Calibrated public statements against coercive GZ cyberattacks complement this diplomacy. Historically, Singapore has condemned behaviours rather than naming perpetrators. Even after the 2018 SingHealth breach affecting 1.5 million citizens, official statements only highlighted that it was “a deliberate, targeted and well-planned cyberattack... not the work of casual hackers or criminal gangs, “implying state sponsorship.”¹¹⁸ In July 2025, Singapore raised the bar by issuing its first public attribution, naming the APT group UNC3886 as responsible for a sophisticated campaign targeting Singapore’s CII.¹¹⁹ Although no state was identified, the move narrowed plausible deniability, cued partners and platform mitigations,¹²⁰ and signalled

Lawfare, 13 August 2025, <https://www.lawfaremedia.org/article/the-un-s-permanent-process-on-cybersecurity-faces-an-uphill-battle>.

¹¹⁶ Cyber Security Agency (CSA), ‘ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts’, Cyber Security Agency of Singapore, 19 September 2018, <https://www.csa.gov.sg/news-events/press-releases/amcc-2018/>.

¹¹⁷ Cyber Security Agency (CSA), ‘Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region’, Cyber Security Agency of Singapore, 16 October 2024, <https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region/>.

¹¹⁸ ‘SingHealth’s IT System Target of Cyberattack’, Ministry of Health, 20 July 2018, <https://www.moh.gov.sg/newsroom/singhealth-s-it-system-target-of-cyberattack/>.

¹¹⁹ Davina Tham, ‘Singapore Actively Dealing with Ongoing Cyberattack on Critical Infrastructure: Shanmugam’, Channel News Asia, 18 July 2025, <https://www.channelnewsasia.com/singapore/unc3886-cyber-security-threat-actor-attack-singapore-5245791>.

¹²⁰ UNC3886 is identified by cybersecurity firm Mandiant as a “China-nexus espionage group”. Following the announcement, the National Cyber Threat Alert Level was raised and new regulations for CII owners were rolled out. See: Cyber and Infrastructure Security Centre, *Critical Infrastructure Annual Risk Review (Second Edition) - November 2024* (Australian Government Department of Home Affairs, 2024), 35, <https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2024.pdf>.

a willingness to escalate messaging when thresholds are crossed. The aim is not retaliation but to enable coordinated, rules-based responses and to harden the reputational and operational downsides for repeat violations.

Net effect: Norm entrepreneurship with diplomatic convening gives Singapore outsized leverage. It supplies a common language for calling out unacceptable behaviours, puts partners in position to act together quickly, and raises the reputational and operational costs for would-be violators. However, limits remain: some actors discount reputation; ASEAN capacity is uneven; consensus processes can be slow. In 3Cs terms, Singapore's diplomatic actions strengthen credibility, sharpen communication, and build capability by diffusing workable procedures across the region.

4.4 Deterrence by Entanglement

Singapore's deterrent value from entanglement is economic-infrastructure. As a global financial centre, maritime hub, and regional data hub,¹²¹ it sits at junctions where disruption of its CII can generate second- and third-order costs across borders – creating a form of *self-deterrence* for state actors contemplating high-impact cyber operations.

In maritime trade, interference with port logistics, terminal operating systems, or key vendors would propagate through charter schedules, bills of lading, insurer liabilities and supply-chain contracts. As a finance hub, degradation of market infrastructure, core banking interfaces or payment rails would reverberate through correspondent networks and regional corporates with Singapore exposure. In the data layer, concentrated data-centre capacity and submarine-cable connectivity mean outages affect cloud tenancy and content delivery for regional customers, including entities linked to the attacker's own economy. Because these systems are embedded in a dense web of interdependence, adversaries face downside uncertainties: collateral damage can exceed intended boundaries and raise the cost-benefit threshold for any large-scale cyber disruption.

Net effect: Interdependence raises the expected blowback from major disruption and can hurt the adversary's own interest. However, it may not deter criminals or ideologically driven actors; states can also reroute over time; and the prospect of outsized impact can entice risk-acceptant adversaries. Entanglement therefore works best as shaping pressure, complementing denial by shortening outages, and norms by mobilising third parties. In 3Cs terms, it primarily strengthens credibility by making escalation risks and collateral costs more salient to adversaries.

4.5 Deterrence by Denial

Denial is Singapore's centre of gravity for deterrence in cyberspace. The aim is to lower the expected utility of hostile operations by making successful penetration less likely, containing any intrusion quickly to prevent spread, and assuring continuity of essential services. The approach combines statutory leverage, institutional coordination, rehearsed crisis management, and broad-based user hygiene.

At the core is a law-backed, centrally managed capability. The Cybersecurity Act converts best practice into enforceable duties on CII operators: risk assessments, periodic audits, and prompt incident reporting. Non-compliance is expressly criminalised

¹²¹ Brian Yap, 'Data Centres: The New Boom', *Law.Asia*, 3 September 2025, <https://law.asia/asia/data-centre-investment-boom-asia-2025/>.

and carries penalties ranging from substantial fines to imprisonment.¹²² The Cyber Security Agency of Singapore (CSA) leads national cybersecurity strategy and operations, and enforces the Act.¹²³ Sectoral regulators also oversee periodic audits, red-team/penetration-test programmes, and incident-reporting rehearsals to validate playbooks and escalation paths.¹²⁴ In a crisis, CSA can issue binding directions to CII operators or temporarily assume control of systems, reflecting Singapore's preference for centralised, top-down resilience.¹²⁵ SingCERT serves as the incident-response arm, providing early warning, technical advisories, and incident handling for government, industry, and the public.¹²⁶ Because compliance is monitored and breaches attract penalties, the rules bite; this is where capability and credibility meet in day-to-day regulation rather than in one-off statements.

Operational readiness is built and tested regularly. The Singapore Armed Forces' (SAF's) Digital and Intelligence Service (DIS) defends military networks, provides cyber



threat intelligence, and works with CSA and other agencies to harden national systems.¹²⁷ Each year, DIS and CSA co-organise the Critical Infrastructure Defence Exercise (CIDE), bringing CII operators into realistic detect-and-contain scenarios that validate sector playbooks and inter-agency procedures.¹²⁸ Readiness is also stress-tested in the biennial

Exercise Cyber Star, a whole-of-government cyber crisis management exercise that rehearses decision-making and cross-sector dependencies across all 11 CII sectors.¹²⁹

¹²² 'Cybersecurity Act 2018 (2020 Revised Edition)', Singapore Statutes Online, pt 3, accessed 18 August 2025, <https://sso.agc.gov.sg/Act/CA2018?WholeDoc=1>.

¹²³ Cyber Security Agency (CSA), 'Who We Are', Cyber Security Agency of Singapore, 22 January 2025, <https://www.csa.gov.sg/about-csa/who-we-are/>.

¹²⁴ Sectoral regulators include the Monetary Authority of Singapore, Infocomm Media Development Authority, Energy Market Authority. See: 'Business Continuity Exercise to Bolster Singapore Financial Resilience', The Asian Banker, 17 September 2025, <https://www.theasianbanker.com/press-releases/business-continuity-exercise-to-bolster-singapore-financial-resilience>.

¹²⁵ Singapore Statutes Online, 'Cybersecurity Act 2018 (2020 Revised Edition)', pt 4.

¹²⁶ SingCERT is shorthand for Singapore Cyber Emergency Response Team. See: Cyber Security Agency (CSA), 'SingCERT', Cyber Security Agency of Singapore, 24 June 2025, sect. General, <https://www.csa.gov.sg/faqs/singcert/>.

¹²⁷ Mike Yeo, 'SAF's Digital Service Inaugurates Two New Commands to Sharpen Cyber-Security Edge', *The Straits Times* (Singapore), 18 March 2025, <https://www.straitstimes.com/singapore/safs-digital-service-inaugurates-two-new-commands-to-sharpen-cybersecurity-edge>; 'Fact Sheet: Defence Cyber Command and SAF C4 & Digitalisation Command', Ministry of Defence, 3 March 2025, https://www.mindef.gov.sg/news-and-events/latest-releases/03mar25_fs/.

¹²⁸ Wei Kai Ng, 'Singapore Cyber Defenders Fight Simulated Attacks on AI-Enabled Systems in 4-Day Exercise', *The Straits Times* (Singapore), 15 November 2024, <https://www.straitstimes.com/singapore/singapore-cyber-defenders-fight-simulated-attacks-to-ai-enabled-systems-in-3-day-exercise>.

¹²⁹ Cyber Security Agency (CSA), '11 Critical Sectors Come Together to Tackle Complex Cyber Threat Scenarios in National Cyber Crisis Management Exercise', Cyber Security Agency of Singapore, 1 August 2025, <https://www.csa.gov.sg/news->

Denial also depends on the demand side. Digital Defence, introduced as the sixth pillar of Total Defence in 2019, extends responsibility to citizens and firms through public advisories, school curricula, and SME toolkits.¹³⁰ Routine campaigns on phishing, patching, and backups shrink the commodity attack surface that often enables higher-end operations.¹³¹ When authorities issue calibrated warnings about APT activity against critical systems, they not only tip off potential targets but also force adversaries to rotate tools and infrastructure, reducing expected returns.

External participation reinforces these effects. The ASEAN CERT Incident Drills embed shared methods with neighbours, improving speed and compatibility of cross-border response.¹³² The DIS also participates in demanding multilateral cyber exercises, such as the British Army's Exercise Defence Cyber Marvel and NATO's Exercise Locked Shields, which expose operators and decision-makers to complex attack chains and independent assessment.¹³³ These exercises strengthen crisis-management readiness for national IT systems and critical infrastructure, and help mature the DIS's ability to lead across agencies.

Net effect: Denial provides observable capability, demonstrates credibility through enforcement and exercised readiness, and sustains clear communication to operators and the public. The posture turns many incursions into tactical nuisances and narrows the window for strategic effect. Residual risks remain in cloud misconfigurations, third-party supply-chain exposures, social-engineering pathways, and APTs. Overall the combination of statute, supervision, rehearsal, and hygiene credibly shifts attacker calculus at the margin.

4.6 Deterrence by Punishment

Singapore's use of punishment as a tool of cyber deterrence is limited and calibrated. As a small state, its posture is shaped by pragmatism and strategic caution: it has no

events/press-releases/11-critical-sectors-come-together-to-tackle-complex-cyber-threat-scenarios-in-national-cyber-crisis-management-exercise/.

¹³⁰ 'Total Defence Strengthened with Addition of Digital Defence as the Sixth Pillar', Ministry of Defence, 15 February 2019, https://www.mindef.gov.sg/news-and-events/latest-releases/15feb19_nr/; 'Fact Sheet: Digital Defence', Ministry of Defence, 15 February 2019, https://www.mindef.gov.sg/news-and-events/latest-releases/15feb19_fs/.

¹³¹ 'Cybersecurity and Digital Resilience', Singapore Public Sector Outcomes Review 2024, 8 November 2024, <https://spor.performancereports.gov.sg/businesses/strong-and-resilient-economy/data-and-cyber-security/>; 'Advisories', Cyber Security Agency of Singapore, accessed 4 September 2025, <https://www.csa.gov.sg/alerts-and-advisories/advisories/>.

¹³² Cyber Security Agency (CSA), '19th Iteration of ASEAN Cyber Emergency Response Team (CERT) Incident Response Drill Tests CERT's Preparedness Against AI-Enabled Cyber Attacks', Cyber Security Agency of Singapore, accessed 23 August 2025, <https://www.csa.gov.sg/news-events/news-articles/19th-iteration-of-asean-cert-incident-response-drill-tests-cert-s-preparedness-against-ai-enabled-cyber-attacks/>.

¹³³ 'Singapore's Digital and Intelligence Service Participates in Multilateral Cyber Defence Exercise', Ministry of Defence, 1 March 2025, https://www.mindef.gov.sg/news-and-events/latest-releases/1mar25_nr1/; 'Digital and Intelligence Service Concludes Participation in Multinational Exercise Locked Shields 2025', Ministry of Defence, 11 May 2025, https://www.mindef.gov.sg/news-and-events/latest-releases/11may25_nr/.

publicly declared offensive cyber capabilities,¹³⁴ and has neither threatened nor taken punitive actions against state or state-linked actors for malicious cyber operations. Punitive effects are therefore most consistent domestically through its criminal law and internationally through multilateral law-enforcement cooperation.

Domestically, the Computer Misuse Act and related statutes provide significant penalties for unauthorised access, data theft and attacks on CII.¹³⁵ While primarily aimed at criminal actors, this enforcement raises the cost of operating within or through Singapore's jurisdiction and signals the state's willingness to pursue exploitation chains end-to-end. The signal is simple: exploitation chains that touch Singaporean jurisdiction face real legal risk.

Internationally, Singapore leans on cooperative policing and transparency to sharpen punishment. Participation in INTERPOL operations and joint investigations increases the probability that infrastructure and enablers are identified and disrupted. In 2025, Singapore contributed to an INTERPOL-led crackdown that ran over four months and took down over 1,000 Singapore-based IP addresses linked to cybercrime activity, demonstrating cross-border coordination alongside domestic enforcement.¹³⁶

Net effect: As a stand-alone pillar against state adversaries, punishment remains the weakest leg; escalation risks and scale constraints limit overt options. Its value is additive: domestic and international law-enforcement pressure increase costs for enablers and proxies. In 3Cs terms, punishment modestly supports credibility by demonstrating consequences and strengthens communication by clarifying thresholds, while norms and denial carry most of the deterrent load.

4.7 Assessment - Effectiveness of Cyber Deterrence

A zero-incident standard for cyber deterrence is unrealistic and unhelpful. In line with the benchmark set in Chapter 2 – Section 2.6, the question is whether adversaries refrain from large-scale, destructive, or politically significant operations, and whether, when intrusions occur, Singapore contains compromises and restores services quickly. Put differently, the test is whether Singapore raises perceived costs, reduces likely gains, and denies easy success.

Where deterrence worked

Due to national security considerations, Singapore publishes limited details on the GZ cyberattacks that it faces. That said, there have been no known cyber incidents that

¹³⁴ International Institute for Strategic Studies, *Chapter 10: "Singapore" — in Cyber Capabilities and National Power*, Volume 2, IISS Research Paper (International Institute for Strategic Studies, 2023), 18, https://www.iiss.org/globalassets/media-library---content-migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_10-singapore.pdf.

¹³⁵ 'Computer Misuse Act 1993 (2020 Revised Edition)', Singapore Statutes Online, accessed 18 August 2025, <https://sso.agc.gov.sg/Act/CMA1993?WholeDoc>.

¹³⁶ 'Singapore Authorities Take down over 1,000 IP Addresses Linked to Cybercrimes', Channel News Asia, 11 June 2025, <https://www.channelnewsasia.com/singapore/singapore-authorities-take-down-ip-addresses-link-cybercrimes-5174756>.

resulted in sustained disruption of essential services or politically decisive effects.¹³⁷ Statutory duties on CII operators, exercised crisis management through CIDEX and Exercise Cyber Star, and the ability to issue binding directions have likely supported rapid containment and continuity.¹³⁸

A recent stress test of recovery capacity was the 19 July 2024 CrowdStrike global IT outage. In that incident, Changi Airport was the most affected local operator: business continuity plans were activated, the airport operator switched to manual processes, and SingCERT issued an advisory to guide recovery. One flight was cancelled and 108 flights were delayed by more than 30 minutes, after which affected systems largely recovered within a day and services returned to normal.¹³⁹ Although this was not a cyberattack, the episode shows readiness and recovery processes consistent with a deterrence by denial posture.

Where deterrence remains limited

Suspected APT activity increased more than fourfold between 2021 and 2024, indicating persistent pressure from capable state-linked actors.¹⁴⁰ Prevention is not assured against APTs, particularly stealthy espionage and supply-chain compromise. Strong cyber defences did not prevent the 2014 MFA breach, the 2017 NUS and NTU breaches, the 2018 SingHealth breach, and the 2025 campaign attributed publicly to UNC3886 that targeted CII.¹⁴¹ Because Singapore has not publicly attributed GZ cyberattacks to any state, there is limited basis for state-level punitive measures. With a few lines of code, a breach can transform from espionage to deliver a destructive payload,¹⁴² and unless that happens, entanglement bears no weight.

Summary

In sum, Singapore's posture has constrained adversaries rather than eliminated hostile activity. It has worked in the sense that attempts at coercive disruption have not produced strategic outcomes, and recovery has been fast when systems were stressed. Denial is the most reliable pillar, supported by law-backed baselines, visible supervision, and rehearsed cross-sector drills that raise attacker costs and compress the window for effect. Normative diplomacy socialises expectations and helps partners coordinate

¹³⁷ Tan, 'A Small State Perspective on the Evolving Nature of Cyber Conflict', 165.

¹³⁸ Ng, 'Singapore Cyber Defenders Fight Simulated Attacks on AI-Enabled Systems in 4-Day Exercise'; Cyber Security Agency (CSA), '11 Critical Sectors Come Together to Tackle Complex Cyber Threat Scenarios in National Cyber Crisis Management Exercise'.

¹³⁹ 'MDDI's Response to PQs on Impact of CrowdStrike Outage on SG Gov Services', Ministry of Digital Development and Information, 7 August 2024, <https://www.mddi.gov.sg/newsroom/mddi-s-response-to-pqs-on-impact-of-crowdstrike-outage-on-sg-gov-services/>.

¹⁴⁰ Shanmugam, 'Opening Speech by Mr K Shanmugam, Coordinating Minister for National Security and Minister for Home Affairs, at CSA's 10th Anniversary Dinner', Annex 1.

¹⁴¹ Shanmugam, 'Opening Speech by Mr K Shanmugam, Coordinating Minister for National Security and Minister for Home Affairs, at CSA's 10th Anniversary Dinner', Annex 1.

¹⁴² Nye, 'Deterrence and Dissuasion in Cyberspace', 47.

responses and frame violations, which reduces perceived gains from escalation. Entanglement raises the blowback risk for large-scale disruptions. Punishment remains the least decisive lever against state-linked actors, especially since no direct public attribution has been made.

The next chapter synthesises the Estonia and Singapore cases to draw comparative lessons and policy implications for small states.

Chapter 5: Lessons for Small States

5.1 Introduction

Small states cannot deter cyber coercion by matching great-power capabilities; they deter by shaping adversaries' cost-benefit calculations. This chapter distils comparative lessons from Estonia and Singapore across the four mechanisms – denial, norms, entanglement, and punishment – and draws out applicable lessons for small states to deter GZ cyber operations. The aim is practical: identify what travels, what must be tailored, and how to combine mechanisms so that GZ cyber operations become costly, and strategically unproductive. The lessons are organised to cover the four mechanisms – norms, entanglement, denial and punishment – followed by overarching guidance on layering, context-fit, and signalling. Throughout, the benchmark is not a zero-incident standard, but whether adversaries refrain from large-scale, destructive, or politically significant cyberattacks, and whether routine intrusions are contained and recovered from swiftly so that essential services endure, partners rally, and reputational or regulatory costs mount for the attacker.

5.2 Lesson 1: Normative Deterrence is a Practical Toolkit

First, normative deterrence is a practical toolkit and a long game of building adherence. For small states, norms function as a strategic equaliser: when material power is limited, rule-based constraints, reputational costs, and institutionalised expectations curb predation and create predictable operating space.¹⁴³ Hence, small states should expand and deepen buy-in through international and regional organisations, and operational partnerships that turn abstract rules into routine practice.

Estonia's norm entrepreneurship shows what this looks like in practice:¹⁴⁴ it leveraged the 2007 cyberattacks to drive cyber onto EU, NATO and UN agendas, hosting the NATO CCDCOE and facilitating the Tallinn Manual process.¹⁴⁵ Crandall and Allan characterise Estonia's norm strategy as a "small state, big ideas" strategy – agenda-setting and institutional entrepreneurship to socialise expectations.¹⁴⁶ Estonia has regularly used public attribution to communicate unacceptable state behaviour.¹⁴⁷ In 2019, Estonia adopted public-attribution guidelines, codified decision processes and established an inter-agency working group to align responses and evidence thresholds, thereby translating normative commitments into predictable state practice.¹⁴⁸

¹⁴³ Adam Lupel and Lauri Mälksoo, *A Necessary Voice: Small States, International Law, and the UN Security Council* (International Peace Institute, 2019), sect. Executive Summary.

¹⁴⁴ , A norm entrepreneur brings an issue to attention and tries to convince others to adopt the new norm to address the issue. This is the takes place during the first stage in the "life-cycle" of norm – i.e. the emergence of norms. See: Crandall and Allan, 'Small States and Big Ideas', 348.

¹⁴⁵ See Chapter 3, "Normative Deterrence".

¹⁴⁶ Crandall and Allan, 'Small States and Big Ideas'.

¹⁴⁷ Pernik, *Cyber Deterrence*, 17.

¹⁴⁸ Information System Authority (RIA), *Cyber Security in Estonia 2020*, 23–24.

Singapore's contribution to norm building as a norm leader is complementary, championing sustained, multilateral norm development and confidence-building measures as a way to prevent escalation in a globalised, interdependent environment.¹⁴⁹ For example, as chair for the 2nd OEWG, it secured the establishment for the Global Mechanism to continue sustained dialogue for cyberspace normative development. Within ASEAN it also drove regional CBMs and capacity-building, including the ASEAN-Singapore Cybersecurity Centre of Excellence and the ASEAN Regional CERT initiative.¹⁵⁰ Compared to Estonia, its attribution practice is limited and highly calibrated – to keep diplomatic temperatures low. Singapore made its first public naming of an APT – UNC3886 – via a technical attribution that avoided naming any country, timed to coincide with the gathering of cyber professionals at the CSA's 10th-anniversary dinner.¹⁵¹ Beijing did not announce any formal protest; instead, the Chinese Embassy issued a public rebuttal on its website and Facebook denying any China link to UNC3886.¹⁵²

In concrete terms for other small states: embed agreed norms into regional instruments so breaches draw collective diplomatic or regulatory responses; and operationalise them through CERT-to-CERT channels, joint exercises, and CBMs. Small states should also be clear about their attribution principles and develop their own guidelines or “attribution ladder” that sets clear conditions for when to attribute publicly, at what level of government, and with what evidentiary threshold because guidelines make signalling credible and consistent, protect sensitive sources and methods, enable coalition/joint attributions, and manage escalation risks while preserving participation incentives.

5.3 Lesson 2: External Amplification Multiplies Deterrent Effect

Second, external amplification multiplies deterrent effects. It is generated by entanglement that gives other actors a stake in a small state's stability and incentives to act with it. Small states' deterrent signals can also be amplified by larger structures.

Estonia demonstrates how alliance entanglement through the EU and NATO magnifies both norms and punishment: coordinated EU attributions and targeted sanctions under the EU Cyber Diplomacy Toolbox raise costs on offenders; and NATO's declared readiness to employ full range of capabilities and to consider collective defence (Article 5) in certain circumstances adds weight to national signalling.¹⁵³ Thorhallsson describes this as political shelter-seeking behaviour by small states — obtaining “diplomatic,

¹⁴⁹ A norm leader influences other states to accept the norms. This takes place during the second stage in the “life-cycle” of norms - i.e., the acceptance of norms. During which, See: Crandall and Allan, ‘Small States and Big Ideas’, 348.

¹⁵⁰ See Chapter 4, “Normative Deterrence”.

¹⁵¹ Tham, ‘Singapore Actively Dealing with Ongoing Cyberattack on Critical Infrastructure’.

¹⁵² Xinghui Kok, ‘China Denies Link to Espionage Group Accused of Attacking Singapore Critical Infrastructure’, China, *Reuters*, 21 July 2025, <https://www.reuters.com/world/china/china-denies-link-espionage-group-accused-attacking-singapore-critical-2025-07-21/>.

¹⁵³ See Chapter 3, “Deterrence by Entanglement”.

military, and administrative backing from large states and international organisations,” and benefiting from norms and rules that reduce coercion.¹⁵⁴

Singapore shows that market entanglement can play a similar role via a different channel: a rules-first environment that partners rely on for trade and finance creates shared interests in stability, raising the reputational, diplomatic, and collateral costs of disruption for any would-be aggressor.

In both variants, gains are contingent – on alliance cohesion in Estonia's case and on sustained interdependence in Singapore's. Small states should therefore assess their structural position and cultivate avenues for amplification.

5.4 Lesson 3: Denial is the Foundation – Resilience makes it Credible

Third, denial is the foundation on which other mechanisms stand, and in GZ, resilience is the operational expression of deterrence by denial. For small states, denial is attractive because it can be built unilaterally, scales with capacity, and signals staying power without inviting escalation. In practice, whole-of-society resilience – baseline controls, rehearsed playbooks, and rapid recovery – functions as small-state strategy: it lowers expected returns even when attribution is contested.

The operational test is simple but decisive: whether essential services can absorb, contain, and recover under stress; whether decision pathways are rehearsed before a crisis; and whether public confidence in digital functions is sustained during and after incidents. Tim Prior describes resilience as a *fifth wave* of deterrence – deterring by limiting returns and demonstrating staying power.¹⁵⁵ Credible denial begins with strong defences: baseline controls and secure-by-design architectures; segmentation and least privilege; tested offline backups and data-recovery tiers; continuous monitoring and threat-intelligence sharing; crisis-management drills (technical and executive); and practised public communication to sustain trust.

Estonia's ecosystem offers concrete examples: at home, Estonia's Cybersecurity Act obliges operators of essential services to conduct risk assessments, implement baseline controls, report incidents, and participate in regular national and sector-specific drills and table-top exercises coordinated by RIA and sectoral regulators; the data embassy in Luxembourg hosts critical replicas of core state systems, ensuring continuity of state data and services hosted from abroad; and the Defence League's Cyber Defence Unit (CDU) extends surge capacity to peacetime and private-sector incidents – all of which

¹⁵⁴ Baldur Thorhallsson and Sverrir Steinsson, 'Chapter 2 - A Theory of Shelter', in *Small States and Shelter Theory: Iceland's External Affairs / Edited by Baldur Thorhallsson.*, 1st. (Routledge, 2018), sect. Introduction, deakin.b4211480, <https://research.ebsco.com/linkprocessor/plink?id=91f12d98-5bf8-3275-a81a-3edd7cc7db17>.

¹⁵⁵ Tim Prior, 'Resilience: The "Fifth Wave" in the Evolution of Deterrence', in *Strategic Trends 2018: Key Developments in Global Affairs* (Centre for Security Studies - ETH Zurich, 2018), https://www.researchgate.net/publication/325735191_Resilience_The_'Fifth_Wave'_in_the_Evolution_of_Deterrence.

directly reduce attacker pay-offs. Collectively, these domestic measures implement denial by shortening dwell time, preserving service continuity, and raising recovery confidence. Complementing this day-to-day posture, Estonia rehearses allied crisis coordination through the annual NATO Cyber Coalition exercise, while Locked Shields adds a complementary readiness strand by stress-testing decision-making and technical teams under realistic pressure.¹⁵⁶

Singapore's ecosystem similarly extends into the private sector: the CSA and SingCERT coordinate advisories, incident reporting, and response with industry; CII operators are legally mandated under Singapore's Cybersecurity Act to maintain system safeguards and report incidents; and national exercises such as CIDEX and Exercise Cyber Star regularly drill CII operators alongside whole-of-government agencies. Sectoral regulators (e.g., Monetary Authority of Singapore, Infocomm Media Development Authority, Energy Market Authority) also oversee periodic audits, red-team/ penetration-testing programmes, and incident-reporting rehearsals to validate playbooks and escalation paths.¹⁵⁷ Together, these instruments make denial credible in day-to-day operations by tightening baselines, clarifying roles, and rehearsing recovery.¹⁵⁸

Common to both is whole-of-society involvement: sustained public education and media-literacy programmes; baseline cyber-hygiene by default (e.g., multi-factor authentication, timely patching, password managers, and tested backups); clear incident-reporting channels and public hotlines; structured public-private information-sharing through sector forums and regulator-industry briefings; regular joint exercises that include private operators and key vendors; and volunteer or auxiliary cyber programmes to surge specialist capacity. Both states also invest in workforce and SME uplift – scholarships, competitions, certification pathways, and practical toolkits or incentives for small and medium enterprises—to normalise safe behaviour, accelerate detection and reporting, and build redundancy beyond government. In short, resilience is deterrence-by-denial in practice: it lowers adversaries' expected returns even when attribution is contested and escalation is undesirable.

Together, these measures keep essential services running under stress, lowering the expected pay-off of coercive cyber operations even when attribution is contested and escalation is undesirable. For many small states, building this kind of continuity, redundancy, and exercise culture is not merely “defensive”; it is core deterrence-by-denial. Investment must be persistent and adaptive to evolving technology and adversary tradecraft, and as such, costly.

5.5 Lesson 4: Punishment Requires Innovation and Restraint

A fourth lesson is that punishment requires innovation and restraint in equal measure. Small states cannot credibly threaten large-scale retaliation against a major power. As such, punitive credibility rests on two logics: pooling coercive tools through alliances

¹⁵⁶ See Chapter 3, “Deterrence by Denial”.

¹⁵⁷ See Chapter 4, “Deterrence by Denial”.

¹⁵⁸ See Chapter 4, “Deterrence by Denial”.

and institutions, and using legal and regulatory and law-enforcement measures to impose targeted costs on jurisdictionally reachable actors while keeping escalation low.

Estonia compensates by pooling measures with allies and being willing to *go visible* when the normative and political returns are high – in 2018, it joined U.S., U.K. and Australia in the collective attribution of NotPetya to Russian state-linked actors, and in 2020, it supported the EU's first cyber sanctions – together illustrate the approach.¹⁵⁹ In September 2024, Estonia issued a unilateral attribution of GRU espionage against its ministries; it was a calculated move, tightly calibrated to the U.S. indictment of the broader GRU campaign (which Estonia had supported), thereby priming EU follow-on sanctions and converting a national signal into allied consequences.¹⁶⁰

Singapore channels punishment primarily through law enforcement and regulatory action, while keeping diplomatic temperatures low. Its Cybersecurity Act, Computer Misuse Act, and sectoral regulators enable targeted investigations, fines, and directives against reachable actors; CSA and SingCERT also publish technical exposures to warn industry and signal resolve without interstate escalation.¹⁶¹ Despite facing cyberattacks over the years, Singapore has yet to retaliate against any state for cyberattacks. The closest analogue has been its public naming of UNC3886 – a calibrated signal of resolve that raised costs while signalling a willingness to escalate messaging – as discussed earlier.

For small states: think creatively about targeted legal tools, joint attributions, and coalition mechanisms that impose real costs on reachable actors, without making promises you cannot keep against those you cannot reach.

5.6 Lesson 5: Layered Deterrence Posture is Cardinal

Fifth, layered deterrence is not optional but cardinal.

From the case studies, neither state relies on any single mechanism. Estonia's posture illustrates this: it couples denial through technical hardening and whole-of-society response with entanglement through membership in NATO and the EU, and punishment and norms through unilateral and collective attributions backed by EU restrictive measures. These instruments mutually reinforce one another. Singapore's layering is different in form but similar in function: a centralised regulatory model with whole-of-society contribution, hub-economy interdependence, and norms-centred diplomacy work together to limit adversaries' gains and broaden the circle of actors inclined to respond.

¹⁵⁹ See Chapter 3, "Deterrence by Punishment".

¹⁶⁰ Public Relations Department, 'Estonia Names Russia's Military Intelligence in a First-Ever Attribution of Cyberattacks'; 'Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government', United States Department of Justice - Archives, 5 September 2024, <https://www.justice.gov/archives/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government>.

¹⁶¹ See Chapter 4, "Deterrence by Punishment".

In practice, the mechanisms do distinct, complementary jobs for small states: denial keeps essential services running and depresses attackers' expected returns; norms mobilise partners for joint attribution and regulatory follow-through; entanglement channels costs via alliances and markets (e.g., EU restrictive measures; reliance on Singapore's hub functions); and punishment is used selectively against reachable actors through legal and financial tools.

For small states, the lesson is to design for complementarity: each mechanism should compensate for predictable limits in the others so that the overall effect is to make coercion costly, conspicuous, and strategically unproductive.

5.7 Lesson 6: Design Must Fit Context

Sixth, the design of each deterrence mechanism must fit context.

Estonia's proximity to Russia, a persistent state adversary, and its integration into NATO and the EU have made visible the mutually reinforcing roles of norm enforcement, political-security entanglement, and societal resilience. Concrete manifestations include the 2007 cyberattack catalysing institution-building, including NATO CCDCOE and the Tallinn Manual process, the government's adoption of public-attribution guidelines in 2019, and selective joint attributions with partners where the political pay-off warranted visibility. Estonia also participates in the EU's cyber-diplomacy toolbox and sanctions regime, and rehearses allied crisis playbooks through large-scale exercises such as Cyber Coalition, aligning national responses with allied expectations.¹⁶²

Singapore, by contrast, operates at the crossroads of major-power competition and global commerce; centralised regulation, economic interdependence, and consensus-oriented diplomacy are the natural complements to its role as a trusted hub. In practice, this means centralised authority in the CSA to enforce its Cybersecurity Act, which mandates robust cyber defence measures for CII operators; regular cyber defence and crisis management exercises through CIDEX and Exercise Cyber Star; and investment in regional CBMs through initiatives such as the ASEAN-Singapore Cybersecurity Centre of Excellence and the ASEAN Regional CERT to promote stability and reduce escalation incentives.¹⁶³

For small states, the transferable insight is the logic, not the template: keep the deterrence logic constant, but tailor the form of each mechanism to your threats, alliances, institutions and economy.

5.8 Lesson 7: Communication is Part of the Mechanism – Align Words and Deeds

Finally, communication is part of the mechanism, not an afterthought. Estonia communicates resolve by making attacks and responses visible: public attribution is explicitly framed to send clear messages, set expectations of conduct, and reinforce

¹⁶² See Chapter 3.

¹⁶³ See Chapter 4.

collective action;¹⁶⁴ this visibility pairs with exercises and allied infrastructure on Estonian soil to show that coercion fails because functions persist and allies rally.

Singapore communicates credibility by projecting stability: the absence of major disruptions and the regularity of enforcement and compliance keep rhetorical temperature low, while exercises convey that attacks are unlikely to yield strategic returns. Its emphasis on norms and CBMs reinforces this signal to external audiences.

Neither approach is inherently superior; each matches the state's broader strategy. The practical lesson is to align words and deeds. If a state chooses ambiguity to preserve room for manoeuvre, its domestic institutions must reliably deliver quiet resilience. If a state chooses visibility to galvanise allies and deter adversaries, it must be prepared to weather short-term friction in exchange for long-term credibility.

5.9 Putting it Together: A Sequencing Logic for Small States

Taken together, these lessons suggest a simple sequencing logic for small-state strategy in cyberspace. Start with denial and build outward: ensure that essential services can withstand and recover from attacks, and institutionalise resilience as deterrence; promote norms and work with like-minded partners to entrench their adoption regionally and internationally; select the form of entanglement that best leverages your structural position; and deploy punishment selectively. This reflects Nye's insight that mutually reinforcing mechanisms – norms, entanglement, denial, and tailored punishment – must be combined to shape adversaries' calculus. The precise mix will vary, but the objective remains constant: to make hostile operations in GZ unattractive not because they are impossible but because they are unlikely to achieve strategic effects, especially large-scale, destructive, or politically significant ones.

5.10 Summary

Estonia and Singapore show that small states can deter GZ cyber threats by layering mechanisms whose credibility does not hinge on great-power capabilities. Both employ norms, entanglement, denial, and punishment, but weight them differently: Estonia combines visible norm entrepreneurship and allied entanglement with a decentralised, whole-of-society denial posture; Singapore relies on consensus-based norm building and economic interdependence under a centralised denial model. Punishment is constrained in both cases and thus nested within alliances (Estonia) or technical and legal exposure (Singapore). Across the cases, denial is foundational: credible resilience makes other signals believable and keeps hostile operations strategically unproductive. Again, success is evidenced not by incident-free networks but by the absence of large-scale, destructive, or politically significant outcomes, and by rapid containment and recovery when intrusions occur.

For small states, the implications are practical: harden first for continuity and rapid recovery; fit each mechanism to context and audiences; align communication with what institutions can reliably deliver; and treat normative deterrence as a long game that

¹⁶⁴ Information System Authority (RIA), *Cyber Security in Estonia 2020*, 24.

extends beyond the UN into regional bodies, operational partnerships, industry forums, and domestic law. Deterrence in cyberspace will remain partial, but by making attacks costly, conspicuous, and ineffective, small states can blunt coercion without matching the capabilities of larger powers.

Chapter 6: Conclusion

This thesis set out to answer the question: how can small states deter cyberattacks that sit in the GZ between peace and war? The answer is not to mimic great-power playbooks, but to layer four distinct mechanisms – punishment, denial, norms, and entanglement – in ways that fit domestic institutions, alliances, and political style. Joseph Nye's framework remains the most serviceable map.¹⁶⁵ Small states raise costs and reduce expected gains by combining denial with calibrated punishment, and by leveraging norms and interdependence to widen the circle of actors with a stake in stability. Crucially, cyber deterrence must be tailored, context-aware, and judged by behavioural outcomes rather than incident-free perfection.

Across the two cases, a common pattern emerges. Estonia and Singapore both deter not by threatening cyber dominance but by narrowing the payoff for hostile operations, signalling credibility through visible practice, and embedding their security in wider communities. Estonia's experience shows how a small, exposed state can turn crisis into agenda-setting influence – hosting the NATO CCDCOE, driving the Tallinn Manual process, and using public attribution and EU instruments to translate legal argument into coordinated response.¹⁶⁶ Singapore, operating as a highly connected hub in a contested region, emphasises law-backed baselines for critical infrastructure, whole-of-society drills, and norms-centred diplomacy that lowers the political temperature while expanding practical cooperation.¹⁶⁷ Neither relies on a single lever. Each state layers mechanisms to make coercion costly, conspicuous, and strategically unproductive.

The central pillar is denial, operationalised as resilience. Tim Prior captures this shift as a “fifth wave” of deterrence in which resilient socio-technical systems anticipate, absorb, and recover from shocks, denying attackers decisive effects even when attribution is delayed or contested.¹⁶⁸ Viewed from this angle, resilience as operationalised by Estonia and Singapore is a governance style (flexible, distributed, and rehearsal-heavy) that reduces the adversary's expected returns and demonstrates staying power under stress. For small states, this is deterrence they can afford, scale, and prove in peacetime.

Norms and entanglement then amplify denial. Estonia's cyber diplomacy illustrates how multi-lateralising norms raises reputational costs for irresponsible behaviour and enables joint responses – from collective attribution to EU restrictive measures. More broadly, small states benefit disproportionately when international law is taken seriously. Legalism is not naïve idealism but a strategic hedge that substitutes rules for raw power.¹⁶⁹ Singapore's regional initiatives similarly entrench expectations and practical

¹⁶⁵ Nye, 'Deterrence and Dissuasion in Cyberspace', sect. Four Means of Deterrence and Dissuasion.

¹⁶⁶ Crandall and Allan, 'Small States and Big Ideas', sect. Building Estonia's Cybersecurity Norms; Pernik, *Cyber Deterrence*, sect. Practising cyber deterrence in Estonia.

¹⁶⁷ Tan, 'A Small State Perspective on the Evolving Nature of Cyber Conflict'.

¹⁶⁸ Prior, '(PDF) Resilience'.

¹⁶⁹ Lupel and Mälksoo, *A Necessary Voice*; Janet H. Anderson, 'Is the ICJ the New “Nuclear Weapon” of Small States?', *JusticeInfo.Net*, 5 March 2024,

confidence-building measures, turning abstract norms into routines across CERTs, regulators, and operators. In short, norms give small states voice and leverage, while entanglement ensures that attacks risk collateral consequences for larger stakeholders.

Yet the GZ is a lawyer's minefield and a strategist's headache. Adversaries operate below the threshold of armed attack and hence responses must draw on legal and regulatory tools, cross-government coordination, and alliance or market instruments short of force. The lesson is not to abandon deterrence, but to accept that the decisive battles are often fought in law, process, and partnerships – areas where small states can compete.

There are limits. Alignment politics can slow norm “cascades.” Entanglement may not bite if partners are distracted or divided. Punishment against state-linked actors is inherently constrained for small states. Resilience is resource-intensive and uneven across sectors. These are reminders that layered deterrence must be constantly maintained, communicated, and adapted.

For small states, the lessons are pragmatic and actionable:

1. Normative deterrence is a practical toolkit: Keep investing in norm entrepreneurship, and codify an attribution ladder your partners recognise. Translate UN/ASEAN commitments into repeatable CBMs, maintained points-of-contact directories, standing CERT-to-CERT channels and supply-chain assurance. Pre-agree evidence thresholds, decision venues and communications templates so movement from technical to political attribution is timely, coalition-minded and controlled.
2. Entanglement multiplies costs through alliances and markets: Pre-wire collective tools. Align national playbooks with regional or alliance instruments (for example, coordinated attribution, sanctions, regulatory actions) and set trigger criteria with partners in advance. Use market levers – joint procurement conditions, cyber insurance requirements, and vendor standards – to raise costs for attackers and enablers.
3. Denial is the foundation – resilience makes it credible: Institutionalise resilience as deterrence. Mandate sector baselines, run joint technical–executive exercises and publish after-action improvements. Harden by default (segmentation, least privilege, offline tested backups, monitored recovery tiers). Drill crisis communications so confidence in essential services hold under stress. Treat service continuity as the public metric of success.
4. Punishment requires innovation and restraint: Innovate punishment proportionately. Pool coercive power where possible. Otherwise, target reachable actors: legal seizures, compliance penalties, export-control designations, civil liability against facilitators and exclusion from government markets. Sequence measures on a pre-planned ladder to keep credibility high and escalation controlled.

5. Layered deterrence posture is cardinal: Anticipate cross-domain spillovers. Integrate cyber, information, economic and diplomatic instruments. Create an integrated-effects cell to synchronise timing and messaging, and run cross-domain exercises so hand-offs are smooth under pressure.

6. Design must fit context: Tailor to strategic culture, legal authorities, risk appetite and sector exposure. Choose governance that matches your system, and pick a signalling style that suits. Prioritise selected sectors, then scale. Measure what matters for your context (time-to-detect, time-to-contain, service continuity under stress, coalition response speed) and report annually.

7. Align words and deeds: Sustain audience-aware signalling. Match declarations, budgets, exercises and consequences so commitments remain credible. Coordinate releases with partners, explain incidents and fixes promptly and keep message discipline. When you signal red lines, enforce them; when you promise learning, show the fixes.

Further studies could develop shared, behaviour-based metrics (e.g., time to detect and contain, service continuity under stress, coalition response speed) that enable cross-country comparison; probe when entanglement truly deters versus when interdependence becomes leverage, including failure cases where partners are divided or slow; and trace how UN/ASEAN language becomes routine practice by testing specific mechanisms such as joint attribution procedures, incident-notification rules and supply-chain assurance. Advancing these lines will provide small states with a clearer playbook and firmer evidence for what works, what does not and what to fix next.

In conclusion, small states can deter cyber coercion not by out-muscling adversaries, but by making aggressive operations unlikely to deliver strategic effect. Layering denial, norms, entanglement, and selective punishment, they convert vulnerability into a posture that is credible, communicable, and coalition-ready. Estonia and Singapore demonstrate that when resilience holds, rules are socialised, and partners have skin in the game, adversaries learn that the returns to coercion are meagre and the risks of exposure are real. Cyber deterrence will never be perfect, but perfection is not the point. The point is to ensure that those who would coerce find that, in practice, they cannot, because essential services endure, partners rally, and the costs mount faster than the gains. That is how small states can deter in the GZ: not by shouting the loudest, but by designing failure into the attacker's plan.

Bibliography

Anderson, Janet H. 'Is the ICJ the New "Nuclear Weapon" of Small States?' *JusticeInfo.Net*, 5 March 2024. <https://www.justiceinfo.net/en/129172-is-the-icj-the-new-nuclear-weapon-of-small-states.html>.

Andrea Ó Súilleabháin. *Small States at the United Nations: Diverse Perspectives, Shared Opportunities*. International Peace Institute, 2014. https://www.ipinst.org/wp-content/uploads/publications/ipi_e_pub_small_states_at_un.pdf.

Armstrong, H., R.J. De Kervenoael, X. Li, and R. Read. 'A Comparison of the Economic Performance of Different Micro-States, and between Micro-States and Larger Countries'. *World Development* 26, no. 4 (1998): 639–56. [https://doi.org/10.1016/S0305-750X\(98\)00006-0](https://doi.org/10.1016/S0305-750X(98)00006-0).

Armstrong, Harvey, and Robert Read. 'Geographical "handicaps" and Small States: Some Implications for the Pacific from a Global Perspective'. *Asia Pacific Viewpoint* 47, no. 1 (2006): 79–92. <https://doi.org/10.1111/j.1467-8373.2006.00294.x>.

Azubuike, Callistus Francis. 'Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks'. *Nnamdi Azikiwe Journal of Political Science* 8, no. 3 (2023): 101–14.

Baker, Kurt. 'What Is an Advanced Persistent Threat (APT)?' CrowdStrike, 4 March 2025. <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/>.

Bendiek, Annegret, and Matthias Schulze. 'Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW'. *SWP Research Paper*, Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, 2021, 11/2021. <https://doi.org/10.18449/2021RP11>.

Borghard, Erica D., and Shawn W. Lonergan. 'Deterrence by Denial in Cyberspace'. *Journal of Strategic Studies* 46, no. 3 (2023): 534–69. <https://doi.org/10.1080/01402390.2021.1944856>.

Brands, Hal. 'Paradoxes of the Gray Zone'. SSRN Scholarly Paper No. 2737593. Social Science Research Network, 1 January 2016. <https://doi.org/10.2139/ssrn.2737593>.

Brock, Julia. 'ASEAN's Cyber Initiatives: A Select List'. Centre for Strategic Studies & International Studies (CSIS), 16 July 2024. <https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list>.

Cardash, Sharon L., Frank J. Cilluffo, and Rain Ottis. 'Estonia's Cyber Defence League: A Model for the United States?' *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777–87. 89890772. <https://doi.org/10.1080/1057610X.2013.813273>.

Channel News Asia. 'Singapore Authorities Take down over 1,000 IP Addresses Linked to Cybercrimes'. 11 June 2025. <https://www.channelnewsasia.com/singapore/singapore-authorities-take-down-ip-addresses-link-cybercrimes-5174756>

Council of the European Union. 'Cyber-Attacks: Three Individuals Added to EU Sanctions List for Malicious Cyber Activities against Estonia'. 27 January 2025. <https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia/>.

Council of the European Union. 'The EU Sanctions Process Explained'. Accessed 7 September 2025. <https://www.consilium.europa.eu/en/infographics/the-eu-sanctions-process-explained/>.

Council of the European Union (General Secretariat). 'Council Conclusions on the Development of the European Union's Cyber Posture'. Council of the European Union, 23 May 2022. <https://www.consilium.europa.eu/media/56358/st09364-en22.pdf>.

Crandall, Matthew, and Collin Allan. 'Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms'. *Contemporary Security Policy* 36, no. 2 (2015): 346–68. edselc.2-52.0-84937643444. <https://doi.org/10.1080/13523260.2015.1061765>.

Cyber and Infrastructure Security Centre. *Critical Infrastructure Annual Risk Review (Second Edition) - November 2024*. Australian Government Department of Home Affairs, 2024. <https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2024.pdf>.

Cyber Security Agency (CSA). '11 Critical Sectors Come Together to Tackle Complex Cyber Threat Scenarios in National Cyber Crisis Management Exercise'. Cyber Security Agency of Singapore, 1 August 2025. <https://www.csa.gov.sg/news-events/press-releases/11-critical-sectors-come-together-to-tackle-complex-cyber-threat-scenarios-in-national-cyber-crisis-management-exercise/>.

Cyber Security Agency (CSA). '19th Iteration of ASEAN Cyber Emergency Response Team (CERT) Incident Response Drill Tests CERT's Preparedness Against AI-Enabled Cyber Attacks'. Cyber Security Agency of Singapore. Accessed 23 August 2025. <https://www.csa.gov.sg/news-events/news-articles/19th-iteration-of-asean-cert-incident-response-drill-tests-cert-s-preparedness-against-ai-enabled-cyber-attacks/>.

Cyber Security Agency (CSA). 'ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts'. Cyber Security Agency of Singapore, 19 September 2018. <https://www.csa.gov.sg/news-events/press-releases/amcc-2018/>.

Cyber Security Agency (CSA). 'CSA Releases Key Findings from Singapore Cybersecurity Health Report 2023'. Cyber Security Agency of Singapore, 28 March 2024. <https://www.csa.gov.sg/news-events/press-releases/csa-releases-key-findings-from-singapore-cybersecurity-health-report-2023/>.

Cyber Security Agency (CSA). 'Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region'. Cyber Security Agency of Singapore, 16 October 2024. <https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region/>.

Cyber Security Agency (CSA). 'Singapore Cybersecurity Health Report'. Cyber Security Agency of Singapore, 2024. <https://isomer-user-content.by.gov.sg/36/1051bace-6be7-4c59-934a-e43c952a32ed/csa-singapore-cybersecurity-health-report-2023.pdf>.

Cyber Security Agency (CSA). *Singapore Cybersecurity Strategy 2021*. Cyber Security Agency of Singapore, 2021. <https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf>.

Cyber Security Agency (CSA). 'SingCERT'. Cyber Security Agency of Singapore, 24 June 2025. <https://www.csa.gov.sg/faqs/singcert/>.

Cyber Security Agency (CSA). 'Who We Are'. Cyber Security Agency of Singapore, 22 January 2025. <https://www.csa.gov.sg/about-csa/who-we-are/>.

Cyber Security Agency of Singapore. 'Advisories'. Accessed 4 September 2025. <https://www.csa.gov.sg/alerts-and-advisories/advisories/>.

Economic Development Board (EDB) Singapore. 'Singapore Boosts Maritime, Aviation Hub Role as Cargo Flows Shift and Supply Chain Risks Rise'. 20 December 2024. <https://www.edb.gov.sg/en/business-insights/insights/singapore-boosts-maritime-aviation-hub-role-as-cargo-flows-shift-and-supply-chain-risks-rise.html>.

Economic Development Board (EDB) Singapore. 'Singapore Ranks as World's 12th Tech City, with Room to Grow as Tech-Savvy Generation Enter Job Market'. 24 October 2022. <https://www.edb.gov.sg/en/business-insights/insights/singapore-ranks-as-world-s-12th-tech-city-with-room-to-grow-as-tech-savvy-generation-enter-job-market.html>.

Edelman, Eric S., David Manning, and Franklin C. Miller. 'NATO's Decision Process Has an Achilles' Heel'. *Atlantic Council*, 12 March 2024. <https://www.atlanticcouncil.org/blogs/new-atlanticist/natos-decision-process-has-an-achilles-heel/>.

ERR News. 'Police Apprehend Suspects in Cyberattacks against Estonia'. ERR News, 29 September 2020. <https://news.err.ee/1140977/police-apprehend-suspects-in-cyberattacks-against-estonia>.

ERR News. 'RIA: Estonia's State Institutions Hit by Largest Cyberattack to Date'. ERR, 12 March 2024. <https://news.err.ee/1609278921/ria-estonia-s-state-institutions-hit-by-largest-cyberattack-to-date>.

Erskine, Sasha. 'The EU Tiptoes into Cyber Sanctions Regimes'. Royal United Services Institute (RUSI), 12 August 2025. <https://www.rusi.orghttps://www.rusi.org>.

Espinosa, Victor I., and Antonia Pino. 'E-Government as a Development Strategy: The Case of Estonia.' *International Journal of Public Administration* 48, no. 2 (2025): 86–99. 182024438. <https://doi.org/10.1080/01900692.2024.2316128>.

Estonian Business and Innovation Agency. 'Data Embassy'. e-Estonia, 7 June 2024. <https://e-estonia.com/solutions/e-governance/data-embassy/>.

Estonian Business and Innovation Agency. 'e-Estonia Story'. e-Estonia. Accessed 2 August 2025. <https://e-estonia.com/story/>.

Estonian Business and Innovation Agency. 'X-Road'. e-Estonia, 10 June 2024. <https://e-estonia.com/solutions/interoperability-services/x-road/>.

Estonian Defence Forces. 'Estonian Defence Forces'. 30 July 2025. <https://mil.ee/en/defence-forces/>.

Estonian Defence League. 'Frequently Asked Questions - Cyber Unit'. Accessed 5 August 2025. <https://www.kaitseliit.ee/en/frequently-asked-questions>.

European External Action Service (EEAS). 'EU Imposes the First Ever Sanctions against Cyber-Attacks'. 30 July 2020. https://www.eeas.europa.eu/delegations/china/eu-imposes-first-ever-sanctions-against-cyber-attacks_en?s=166.

Fischerkeller, Michael P., and Richard J. Harknett. 'Deterrence Is Not a Credible Strategy for Cyberspace'. *Orbis* 61, no. 3 (2017): 381–93. <https://doi.org/10.1016/j.orbis.2017.05.003>.

Gao, Xinchuchu. 'Challenges and Opportunities: Estonia's Role in Shaping EU Cybersecurity Policy'. In *Small States in EU Policy-Making*, 1st edn, by Anna-Lena Högenauer and Matúš Mišík. Routledge, 2024. <https://doi.org/10.4324/9781003380641-12>.

Gold, Josh. 'How Estonia Uses Cybersecurity to Strengthen Its Position in NATO'. *ICDS*, 27 May 2019. <https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/>.

Government Communication Unit. 'Estonia Hosted the First-Ever Formal Meeting on Cybersecurity in the History of the UN Security Council'. Republic of Estonia - Government (Valitsus), 29 June 2021. <https://www.valitsus.ee/en/news/estonia-hosted-first-ever-formal-meeting-cybersecurity-history-un-security-council>.

Government of the Republic of Estonia. 'National Security Concept of Estonia'. February 2023. https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf.

Haffa, Robert P. 'The Future of Conventional Deterrence: Strategies for Great Power Competition'. *Strategic Studies Quarterly* 12, no. 4 (2018): 94–115.

Hanson, Fergus. 'Naming and Shaming the Unshameable'. *The Strategist*, 17 April 2018. <https://www.aspistrategist.org.au/naming-shaming-unshameable/>.

Harvard Ash Center. 'E-Stonia: One Small Country's Digital Government Is Having a Big Impact'. *Innovations in Government*, 15 April 2021. <https://medium.com/innovations-in-government/e-stonia-one-small-countrys-digital-government-is-having-a-big-impact-a33e30983c0b>.

Hey, Jeanne, ed. *Small States in World Politics : Explaining Foreign Policy Behavior*. Lynne Rienner, 2003. deakin.b2023628. <https://research.ebsco.com/linkprocessor/plink?id=cbcffc5a-30f1-3d14-b114-ddbd7ca7c137>.

Hurel, Louise Marie. 'What Singapore's First Public Cyber Attribution Tells Us'. Royal United Services Institute (RUSI), 30 July 2025. <https://www.rusi.org/explore-our-research/publications/commentary/what-singapores-first-public-cyber-attribution-tells-us>.

IMD World Digital Competitiveness Ranking 2024. Institute for Management Development, 2024. <https://imd.widen.net/s/xvhldkrrkw/20241111-wcc-digital-report-2024-wip>.

Infocomm Media Development Authority. 'Charting Green Growth for Data Centres in SG'. 30 May 2024. <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/charting-green-growth-for-data-centres-in-sg>.

Information System Authority (RIA). *Cyber Security in Estonia 2020*. Republic of Estonia, Information System Authority (RIA), 2020. <https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2020.pdf>.

Information System Authority (RIA). *Cyber Security in Estonia 2023*. Republic of Estonia, Information System Authority (RIA), 2023. <https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf>.

Information System Authority (RIA). *Cyber Security in Estonia 2025*. Republic of Estonia, Information System Authority (RIA), 2025. <https://ria.ee/sites/default/files/documents/2025-02/Cyber-security-in-Estonia-2025.pdf>.

Information System Authority (RIA). 'Monitoring Cyberspace and Impeding Incidents'. Republic of Estonia, Information System Authority (RIA). Accessed 5 August 2025. <https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee>.

Information System Authority (RIA). 'Prevention Efforts for All Generations'. Information System Authority (RIA). Accessed 24 August 2025. <https://www.ria.ee/en/prevention-efforts-all-generations>.

International Institute for Strategic Studies. *Chapter 5: "Estonia" — in Cyber Capabilities and National Power*. Volume 2. IISS Research Paper. International Institute for Strategic Studies, 2023. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_05-estonia.pdf.

International Institute for Strategic Studies. *Chapter 10: "Singapore" — in Cyber Capabilities and National Power*. Volume 2. IISS Research Paper. International Institute for Strategic Studies, 2023. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_10-singapore.pdf.

International Monetary Fund. 'World Economic Outlook (April 2025) - GDP, Current Prices'. Accessed 13 August 2025. <https://www.imf.org/external/datamapper/NGDPD@WEO/USA/CHN/EU>.

International Telecommunication Union (ITU). 'Global Cybersecurity Index 2024'. 1 June 2024. <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>.

Jayakumar, Sashi. 'Commentary: Singapore Is Going from Cybersecurity to Cybermaturity'. Channel News Asia, 5 June 2025. <https://www.channelnewsasia.com/commentary/cybersecurity-attack-scam-ransomware-hackers-ai-5165536>.

Josh Gold. 'Estonia as an international cybersecurity leader'. e-Estonia, 21 August 2019. <https://e-estonia.com/estonia-as-an-international-cybersecurity-leader/>.

Kennan, George F. 'Historical Documents - Office of the Historian'. U.S. Office of the Historian, 4 May 1948. <https://history.state.gov/historicaldocuments/frus1945-50Intel/d269>.

Koh, Sarah. 'Suspected Advanced Persistent Threat Attacks Must Be Reported under S'pore's Amended Cybersecurity Act'. *The Straits Times* (Singapore), 29 July 2025. <https://www.straitstimes.com/tech/suspected-advanced-attacks-must-be-reported-under-singapores-amended-cybersecurity-act>

Kok, Xinghui. 'China Denies Link to Espionage Group Accused of Attacking Singapore Critical Infrastructure'. China. *Reuters*, 21 July 2025. <https://www.reuters.com/world/china/china-denies-link-espionage-group-accused-attacking-singapore-critical-2025-07-21/>.

Kristiansen, Marius, and Njaal Hoem. 'Small Players in a Limitless Domain: Cyber Deterrence as Small State Strategy'. *Comparative Strategy* 41, no. 1 (2022): 19–31. <https://doi.org/10.1080/01495933.2021.2017740>.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. RAND Corporation, 2009. 304894. <https://research.ebsco.com/linkprocessor/plink?id=32d30978-3bb9-3fa2-be80-7e1256a68a1d>.

Lupel, Adam, and Lauri Mälksoo. *A Necessary Voice: Small States, International Law, and the UN Security Council*. International Peace Institute, 2019.

Lynch, Justin, and Emma Morrison. *Through AI-Enabled Detection and Attribution*. The Kissinger Center Papers. John Hopkins School of Advanced International Studies, 2023. <https://mediahost.sais-jhu.edu/saismedia/media/web/files/kissinger/deterrence-through-ai-enabled-detection-attribution-v2.pdf>.

Lynn, William F. III. 'Defending a New Domain - The Pentagon's Cyberstrategy'. *Foreign Affairs* 89, no. 5 (2010): 97–108. [edshol.hein.journals.fora89.79](https://www.jstor.org/stable/2574799).

Meer, Sico van der. 'Deterrence of Cyber-Attacks in International Relations: Denial, Retaliation and Signaling'. *International Affairs Forum* 2 (2017): 85–90.

Ministry of Defence. 'Digital and Intelligence Service Concludes Participation in Multinational Exercise Locked Shields 2025'. 11 May 2025. https://www.mindef.gov.sg/news-and-events/latest-releases/11may25_nr/.

Ministry of Defence. 'Fact Sheet: Defence Cyber Command and SAF C4 & Digitalisation Command'. 3 March 2025. https://www.mindef.gov.sg/news-and-events/latest-releases/03mar25_fs/.

Ministry of Defence. 'Fact Sheet: Digital Defence'. 15 February 2019. https://www.mindef.gov.sg/news-and-events/latest-releases/15feb19_fs/.

Ministry of Defence. 'Singapore's Digital and Intelligence Service Participates in Multilateral Cyber Defence Exercise'. 1 March 2025. https://www.mindef.gov.sg/news-and-events/latest-releases/1mar25_nr1/.

Ministry of Defence. 'Total Defence Strengthened with Addition of Digital Defence as the Sixth Pillar'. 15 February 2019. https://www.mindef.gov.sg/news-and-events/latest-releases/15feb19_nr/.

Ministry of Digital Development and Information. 'MDDI's Response to PQs on Impact of CrowdStrike Outage on SG Gov Services'. 7 August 2024. <https://www.mddi.gov.sg/newsroom/mddi-s-response-to-pqs-on-impact-of-crowdstrike-outage-on-sg-gov-services/>.

Ministry of Health. 'SingHealth's IT System Target of Cyberattack'. 20 July 2018. <https://www.moh.gov.sg/newsroom/singhealth-s-it-system-target-of-cyberattack/>.

NATO. 'Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021'. North Atlantic Treaty Organization (NATO), 14 June 2021. https://www.nato.int/cps/en/natohq/news_185000.htm.

NATO. 'Collective Defence and Article 5'. NATO, 4 July 2023. https://www.nato.int/cps/en/natohq/topics_110496.htm.

NATO Cooperative Cyber Defence Centre of Excellence. 'About Us'. Accessed 6 August 2025. <https://ccdcoe.org/about-us/>.

NATO Cooperative Cyber Defence Centre of Excellence. 'Locked Shields'. Accessed 6 August 2025. <https://ccdcoe.org/exercises/locked-shields/>.

NATO Strategic Communications Centre of Excellence. 'Hybrid Threats: 2007 Cyber Attacks on Estonia'. 6 June 2019. <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>.

NCSI. 'National Cyber Security Index: Ranking'. Accessed 17 September 2025. <https://ncsi.ega.ee/ncsi-index/?order=rank>.

Ng, Wei Kai. 'Singapore Cyber Defenders Fight Simulated Attacks on AI-Enabled Systems in 4-Day Exercise'. *The Straits Times* (Singapore), 15 November 2024. <https://www.straitstimes.com/singapore/singapore-cyber-defenders-fight-simulated-attacks-to-ai-enabled-systems-in-3-day-exercise>.

Nye, Joseph S. 'Deterrence and Dissuasion in Cyberspace'. *International Security* 41, no. 3 (2017): 44–71. https://doi.org/10.1162/isec_a_00266.

Oh, Lionel. 'Exploring Policy Conditions for Cyber Deterrence: A Case Study of Estonia'. *The Cornell International Affairs Review* XII, no. 2 (2019): 119–57.

Pavlova, Pavlina, and Christopher Painter. 'The UN's Permanent Process on Cybersecurity Faces an Uphill Battle'. *Lawfare*, Lawfare, 13 August 2025. <https://www.lawfaremedia.org/article/the-un-s-permanent-process-on-cybersecurity-faces-an-uphill-battle>.

Pedersen, Torbjørn. 'A Small State's Cyber Posture: Deterrence by Punishment and Beyond'. *Scandinavian Journal of Military Studies* 6, no. 1 (2023): 58–68. <https://doi.org/10.31374/sjms.191>.

Pernik, Piret. *Cyber Deterrence: A Case Study on Estonia's Policies and Practice*. No. 8. Hybrid CoE Paper. European Centre of Excellence for Countering Hybrid Threats, 2021. https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf.

Peters, Robert, Justin Anderson, and Harrison Menke. 'Deterrence in the 21st Century: Integrating Nuclear and Conventional Force'. *Strategic Studies Quarterly* 12, no. 4 (2018): 15–43.

Petra Holm. 'Estonia's approach to cyber security: a model for Europe'. e-Estonia, 19 March 2025. <https://e-estonia.com/estonias-cyber-security-model-for-europe/>.

'Press Release | Digital Transformation Accelerates, but Gaps Underscore Need for New Framework to Advance Use of Technologies in Governments'. *United Nations Sustainable Development*, 17 September 2024. <https://www.un.org/sustainabledevelopment/blog/2024/09/press-release-e-government-survey/>.

Prior, Tim. 'Resilience: The "Fifth Wave" in the Evolution of Deterrence'. In *Strategic Trends 2018: Key Developments in Global Affairs*. Centre for Security Studies - ETH Zurich, 2018. https://www.researchgate.net/publication/325735191_Resilience_The_'Fifth_Wave'_in_the_Evolution_of_Deterrence.

Public Relations Department. 'Estonia Names Russia's Military Intelligence in a First-Ever Attribution of Cyberattacks'. Republic of Estonia, Ministry of Foreign Affairs (Välisministeerium), 5 September 2024. <https://vm.ee/en/news/estonia-names-russias-military-intelligence-first-ever-attribution-cyberattacks>.

Republic of Estonia - Ministry of Foreign Affairs (Välisministeerium). 'Cybersecurity Cooperation – Regional Activities'. Accessed 7 August 2025. <https://vm.ee/en/activity/digital-and-cyber-diplomacy/cybersecurity-cooperation>.

Republic of Estonia, Information System Authority (RIA). *Cybersecurity Strategy 2024–2030: Cyber-Conscious Estonia*. Republic of Estonia, Information System Authority (RIA), 2024. https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf.

Republic of Estonia, Information System Authority (RIA). 'Situation in the Cyberspace'. Accessed 7 August 2025. <https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/situation-cyberspace>.

Republic of Estonia, Information System Authority (RIA). 'Tasks and Structure of the Authority'. Accessed 5 August 2025. <https://www.ria.ee/en/authority-news-and-contact/authority-and-management/tasks-and-structure-authority>.

Riigi Teataja. 'Penal Code'. Accessed 24 August 2025. <https://www.riigiteataja.ee/en/eli/522012015002/consolide>.

Sandra Kamilova. 'Foreign Minister Mikser Condemns Russia for NotPetya Attacks against Ukraine'. Välisministeerium, 15 February 2018. <https://vm.ee/en/news/foreign-minister-mikser-condemns-notpetya-attacks-against-ukraine>.

SCHAAKE, Marietje. 'Question for Written Answer E-001005/2018 to the Council: "Attribution of the NotPetya Attack"'. European Parliament, 19 February 2018. https://www.europarl.europa.eu/doceo/document/E-8-2018-001005_EN.html.

Schelling, Thomas C., 1921-2016, author., and Anne-Marie Slaughter. *Arms and Influence / by Thomas C. Schelling ; with a New Introduction by Anne-Marie Slaughter*. Veritas paperback edition. Yale University Press, 2020. deakin.b4348287. <https://research.ebsco.com/linkprocessor/plink?id=aa500363-cb53-37a5-a63a-9b513c836277>.

Shanmugam, K. 'Opening Speech by Mr K Shanmugam, Coordinating Minister for National Security and Minister for Home Affairs, at CSA's 10th Anniversary Dinner'. Cyber Security Agency of Singapore, 19 July 2025. <https://www.csa.gov.sg/news-events/speeches/opening-speech-by-mr-k-shanmugam--coordinating-minister-for-national-security-and-minister-for-home-affairs--at-csa-10th-anniversary-dinner/>.

Siers, Rhea. 'Cybersecurity'. In *Security Studies*, 4th edn, by Paul D Williams and Matt McDonald. Routledge, 2023. <https://doi.org/10.4324/9781003247821-44>.

Singapore Ministry of Digital Development and Information. *Smart Nation 2.0 - A Thriving Digital Future for All*. MDDI, 2024. <https://file.go.gov.sg/smartnation2-report.pdf>.

Singapore Public Sector Outcomes Review 2024. 'Cybersecurity and Digital Resilience'. 8 November 2024. <https://spor.performancereports.gov.sg/businesses/strong-and-resilient-economy/data-and-cyber-security/>.

Singapore Statutes Online. 'Computer Misuse Act 1993 (2020 Revised Edition)'. Accessed 18 August 2025. <https://sso.agc.gov.sg/Act/CMA1993?WholeDoc>.

Singapore Statutes Online. 'Cybersecurity Act 2018 (2020 Revised Edition)'. Accessed 18 August 2025. <https://sso.agc.gov.sg/Act/CA2018?WholeDoc=1>.

Snyder, Glenn H. (Glenn Herald), 1924-2013. *Deterrence and Defense: Toward a Theory of National Security*. Princeton University Press, 1961. deakin.b3376548. <https://research.ebsco.com/linkprocessor/plink?id=5bd036b2-3de4-340b-80f3-96b7e11d2605>.

Stefan Soesanto. 'Inside the Fourth EU Cyber Sanctions Package'. Lawfare, 23 March 2025. <https://www.lawfaremedia.org/article/inside-the-fourth-eu-cyber-sanctions-package>.

Supreme Headquarters Allied Powers Europe (SHAPE). 'Exercise Cyber Coalition 2020'. 14 November 2020. <https://shape.nato.int/news-archive/2020/exercise-cyber-coalition-2020.aspx>.

Tan, Eugene E.G. 'A Small State Perspective on the Evolving Nature of Cyber Conflict : Lessons from Singapore'. *PRISM* 8, no. 3 (2019): 158–71.

Tham, Davina. 'Singapore Actively Dealing with Ongoing Cyberattack on Critical Infrastructure: Shanmugam'. Channel News Asia, 18 July 2025. <https://www.channelnewsasia.com/singapore/unc3886-cyber-security-threat-actor-attack-singapore-5245791>.

The Asian Banker. 'Business Continuity Exercise to Bolster Singapore Financial Resilience'. 17 September 2025. <https://www.theasianbanker.com/press-releases/business-continuity-exercise-to-bolster-singapore-financial-resilience>.

The World Factbook. 'Country Comparisons - Population'. Accessed 17 September 2025. <https://www.cia.gov/the-world-factbook/field/population/country-comparison/>.

Thorhallsson, Baldur, and Sverrir Steinsson. 'Chapter 2 - A Theory of Shelter'. In *Small States and Shelter Theory: Iceland's External Affairs / Edited by Baldur Thorhallsson.*, 1st. Routledge, 2018. deakin.b4211480. <https://research.ebsco.com/linkprocessor/plink?id=91f12d98-5bf8-3275-a81a-3edd7cc7db17>.

UN Office for Disarmament Affairs (UNODA). 'Open-Ended Working Group on Information and Communication Technologies (2021)'. Accessed 8 August 2025. <https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021>.

United Nations Office for Disarmament Affairs (UNODA). 'Developments in the Field of Information and Telecommunications in the Context of International Security'. Accessed 8 August 2025. <https://disarmament.unoda.org/ict-security/>.

United Nations Secretariat. *Compendium of Statements in Explanation of Position on the Adoption of the Final Report of the Open-Ended Working Group*. A/80/257. United Nations, 2025. <https://docs.un.org/en/A/AC.292/2025/INF/5>.

United Nations Secretariat. *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. A/76/50. United Nations, 2021. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

United States Department of Justice - Archives. 'Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government'. 5 September 2024. <https://www.justice.gov/archives/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government>.

U.S. Cyber Command. 'Hunt Forward Estonia: Estonia, US Strengthen Partnership in Cyber Domain with Joint Operation'. 3 December 2020. <https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi>.

Vaicekauskaitė, Živilė Marija. 'Security Strategies of Small States in a Changing World'. *Journal on Baltic Security* 3, no. 2 (2017): 7–15. <https://doi.org/10.1515/jobs-2017-0006>.

Valeriano, Brandon, and Benjamin Jensen. 'Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report'. *13th International Conference on Cyber Conflict: Going Viral – Proceedings*, NATO Cooperative Cyber Defence Centre of Excellence, 2021, 189–214. <https://ccdcoe.org/uploads/2018/10/Art-01-Achieving-Cyberdeterrence-and-the-Ability-of-Small-States-to-Hold-Large-States-at-Risk.pdf>.

Väljataga, Ann. 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly'. NATO Cooperative Cyber Defence Centre of

Excellence. Accessed 2 September 2025. <https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/>.

Ventura, Luca. 'Richest Countries in the World 2025'. *Global Finance Magazine*, 3 September 2025. <https://gfmag.com/data/richest-countries-in-the-world/>.

Willett, Marcus. 'Lessons of the SolarWinds Hack.' *Survival* (0039-6338) 63, no. 2 (2021): 7–26. 157382767. <https://doi.org/10.1080/00396338.2021.1906001>.

World Bank. 'Overview'. Text/HTML. Accessed 16 September 2025. <https://www.worldbank.org/en/country/smallstates/overview>.

Yap, Brian. 'Data Centres: The New Boom'. *Law.Asia*, 3 September 2025. <https://law.asia/asia/data-centre-investment-boom-asia-2025/>.

Yeo, Mike. 'SAF's Digital Service Inaugurates Two New Commands to Sharpen Cyber-Security Edge'. *The Straits Times* (Singapore), 18 March 2025. <https://www.straitstimes.com/singapore/safs-digital-service-inaugurates-two-new-commands-to-sharpen-cybersecurity-edge>.



ADF
Australian Defence Force

Siloed Systems, Shared Stakes: Keeping the Nation's Engine from Stalling

William Nichols



About the Author



Will Nichols is a senior public servant with nearly two decades of experience across multiple Commonwealth portfolios. In 2025, he was selected to attend the Defence and Strategic Studies Course (DSSC) at the Australian War College, an appointment reserved for leaders with the potential to influence defence and national security policy. During the course, Will focused on civilian–military approaches to complex crises and graduated with a Master of National Security and Strategy from Deakin University. He was awarded the Deakin Academic Principles Research Prize for his thesis. Will has also received a Gold Commendation for his leadership in developing the Defence Future Energy Strategy, the Clean Energy Acceleration Plan, and for his work establishing and advancing the National

Fuel Council. Following DSSC, he continues to contribute to Australia's national security priorities as a Director in Defence's Security and Estate Group.

Summary

Australia's reliance on imported liquid fuels is one of the nation's most profound structural risks, reducing resilience, hindering Defence readiness, and threatening economic stability during crises or disruptions. Fuel underpins sectors such as aviation, freight, agriculture, mining, emergency services, and Defence—areas lacking scalable alternatives—making national capability vulnerable to failures. Decades of deregulation have entrenched cost-driven policies, resulting in lower stockpiles, reduced refining capacity, and greater dependence on imports, which create a fragile system with limited redundancy or sovereign control. The 2019 Liquid Fuel Security Review formalised this vulnerability by prioritising efficiency over resilience, sidelining Defence needs, and failing to prepare for long-term disruptions. Meanwhile, billions committed to Defence capabilities face paralysis if access to liquid fuel is not assured. Finland and Japan demonstrate that fuel resilience is achievable when regarded as a sovereign capability, built through robust legal frameworks, strong institutions, and public acceptance of higher costs. For Australia, developing this resilience also entails climate responsibility, with regional partners assessing the country's commitment to climate action through its energy policies. A sovereign, low-carbon liquid fuels industry is thus the only viable option to expand refining capacity, reconcile security with climate commitments, and ensure long-term national preparedness.

Introduction

Australia's national security, economic stability, and crisis response capacity are reliant upon secure access to liquid fuels, yet this strategic foundation is critically exposed. Over the past decade, intensifying geopolitical competition throughout the Indo-Pacific, the closure of domestic refineries,¹ mounting pressure on maritime chokepoints² and the disruptive dynamics of a global energy transition have magnified this vulnerability. Despite these converging risks, Australia's public and political discourse on energy has remained preoccupied with emissions reduction and affordability, thereby marginalising systemic fuel supply vulnerabilities and preventing strategic planning to address them.³ This neglect is compounded by energy policymaking that isolates economic, security, and environmental considerations. To this end, the central research question guiding this thesis is: How can Australia address its fuel vulnerability while supporting national security, economic continuity, and environmental goals? Four subsidiary questions direct the inquiry:

- Why do liquid fuels remain essential to Australia's national capability?
- What structural and institutional factors have allowed this vulnerability to persist despite repeated warnings?
- What can be learned from international approaches to treating liquid fuels as a sovereign capability embedded in national planning?
- How can low-carbon liquid fuels (LCLFs) contribute to a more resilient and strategically aligned national fuel posture?

Although Australia's dependence on imported liquid fuels is not a new concern, it has grown more problematic over time. As of 2023, Australia imported more than 90 per cent of its liquid fuels, mainly from a few refineries in North and Southeast Asia, with only minimal onshore stockpiles to buffer potential supply shocks.⁴ Almost all shipments pass through contested sea lines of communication, including chokepoints that are vulnerable to geopolitical tensions, congestion, and disruption.⁵ Despite this exposure, Australia continues to operate a "just-in-time" supply model, even though its refining

¹ Oil & Gas Journal, "BP to close Kwinana oil refinery," 2020, <https://www.ogj.com/refining-processing/refining/operations/article/14186463/bp-to-close>

² Observer Research Foundation, "Securing Sea Lines of Communication in Asia," October 15, 2024, <https://www.orfonline.org/research/securing-sea-lines-of-communication-in-asia>

³ "Falling well short: FOI documents reveal shocking state of nation's fuel security preparedness," Defence Connect, January 14, 2025, <https://www.defenceconnect.com.au/geopolitics-and-policy/15357-falling-well-short-foi-documents-reveal-shocking-state-of-nations-fuel-security-preparedness>.

⁴ Matt Grudnoff, *Over a barrel: A review of Australia's liquid fuel security*, Discussion Paper (Canberra, ACT: The Australia Institute, April 2022), https://australiainstitute.org.au/wp-content/uploads/2022/04/P1036-Over-a-barrel_liquid-fuel-security-WEB.pdf.

⁵ "A Conflict in the Pacific Could Prompt a Fight Over the Strait of Malacca," *The Maritime Executive*, July 2, 2023, <https://maritime-executive.com/editorials/a-conflict-in-pacific-could-prompt-a-fight-over-strait-of-malacca>.

capacity has shrunk to just two operational facilities.⁶

The 2019 Liquid Fuel Security Review identified these vulnerabilities and proposed modest interventions, but progress has been slow.⁷ The Fuel Security Act 2021, enacted in response, established new policy measures, including a Minimum Stockholding Obligation and subsidies for the last two refineries to ensure they remain operational until 2027.⁸ However, analysts warn that Australia still does not meet International Energy Agency stockholding benchmarks and remains vulnerable to external shocks.⁹ The system continues to rely on fragile assumptions about the stability of global markets, even as the Indo-Pacific region becomes more contested.¹⁰

This vulnerability is exacerbated by fragmented policymaking, where economic, security, and environmental portfolios pursue diverging objectives instead of operating within a cohesive framework.¹¹ Defence has historically assumed that the energy portfolio, responsible for national fuel security, would safeguard military surge demands.¹² Conversely, energy policymakers have long prioritised price stability and minimal market intervention, encouraging suppliers to maintain the leanest possible inventories. This efficiency approach has created a fuel system optimised for cost but dangerously deficient in resilience, leaving critical sectors vulnerable to cascading risks in the event of a disruption.¹³ At the same time, the energy transition has fostered a flawed assumption that liquid fuel demand will soon decrease, despite forecasts indicating sustained long-term growth.¹⁴ Demand is projected to rise significantly across the economy, particularly in heavy industries such as transportation, aviation, agriculture, and Defence. The result is a significant blind spot in national capability, where Australia's fuel vulnerability undermines both military preparedness and

⁶ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report* (Canberra, ACT: DCCEEW, April 2019), <https://www.dcceew.gov.au/sites/default/files/documents/liquid-fuel-security-review-interim-report.pdf>.

⁷ Ibid.

⁸ Australian Parliament House, *Fuel Security Bill 2021*, Bills Digest No. 81, 2020–21 (Canberra, ACT: Parliamentary Library, June 17, 2021), https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/FlagPost/2021/June/Fuel_Security_Bill_2021.

⁹ “Australia's fuel insecurity is not hypothetical,” *The Strategist*, August 2, 2023, <https://www.aspistrategist.org.au/australias-fuel-insecurity-is-not-hypothetical/>.

¹⁰ Ibid.

¹¹ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Final Report* (Canberra, ACT: DCCEEW, October 2020), <https://www.dcceew.gov.au/sites/default/files/documents/72895-1.pdf>.

¹² Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

¹³ Strati Pantges, “Fuel Security and Minimum Stockholding Obligations: What it means for you and your business,” McCullough Robertson, September 30, 2024, <https://mccullough.com.au/2024/09/30/fuel-security-and-minimum-stockholding-obligations-what-it-means-for-you-and-your-business/>.

¹⁴ Clean Energy Finance Corporation and Deloitte, *Refined Ambitions: Exploring Australia's low carbon liquid fuel potential* (Sydney, NSW: CEFC, July 2025), 11–15, <https://www.cefc.com.au/media/jh3gvm14/refined-ambitions-exploring-australia-s-low-carbon-liquid-fuel-potential.pdf>.

economic stability.¹⁵

The strategic consequences of this disconnection are clear. The 2019 Liquid Fuel Security Review identified systemic risks but opposed structural reform, warning instead that higher prices would burden consumers.¹⁶ This dependence on market logic delayed investment in sovereign refining, storage, and distribution infrastructure. Meanwhile, the 2023 Defence Strategic Review called for the adoption of a deterrence-by-denial strategy, which requires long-range strike systems, littoral manoeuvre forces, and fortified northern bases.¹⁷ All of these capabilities rely heavily on fuel, requiring constant access to diesel and jet fuel, particularly in Northern Australia, to sustain minimum operational capacity. However, billions are being invested in these new military capabilities without ensuring the fuel networks that support them.¹⁸

Australia's strategic credibility, therefore, relies on integrating liquid fuel resilience into national planning, alongside defence modernisation and the energy transition.¹⁹ The gap between Defence's fuel-intensive denial strategy and the market-based fuel supply approach reveals a structural flaw, where neither resilience nor transition pathways are sufficiently planned.²⁰ This thesis argues that Australia's market-led approach has created systemic vulnerabilities that have been worsened by fragmented policymaking.²¹ Tackling this fragmentation will require a unified strategy that considers Australia's fuel security a vital component of its national capability.

Methodology

This thesis employs policy and discourse analysis, supported by comparative case studies and descriptive data, to interrogate Australia's structural fuel vulnerabilities and the policy frameworks that have shaped them. The analysis draws on government legislation, strategy reviews, institutional submissions, and industry reports, focusing on how Australia's fuel security has been framed, understood, and inadequately addressed by its policies. The thesis evaluates how vulnerabilities have been repeatedly recognised yet left unresolved, highlighting the institutional gaps that continue to weaken Australia's national resilience.

Comparative case studies of Finland and Japan offer practical insights into how fuel can be institutionalised as a sovereign capability. The actions of these countries demonstrate the importance of legal mandates, empowered institutions, and civil–military planning in embedding fuel planning within their national resilience frameworks.

¹⁵ Ben Garside, *The ADF and its future energy requirements*, Special Report Issue 187 (Canberra, ACT: Australian Strategic Policy Institute, June 2022), 15–16, 17–18, 23–25, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-06/SR%20187%20The%20ADF%20and%20its%20future%20energy%20requirements.pdf?VersionId=NXnGVnZgWDv7_GOm7vdezIVTj_aNxTkT3.

¹⁶ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report* (Canberra: DCCEEW, 2019), 4, 6–7, 10.

¹⁷ Department of Defence. *Defence Strategic Review 2023: National Defence*. Canberra: Commonwealth of Australia, 2023, 18–19, 55–59, <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>

¹⁸ Garside, *The ADF and its future energy requirements*.

¹⁹ Clean Energy Finance Corporation and Deloitte, *Refined Ambitions*, 8, 14–15, 17.

²⁰ Garside, *The ADF and its future energy requirements*, 4–6, 13–15, 16–18.

²¹ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*, 10.

Their experiences offer relevant lessons for Australia, not as models to replicate, but as reference points for understanding how other states have integrated this fuel planning into broader strategies of national preparedness.

The analysis also examines the role of LCLFs within Australia's policy framework. Instead of a technical evaluation, it concentrates on their potential as a strategically aligned policy tool capable of reconciling both national resilience and decarbonisation. This approach enables a systematic assessment of how Australia can balance its security, economic, and climate goals in developing a cohesive national fuel strategy to address one of its most critical vulnerabilities.

Significance

The significance of this research lies in redefining national fuel resilience as a strategic capability rather than just a narrow market issue. By demonstrating that liquid fuels support economic stability, emergency response, and military capacity, the thesis shows that Australia's fuel security is fundamentally linked to national resilience. The ongoing reliance on fragile international supply chains makes Australia vulnerable to coercion and disruptions, while its fragmented policy approach has hampered coordinated planning.

This thesis aims to address shortcomings in the current body of literature on Australian fuel strategy, which remains fragmented. It consolidates previously isolated fields (security, energy policy, and climate transition) to tackle a vital national blind spot. Existing research on Australian energy needs has mainly concentrated on emissions reduction, while security studies have focused on military capability in isolation. Few works examine how the energy transition intersects with national preparedness and resilience. By connecting these areas, the thesis closes a significant gap in understanding how Australia can reduce this systemic vulnerability while advancing security, economic, and environmental goals simultaneously.

Structure

The thesis presents a cumulative argument across five chapters, moving from a structural diagnosis to coherent reforms, and ending with a conclusion that reaffirms the central argument. Chapter One traces how efficiency-focused reforms dismantled resilience, leading to the collapse of refining capacity, a thinning of storage, and the exposure of distribution systems, thereby embedding systemic vulnerability within Australia's national fuel system. Building on this, Chapter Two demonstrates why liquid fuels remain essential to sovereign capability, analysing cascading dependencies across freight, aviation, mining, agriculture, emergency services, and Defence without scalable substitutes. Chapter Three critiques the government's Liquid Fuel Security Review and the subsequent policy and legislative package, illustrating how efficiency bias and the exclusion of Defence's requirements limited their strategic adequacy.

In contrast, Chapter Four explores the cases of Finland and Japan, illustrating how legal mandates, empowered institutions, and civil–military planning integrate fuel resilience as a national capability. Finally, Chapter Five assesses low-carbon liquid fuels as a strategic opportunity, arguing that they offer a means to align resilience with decarbonisation by providing compatibility, sovereign production potential, and measurable emissions reductions. The conclusion summarises these findings, arguing that fragmented policymaking has reinforced Australia's fuel vulnerability and that only

a cohesive strategy, supported by measures such as governance reform, mandated stockpiling, and investment in LCLFs, can redefine the importance of fuel as a core aspect of Australia's sovereign capability.

Chapter 1: How Market Logic Undermined Resilience

The overall condition of Australia's national fuel network reflects decades of policies favouring efficiency and integration with global markets.²² Yet, this legacy has left the country dangerously exposed to modern security threats. The current literature shows how long-standing policies favouring deregulation and privatisation built a market-driven system centred on cost, while systematically diminishing national resilience and preparedness.²³ Building on these findings, this chapter examines the structural and institutional roots of Australia's fragility, highlighting the efficiency-oriented decisions that have created enduring weaknesses within the national fuel system.

1.1 Sovereign Production to Import Dependency: The Dismantling of Domestic Refining

This fragility became most apparent with the decline of Australia's domestic refining industry. Privatisation and deregulation reduced government involvement just as larger, more efficient Asian refineries undercut local production in terms of cost.²⁴ Rather than being protected as a strategic asset, Australia's refineries were left to compete in global markets where scale dictated survival. As a result, refinery closures accelerated, and the national system grew increasingly dependent on imported fuels transported through extensive maritime supply chains.²⁵ These arrangements were adequate during periods of regional stability, but now conceal significant risks in a contested strategic environment. Despite repeated assessments warning of supply shortfalls, governance over the national fuel system remains fragmented, reactive, and insufficiently prepared for sustained or deliberate disruption.²⁶

Historically, Australia regarded fuel as a strategic resource, particularly during periods of threat, investing in domestic refining, stockpiling, and developing planning systems to ensure a stable supply under stress.²⁷ During World War II and the oil shocks of the

²² Wilson Beaver, "When the tank's empty: Australia's impoverished energy security," *The Interpreter* (Lowy Institute, June 21, 2022), <https://www.lowyinstitute.org/the-interpreter/when-tank-s-empty-australia-s-impoverished-energy-security>.

²³ John Blackburn, *Australia's Liquid Fuel Security* (Report for NRMA Motoring and Services, February 2013), 3–6, 11–12, 17–19, <https://www.aph.gov.au/DocumentStore.ashx?id=86e8dfbc-1467-47fe-ad1e-bc635407ecf8&subId=301736>.

²⁴ Australian Institute of Petroleum, *Report on Australia's oil refinery industry*, Submission to the House of Representatives Standing Committee on Economics (Melbourne, VIC: AIP, September 2017), 14–15, <https://www.aip.com.au/sites/default/files/download-files/2017-09/APH%20Economics%20Committee%20Report%20-%20Oil%20Refining%20Industry.pdf>.

²⁵ Rob Dossor, "Australian oil refineries and fuel security," *FlagPost* (blog), Parliamentary Library, Parliament of Australia, December 10, 2020, https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/FlagPost/2020/December/Oil_refineries_and_fuel_security.

²⁶ Tom Swann, "Submission: Interim Report on the Liquid Fuel Security Review" (The Australia Institute, July 2019), 1–4, https://australiainstitute.org.au/wp-content/uploads/2020/12/P739-Liquid-Fuel-Security-Submission-WEB_0.pdf.

²⁷ John Blackburn AO, "Australia's Liquid Fuel Security - A Report for NRMA Motoring and Services" (Report for NRMA Motoring and Services, 28 February

1970s, there were state-led efforts to build resilience, recognising that market supply could not be assured in crises.²⁸ This approach demonstrated that Australia was once capable of acting decisively when the risks were evident. Nevertheless, that memory has faded and capacity has declined over the course of decades of peace, liberalisation, and fiscal restraint.²⁹ Strategic planning for fuel disruptions has diminished as policymakers now increasingly rely on global markets, eroding the institutional safeguards that once supported national preparedness and self-reliance.³⁰

The most noticeable consequence of this policy change was the collapse of Australia's domestic refining industry, which was once considered vital to the country's sovereignty and adaptability. Seven refineries were operational in 2000; however, by 2021, only two remained, both of which were dependent on government subsidies and at risk of closure in the future without ongoing financial support.³¹ Most decommissioned refineries were converted into import terminals, creating a structural reliance on overseas production and diminishing Australia's ability to control the type, timing, or origin of the fuels supplied into the country.³² This shift confined Australia to long maritime supply chains, reducing sovereign control and its capacity to reprocess crude oil during a supply shortage.³³

1.2 Supply and Storage Vulnerabilities

Today, over 90 per cent of Australia's diesel and jet fuel is transported by sea, much of it originating from Asia and passing through maritime chokepoints that are susceptible to disruption.³⁴ Key shipping routes, including the Strait of Malacca, the South China Sea, and the Lombok Strait, are becoming increasingly congested, contested, and prone to geopolitical pressure, blockade, or conflict.³⁵ These maritime routes are also increasingly being exposed to piracy, cyber interference, and sabotage, all of which could delay or obstruct fuel shipments without resorting to conventional military conflict.³⁶ Australia's fuel security now depends on the unimpeded passage of vessels

2013), 17, <https://www.aph.gov.au/DocumentStore.ashx?id=86e8dfbc-1467-47fe-ad1e-bc635407ecf8&subId=301736>.

²⁸ "Chapter 4. Threats to Australia's liquid fuel security," Parliament of Australia, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Rural_and_Regional_Affairs_and_Transport/Transport_energy_resilience/Report/c04.

²⁹ John Blackburn AO, "Australia's Liquid Fuel Security - A Report for NRMA Motoring and Services," 17.

³⁰ "Chapter 4. Threats to Australia's liquid fuel security"; Department of the Environment and Energy, *Liquid Fuel Security Review—Final Report* (Commonwealth of Australia, October 2020), <https://www.dcceew.gov.au/sites/default/files/documents/72895-2.pdf>, 3.

³¹ "Oil refineries and fuel security," Parliamentary Library, Parliament of Australia, https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/FlagPost/2020/December/Oil_refineries_and_fuel_security; Department of the Environment and Energy, *Liquid Fuel Security Review—Final Report* (Commonwealth of Australia, October 2020), <https://www.dcceew.gov.au/sites/default/files/documents/72895-2.pdf>.

³² Dossor, "Oil refineries and fuel security"; Department of the Environment and Energy, *Liquid Fuel Security Review—Final Report*.

³³ Blackburn, "Australia's Liquid Fuel Security," 17.

³⁴ *Ibid.*

³⁵ "Chapter 4. Threats to Australia's liquid fuel security."

³⁶ Raelene Lockhorst, "The urgent need for a strategic overhaul in Australia's Defence approach to fuel resilience," *The Strategist (ASPI)*, 19 September 2024,

through these delicate corridors, an assumption that cannot be assured, particularly during times of crisis or hostility.³⁷

Australia's onshore fuel storage is limited, typically covering only 19 days of diesel and 14 days of jet fuel at normal consumption levels, which is well below international standards.³⁸ This falls significantly short of the International Energy Agency's 90-day stockholding requirement, which Australia only meets through offshore "ticket" arrangements that provide no physical redundancy.³⁹ The scarcity results from decades of market-led just-in-time logistics, which optimise commercial efficiency and eliminate any redundancy needed to withstand supply shocks or support surge requirements during national emergencies.⁴⁰ Most storage infrastructure is privately owned and commercially managed, with facilities designed for stock turnover rather than buffering.



Image: Darwin's East Arm fuel tank farm, May 2007: [Ken Hodge/Flora](#)

<https://www.aspistrategist.org.au/the-urgent-need-for-a-strategic-overhaul-in-australias-defence-approach-to-fuel-resilience/>.

³⁷ John Blackburn AO, "Australia's Liquid Fuel Security - A Report for NRMA Motoring and Services," 17.

³⁸ Rod Campbell, "Fuel security in Australia and the International Energy Agency's 10-point plan," *The Australia Institute*, 1 October 2024, 2, <https://australiainstitute.org.au/report/fuel-security-in-australia-and-the-international-energy-agencys-10-point-plan/>.

³⁹ "IEA Programme and Treaty," Department of Climate Change, Energy, the Environment and Water, <https://www.dcceew.gov.au/energy/international-activity/iea-program-treaty>; John Blackburn AO, "Australia's Liquid Fuel Security - A Report for NRMA Motoring and Services", 5.

⁴⁰ Nicholas Floyd, "Just in Time: Logistics and Legislative Preparedness in Strategic Competition," *The Cove*, October 21, 2021, <https://cove.army.gov.au/article/just-time-logistics-and-legislative-preparedness-strategic-competition>.

Consequently, there is no obligation to serve national interests during a crisis.⁴¹ In the event of a significant disruption, this lean system lacks strategic depth; stocks in key ports and cities could be depleted within days if maritime routes or key import terminals are disrupted.⁴²

1.3 Fragmented Governance and the Failure of Market Logic

Responsibility for liquid fuel resilience in Australia is spread across various departments and jurisdictions, with no singular authority managing strategy or investment.⁴³ Defence assumes access will continue where needed; energy departments focus on maintaining just-in-time supplies and decarbonisation, as evidenced by their key policies; and emergency agencies prepare for the consequences of localised disruptions rather than developing mitigation measures or planning for long-term national fuel resilience.⁴⁴ The National Oil Supply Emergencies Committee (NOSEC) facilitates coordination during disruptions but lacks the mandate, funding, or statutory authority to lead national infrastructure planning or reserve development.⁴⁵ Repeated reviews have identified these institutionalised gaps, yet no agency has been empowered or resourced to oversee a comprehensive approach to strategic planning to address them.⁴⁶ This is most notable in the Liquid Fuel Security Review, where the report explicitly excludes Defence from the sectors examined as a core pillar of its analysis.

Market mechanisms have failed to provide the required storage, essential distribution infrastructure, or refining capacity needed for a resilient system because resilience does not generate a viable commercial return.⁴⁷ Private firms are designed to optimise efficiency, not to absorb risk; holding surplus fuel or investing in backup infrastructure diminishes profit without offering immediate economic gain.⁴⁸ The closure of refineries, limited surge capacity, and minimal onshore storage all reflect this logic, where national vulnerability arises from short-term commercial choices.⁴⁹ Without clear mandates or government-backed financial incentives, the industry will not develop the necessary strategic reserves or infrastructure, leaving Australia exposed to risks that the market cannot adequately manage.⁵⁰

Australia's fuel distribution network was designed for efficiency under normal conditions, not for resilience during crises or extended regional or national fuel shortages.⁵¹ Refined fuel enters through a limited number of ports in Darwin (NT), Kwinana (WA), Botany (NSW), Geelong (VIC), and Brisbane (QLD), creating a concentration risk and reducing

⁴¹ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

⁴² Swann, "Submission: Interim Report," 1–2.

⁴³ Blackburn, "Australia's Liquid Fuel Security," 17, 21.

⁴⁴ Lockhorst, "The urgent need for a strategic overhaul."

⁴⁵ Blackburn, "Australia's Liquid Fuel Security," 17, 21.

⁴⁶ Blackburn, "Australia's Liquid Fuel Security," 17, 21.

⁴⁷ Campbell, "Fuel security in Australia."

⁴⁸ John Blackburn AO, "Australia's Liquid Fuel Security: A Report for NRMA Motoring and Services" (Engineers Australia, February 2013), <https://www.aph.gov.au/DocumentStore.ashx?id=677ff8dd-ce35-40ee-9af8-bfec1e43d125&subId=301736>.

⁴⁹ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Final Report*.

⁵⁰ Campbell, "Fuel security in Australia."

⁵¹ Blackburn, "Australia's Liquid Fuel Security."

flexibility in the event of disruption.⁵² A single cyberattack, port closure, or industrial dispute at one of these hubs could immediately disrupt supply to multiple regions with no quick alternatives.⁵³ Inland distribution relies on a limited number of pipelines, road tankers, and rail routes, with fuel transported by rail from Brisbane, Kwinana, and Darwin to specific regional centres. Most regional towns, mining centres, and supply corridors rely on single-route delivery chains, with no capability to reroute fuel in the event of a disruption.⁵⁴ There is no national system to coordinate surge logistics or rerouting capacity across jurisdictions during sustained or widespread supply shortfalls.⁵⁵

1.4 Strategic Consequences for National Capability

Australia's national capacity relies on continuous fuel access, as any failure in import, storage, or distribution could quickly undermine response, mobility, and economic stability.⁵⁶ As previously emphasised, critical sectors including freight, emergency services, agriculture, aviation, and defence have no feasible energy alternatives, making fuel availability a vital factor for crisis stability and national resilience.⁵⁷ In a prolonged disruption, cascading failures would degrade logistics, halt supplies, and cause food and medical supply chains to break down.⁵⁸ At the same time, essential services decline without the fuel necessary to sustain operations.⁵⁹ The strategic implication is clear: without reliable fuel access, Australia cannot ensure domestic stability, economic continuity, or national defence in a contested environment.⁶⁰

Australia lacks the sovereign capacity to withstand major fuel disruptions, risking cascading effects across national defence, critical services, and key economic sectors.⁶¹ Even a brief interruption would destabilise the economy, while a prolonged disruption would weaken national resilience, hinder recovery, and leave Australia vulnerable to coercion or strategic isolation.⁶² The literature has shown that this vulnerability is deeply rooted and exposed through weaknesses in supply, storage, distribution, and institutional coordination.⁶³ This interdependence between secure access to liquid fuels and national resilience underscores that the risks discussed here are not theoretical possibilities, but real pressures that can influence Australia's ability to act in an increasingly contested strategic environment.

⁵² Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*, 21.

⁵³ Lockhorst, "The urgent need for a strategic overhaul."

⁵⁴ Blackburn, "Australia's Liquid Fuel Security."

⁵⁵ Department of the Environment and Energy, *Liquid Fuel Security Review—Final Report*.

⁵⁶ Lockhorst, "The urgent need for a strategic overhaul."

⁵⁷ *Ibid.*

⁵⁸ Blackburn, "Australia's Liquid Fuel Security."

⁵⁹ *Ibid.*

⁶⁰ *Ibid.*

⁶¹ Department of the Environment and Energy, *Liquid Fuel Security Review—Final Report*.

⁶² Lockhorst, "The urgent need for a strategic overhaul."

⁶³ Blackburn, "Australia's Liquid Fuel Security."

Chapter 2: Why Liquid Fuels Will Remain Important to National Capability

After illustrating how efficiency-driven reforms have resulted in a fragile fuel network with minimal redundancy, this chapter focuses on liquid fuels that remain vital to Australia's economy, emergency services, and defence capacity. It examines how freight, aviation, mining, agriculture, maritime trade, emergency services, and the ADF rely on diesel and jet fuel without scalable alternatives.⁶⁴ Disruptions would trigger cascading risks that weaken national resilience, economic stability, and strategic credibility, thereby confirming that liquid fuels remain an essential foundation to Australia's sovereign capability.⁶⁵

Their importance becomes most evident when analysing how they support sectors that drive Australia's economy and security, including freight, aviation, mining, agriculture, maritime trade, emergency services, and defence.⁶⁶ Diesel powers heavy transport and industry nationwide, while jet fuel underpins commercial aviation and accounts for about 75 per cent of Defence's total fuel use, particularly across northern and north-western Australia, where it supports air operations, maritime patrols, and force projection.⁶⁷ These fuels collectively enable operations, mobility, and crisis response, meaning their disruption would immediately erode Australia's national capability.

2.1 Economic Dependence: Freight, Mining, Agriculture, and Trade

Nowhere is this reliance on liquid fuels more evident than in Australia's freight and logistics systems. Road freight accounts for over 75 per cent of Australia's domestic goods transport by volume and is powered almost entirely by diesel.⁶⁸ With vast distances between population centres, limited rail options, and freight volumes expected to increase by 77 per cent out to 2050,⁶⁹ Australia's economy and supply networks will likely remain dependent on diesel-powered transport for the foreseeable future.⁷⁰

In 2022–23, diesel accounted for around 69 per cent of Australia's total liquid fuel use, with the freight sector consuming the largest share.⁷¹ Transport emissions account for

⁶⁴ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

⁶⁵ "Australia's fuel insecurity is not hypothetical."

⁶⁶ Office of Impact Analysis, *Regulation Impact Statement*.

⁶⁷ Joint Standing Committee on Foreign Affairs, Defence and Trade, *Inquiry into the Defence Annual Report 2019–20* (Canberra: Commonwealth of Australia, 2021), 27, 29, 32–33,

https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/DefenceAnnualReport19-20/Report.

⁶⁸ Blackburn, "Australia's Liquid Fuel Security."

⁶⁹ Bureau of Infrastructure and Transport Research Economics, *Australian aggregate freight forecasts – 2022 update*, Research Report 154 (Canberra: Commonwealth of Australia, 2022), https://www.bitre.gov.au/sites/default/files/documents/bitre_rr154.pdf.

⁷⁰ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

⁷¹ Bureau of Infrastructure and Transport Research Economics, "Transport Energy and Environment," Australian Infrastructure and Transport Statistics Yearbook 2024, accessed July 16, 2025,

84 per cent of all liquid fuel-related emissions, underscoring their significant contribution to overall consumption, with heavy road vehicles being the primary contributors.⁷² While the number of electric vehicles is projected to increase steadily, there is simply no viable alternative fuel for long-haul freight.⁷³ Hydrogen and electric trucks are still in their early trial stages, and the necessary infrastructure to support them remains decades away from being commercially viable.⁷⁴ This means diesel will continue to power the transportation of food, fuel, pharmaceuticals, and industrial goods across Australia for decades, including to remote communities.⁷⁵ Assured access to these fuels is therefore crucial for maintaining national supply chains, ensuring economic resilience, and sustaining regular societal operations.⁷⁶

The mining sector is one of Australia's largest consumers of diesel. In 2021–22, mining accounted for around 14 per cent of national energy consumption, with more than half of that energy supplied by diesel.⁷⁷ This reliance extends to excavation, haulage, processing, and remote power generation.⁷⁸ Most major mining operations are situated in off-grid or weak-grid regions, where liquid fuels are the only feasible source of reliable, mobile energy.⁷⁹ Liquid fuels are vital not only for production but also for export logistics. Heavy-haul trucks, rail links, and port equipment all rely on diesel or bunker fuels to move bulk commodities, such as iron ore, coal, and critical minerals.⁸⁰

The sector's reliance on liquid fuels has national consequences: in 2022–23, resources and energy exports contributed over \$460 billion to Australia's export earnings, making dependable access to liquid fuel crucial to maintaining the country's economic resilience.⁸¹ Electrification of the mining sector is limited by geography, cost, and the energy density required to meet operational demands.⁸² Although some mining sites are testing hybrid or electric machinery, the energy density and reliability of diesel still outweigh alternatives for most high-load, remote functions.⁸³ Fuel insecurity in this sector could have national consequences. It would significantly impact export income,

<https://www.bitre.gov.au/publications/2024/australian-infrastructure-and-transport-statistics-yearbook-2024/transport-energy-environment>.

⁷² Ibid.

⁷³ Regional Australia Institute, "Towards Net Zero - Fossil Fuel Dependency in Regional Australia," accessed July 16, 2025, <https://regionalaustralia.org.au/common/Uploaded%20files/Files/2025/ISIP/Sustainability/Embargoed%20Fossil%20Fuel%20Dependency%20in%20Regional%20Australia.pdf>.

⁷⁴ "Towards Net Zero - Fossil Fuel Dependency in Regional Australia,"

⁷⁵ Department of the Environment and Energy, *Liquid Fuel Security Review—Interim Report*.

⁷⁶ "Australia's fuel insecurity is not hypothetical."

⁷⁷ Future Battery Industries CRC, *An overview of Australia's mining vehicle and mining equipment electrification* (Report, November 2023), 6, https://fbicrc.com.au/wp-content/uploads/2023/11/FBICRC_Mobile-Mine-Report-VFINAL.pdf.

⁷⁸ Regional Australia Institute, "Towards Net Zero."

⁷⁹ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

⁸⁰ Ibid.

⁸¹ Australian Energy Producers, "AEP Key Statistics 2024," accessed July 16, 2025, https://energyproducers.au/wp-content/uploads/2024/06/AEP_KS24_Web2.pdf.

⁸² Regional Australia Institute, "Towards Net Zero."

⁸³ Ibid.

erode investor confidence, and harm Australia's reputation as a reliable supplier of strategic materials.⁸⁴

Australia's agricultural sector also heavily depends on liquid fuels for its operation. From planting to harvest, fuel powers tractors, harvesters, pumps, and on-site generators across thousands of decentralised locations.⁸⁵ After food is harvested or livestock is reared, diesel remains essential in transporting agricultural products to processors, markets, and ports.⁸⁶ This mobility is vital not only for commercial purposes but also for delivering food to urban centres and remote communities alike. Unlike other parts of the economy, the agricultural industry often operates far from electricity grids and with limited redundancy.⁸⁷ Most farms store only small quantities of diesel, making them very vulnerable to supply disruptions.⁸⁸ The seasonal nature of farming amplifies this risk, so a delay in fuel delivery during critical periods, such as harvest, can cause substantial productivity losses and long-term financial hardship.⁸⁹

Approximately 70 per cent of the food Australians consume is produced locally, and almost all of it is grown, processed, and transported using diesel-powered machinery and freight, directly linking these vulnerabilities to national food security.⁹⁰ In 2021–22, diesel accounted for more than 80 per cent of total on-farm energy use, and for crops like grain and cotton, this proportion exceeds 85 to 90 per cent.⁹¹ Despite this heavy reliance, agriculture is often overlooked in national fuel resilience planning, even though a prolonged disruption could threaten the nation's food supply, price stability, and regional economies, which have limited capacity to respond to supply shocks.⁹²

With no shared land borders and a highly globalised economy, Australia's ability to import and export crucial goods mainly relies on maritime trade. The sea routes that transport refined fuels, food, pharmaceuticals, machinery, and consumer goods form the core of the nation's economic activity. Bulk exports, such as iron ore, coal, and liquefied natural gas, also depend on these networks to sustain Australia's trade surplus and maintain its position in the global market.⁹³ In 2021–22, over 98 per cent of Australia's trade by volume was carried by sea, highlighting how the economy and the country's resilience are closely tied to the secure, uninterrupted flow of maritime freight.⁹⁴

⁸⁴ "Australia's fuel insecurity is not hypothetical."

⁸⁵ NSW Department of Primary Industries, "Diesel Use in NSW Agriculture and Opportunities to Support Net Zero," accessed July 16, 2025, https://www.dpi.nsw.gov.au/_data/assets/pdf_file/0011/1321796/mov3ment-diesel-use-in-ag.pdf.

⁸⁶ *Ibid.*

⁸⁷ Regional Australia Institute, "Towards Net Zero."

⁸⁸ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

⁸⁹ NSW Department of Primary Industries, *Diesel Use in NSW Agriculture*.

⁹⁰ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Final Report*.

⁹¹ NSW Department of Primary Industries, *Diesel Use in NSW Agriculture*.

⁹² "Australia's fuel insecurity is not hypothetical."

⁹³ Australian Strategic Policy Institute, "The trade routes vital to Australia's economic security," accessed July 16, 2025, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2024-03/SR203%20Trade%20routes%20vital%20to%20Australia's%20economic%20security_1.pdf.

⁹⁴ *Ibid.*

These operations, from international trade routes to domestic coastal shipping, are entirely reliant on liquid fuels, especially marine diesel and bunker fuels.⁹⁵ In addition to supporting export and import flows, coastal shipping plays a vital role in maintaining domestic freight networks and supplying fuel to regional communities without pipeline infrastructure.⁹⁶ Many vessels providing essential goods to Northern Australia, offshore facilities, and island territories depend on well-organised, time-sensitive fuel distribution systems.⁹⁷ A disruption to marine diesel supply, whether caused by global market fluctuations, geopolitical tensions, or logistical delays, would have widespread effects on national supply chains, affecting everything from fuel availability to the delivery of essential goods.⁹⁸

Building resilience in the maritime sector is therefore not only about transportation but also a core part of economic security. Currently, there are no viable alternatives to liquid fuels for long-distance shipping. Electrification is technically unfeasible for large commercial vessels, and new fuels like ammonia or methanol are still years away from commercial realisation.⁹⁹ Without alternatives, securing reliable access to marine diesel remains crucial for Australia to sustain its trade, support its population, and protect its strategic independence in an increasingly unpredictable global environment.¹⁰⁰

2.2 National Resilience: Aviation and Emergency Services

Australia's aviation sector depends entirely on liquid fuels, with jet fuel powering commercial flights, air freight, military aviation, and essential services, including aeromedical transport.¹⁰¹

In 2022–23, the country used over 6 billion litres of aviation turbine fuel, accounting for about 15 per cent of total liquid fuel consumption.¹⁰² There are no scalable alternatives for aviation fuel in the short to medium term.¹⁰³ Aviation is crucial for connecting remote communities, supporting the fly-in, fly-out (FIFO) workforce in the resources sector, and facilitating high-value exports.¹⁰⁴ Emergency services, such as the Royal Flying Doctor Service, rely on secure fuel access to deliver life-saving care over vast distances.¹⁰⁵ Air freight volumes continue to rise, with an expected increase of over 100 per cent by 2050,

⁹⁵ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

⁹⁶ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, "Establishing a Strategic Maritime Fleet of Australian Vessels," accessed July 16, 2025, <https://www.infrastructure.gov.au/sites/default/files/documents/establishing-a-strategic-maritime-fleet-of-australian-vessels-aip.pdf>.

⁹⁷ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

⁹⁸ "Australia's fuel insecurity is not hypothetical."

⁹⁹ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, "Establishing a Strategic Maritime Fleet."

¹⁰⁰ "Australia's fuel insecurity is not hypothetical."

¹⁰¹ Bureau of Infrastructure and Transport Research Economics, "Transport Energy and Environment."

¹⁰² Ibid.

¹⁰³ Regional Australia Institute, "Towards Net Zero."

¹⁰⁴ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

¹⁰⁵ Ibid.

and dependence on jet fuel is also likely to grow.¹⁰⁶

Unlike road transport, where battery-electric vehicles are becoming increasingly available, aviation has no viable alternative due to the energy density requirements.¹⁰⁷ Electrified aircraft are still limited to short-haul prototypes, and hydrogen-powered aviation remains in the research phase.¹⁰⁸ Liquid fuels will continue to support domestic and international air travel, medical logistics, and economic continuity for the foreseeable future.¹⁰⁹ Any disruption to jet fuel supply would have immediate effects on national mobility and regional cohesion.¹¹⁰

Liquid fuels are essential for Australia's emergency response capabilities. Firefighting vehicles, ambulances, police fleets, mobile command units, and evacuation transport all depend on assured access to diesel and petrol.¹¹¹ During crises such as bushfires, floods, and cyclones, the ability to quickly deploy these resources, often over large distances, is crucial for saving lives and restoring vital services.¹¹² Liquid fuels also power backup generators for hospitals, telecommunications infrastructure, and emergency coordination centres, particularly when the primary power grid is disrupted.¹¹³

The vulnerability of this system lies in its reliance on just-in-time fuel logistics. Most emergency services do not carry substantial fuel reserves and instead depend on the same commercial supply chains as the rest of the economy.¹¹⁴ This indicates that when fuel supply is disrupted, whether due to a natural disaster, cyberattack, or supply shock, emergency services face the same limitations as the wider public.¹¹⁵ In remote or disaster-affected areas, where roads might be blocked or fuel deliveries delayed, this reliance can significantly reduce operational reach and response times.¹¹⁶

Ensuring a stable fuel supply during emergencies is therefore not just a logistical issue, but a matter of national resilience and preparedness. While contingency plans and localised fuel storage exist in some jurisdictions, there is no consistent national

¹⁰⁶ Bureau of Infrastructure and Transport Research Economics, Australian aggregate freight forecasts, 19-20.

¹⁰⁷ Catherine King, "Have your say on a future made in Australia: unlocking Australia's low carbon liquid fuel opportunity," media release, Department of Infrastructure, Transport, Regional Development and Local Government, accessed 2024, <https://minister.infrastructure.gov.au/c-king/media-release/have-your-say-future-made-australia-unlocking-australias-low-carbon-liquid-fuel-opportunity>.

¹⁰⁸ Regional Australia Institute, "Towards Net Zero."

¹⁰⁹ Department of the Environment and Energy, *Liquid Fuel Security Review—Interim Report*.

¹¹⁰ "Australia's fuel insecurity is not hypothetical."

¹¹¹ Department of the Environment and Energy, *Liquid Fuel Security Review—Interim Report*.

¹¹² Ibid.

¹¹³ Ibid.

¹¹⁴ Ibid.

¹¹⁵ Infrastructure Australia, "A Pathway to Infrastructure Resilience Advisory Paper 1," accessed July 16, 2025, <https://www.infrastructureaustralia.gov.au/sites/default/files/2021-08/Advisory%20Paper%201%20-%20A%20pathway%20to%20Infrastructure%20Resilience%20FINAL.pdf>.

¹¹⁶ Ibid.

framework for emergency fuel assurance.¹¹⁷ As the frequency and severity of climate-related disasters increase, the need for more robust, decentralised, and pre-planned fuel resilience measures will become increasingly urgent, especially for supporting vulnerable communities and maintaining critical services.¹¹⁸

2.3 Defence and Strategic Imperatives

Liquid fuels are vital to Australia's military strength. From air missions and naval deployments to logistics convoys and land mobility, the Australian Defence Force (ADF) remains almost entirely reliant on diesel and jet fuel to project power and sustain operations.¹¹⁹ Unlike other energy sources, these fuels are particularly suitable for the mobility, energy density, and logistical flexibility needed in contested or expeditionary environments.¹²⁰ Currently, no credible alternative exists to meet the operational demands of combat aircraft, naval vessels, armoured vehicles, or deployable support systems on the scale required for modern conflict.¹²¹

This dependence is further heightened by the ADF's regional stance and its evolving strategic outlook. The National Defence Strategy increasingly focuses on deterrence



Image: Department of Defence

from a distance, forward presence, and rapid joint-force deployment across the Indo-Pacific, all of which are energy-intensive and rely heavily on fuel.¹²² However, the ADF does not control its fuel supply chains nor maintain substantial reserves. Its fuel is sourced from the national market and supplied through foreign-owned, commercially operated networks that also support the Australian

economy.¹²³ This creates a risky assumption: that fuel will be available when needed, even during times of disruption, crises or conflict.¹²⁴

Fuel dependency is also deeply ingrained in the long-term structure of Australia's military capability. The ADF's platforms, from Joint Strike Fighters and armoured vehicles to naval destroyers and amphibious ships, are a fleet of multi-billion-dollar assets designed to operate for decades and run exclusively on liquid fuels.¹²⁵ Unlike parts of the civilian economy where electrification is progressing, there is no credible pathway to transition these systems away from petroleum-based energy sources.¹²⁶ This reliance makes fuel security not only a short-term operational concern but also a long-term strategic imperative that will influence Defence readiness and sovereign capability into the 2040s and beyond.¹²⁷

¹¹⁷ Department of the Environment and Energy, *Liquid Fuel Security Review—Interim Report*.

¹¹⁸ Infrastructure Australia, *A Pathway to Infrastructure Resilience*.

¹¹⁹ Department of Defence, *Defence Strategic Review 2023*.

¹²⁰ Ibid.

¹²¹ "Australia's fuel insecurity is not hypothetical."

¹²² Department of Defence, *Defence Strategic Review 2023*.

¹²³ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

¹²⁴ "Australia's fuel insecurity is not hypothetical."

¹²⁵ Department of Defence, *Defence Strategic Review 2023*.

¹²⁶ "Australia's fuel insecurity is not hypothetical."

¹²⁷ Department of Defence, *Defence Strategic Review 2023*.

Wargames and strategic assessments have repeatedly identified this vulnerability. The 2023 Defence Strategic Review (DSR) acknowledged, for the first time, the necessity of evaluating domestic fuel resilience as part of Defence's preparedness.¹²⁸ However, neither Defence nor other commonwealth departments have articulated a clear strategy to ensure fuel supply for the military during crises.¹²⁹ With adversaries increasingly capable of targeting critical infrastructure and exploiting supply chain dependencies, Australia's lack of fuel refining capability and lack of redundancy in the national fuel network pose a significant risk to operational continuity, deterrence credibility, and national sovereignty.¹³⁰

2.4 Cascading Risks to National Capability

Despite differences in geography and infrastructure, Australia's critical economic sectors, emergency services and national security functions are heavily reliant on liquid fuels.¹³¹ Together, they support Australia's economic strength, crisis response, and defence capacity.¹³² Yet this dependence is often overlooked in national planning, where focus remains on electricity and emissions reduction.¹³³ Even as global supply chains tighten, energy geopolitics become increasingly complex, and refining capacity decreases, Australia continues to operate under the assumption that fuel will always be available, without adequately addressing this risk to national capability.¹³⁴ The next chapter explores the implications of this vulnerability and the structural factors that have enabled it to continue.

¹²⁸ Ibid.

¹²⁹ "Australia's fuel insecurity is not hypothetical."

¹³⁰ "Australia's fuel insecurity is not hypothetical."

¹³¹ Department of Climate Change, Energy, the Environment and Water, *Liquid Fuel Security Review—Interim Report*.

¹³² "Australia's fuel insecurity is not hypothetical."

¹³³ Ibid.

¹³⁴ Ibid.

Chapter 3: The Review and Policy Package

Australia's first comprehensive fuel security review in a decade reasserted fuel security as a key issue within national policy discourse, yet its framework left several key vulnerabilities unresolved. By privileging efficiency over resilience, modelling only short-term disruptions, and excluding Defence requirements, the Review produced recommendations suited to stabilising markets rather than preparing for strategic contingencies.¹³⁵ The culminating policy package, including the Fuel Security Services Payment and Minimum Stockholding Obligation, introduced market-stabilising interventions but failed to address enduring structural deficiencies. Scholarly and policy analyses of the Review emphasise that integrated civil-military planning, sovereign production, and preparedness for protracted disruptions were missed, illustrating how it underestimated the strategic dimensions of Australia's national fuel security.¹³⁶

The Liquid Fuel Security Review, commissioned in 2018 and completed in 2020, emerged amid growing concerns about Australia's declining refining capacity, increasing reliance on imports, and contested regional supply chains.¹³⁷ As the first comprehensive government-led assessment of national fuel security in over a decade, it aimed to establish a baseline understanding of fuel system resilience, identify key vulnerabilities, and recommend measures to ensure supply continuity under various conditions.¹³⁸ Its findings directly influenced the government's Liquid Fuel Security Package¹³⁹ which introduced expanded stockholding obligations, targeted infrastructure investment incentives, and legislative amendments under the Liquid Fuel Security Act.¹⁴⁰ This chapter examines the Review's conceptual framework, scenario design, and prioritisation choices, and evaluates how these decisions influenced the policy measures which followed, while leaving critical strategic vulnerabilities unaddressed.

3.1 Framework, Scope, and Scenario Design

While the Liquid Fuel Security Review signified a notable reconnection of fuel security with the national policy agenda, its analytical framework contained inherent biases that curtailed its strategic utility. By prioritising economic efficiency over resilience, excluding Defence from its core definition, and modelling only short-term, recoverable disruptions, the Review produced recommendations better suited to smoothing market volatility than withstanding prolonged, strategically driven supply shocks.¹⁴¹ These choices narrowed the range of policy interventions considered and left Australia's fuel security framework misaligned with the demands of a more contested and unpredictable strategic environment.¹⁴²

¹³⁵ Swann, "Submission: Interim Report," 2-4.

¹³⁶ Matt Grudnoff, *Over a Barrel: A review of Australia's liquid fuel security*, Discussion Paper (Canberra: The Australia Institute, April 2022), 16–18, https://australiainstitute.org.au/wp-content/uploads/2022/04/P1036-Over-a-barrel_liquid-fuel-security-WEB.pdf.

¹³⁷ Australian Government, Department of Industry, Science, Energy and Resources, "Liquid Fuel Security Review - Final Report," October 2020, 17.

¹³⁸ *Ibid.* 1.

¹³⁹ Department of Climate Change, Energy, the Environment and Water, "Australia's fuel security," DCCEEW, accessed August 14, 2025, <https://www.dcceew.gov.au/energy/security/australias-fuel-security>.

¹⁴⁰ *Fuel Security Act 2021* (Cth), Compilation No. 2, October 17, 2024.

¹⁴¹ Swann, "Submission: Interim Report," 2–4.

¹⁴² "Australia's fuel insecurity is not hypothetical."

The Review was conducted in a context where secure access to liquid fuels underpins economic stability, national security, and societal resilience.¹⁴³ Nonetheless, the scope was narrowly defined in terms of whether Australia's fuel system could deliver on Australia's economic, environmental, and social objectives.¹⁴⁴ This definition excluded Defence requirements from its core concept of national fuel security, instead treating Defence's fuel requirements as a separate responsibility to be delivered through its departmental contracting.¹⁴⁵ By assuming Defence could operate independently of the broader national supply system, the Review overlooked a significant element of Australia's national capability, limiting its capacity to assess how fuel disruptions might constrain crisis response and the military's ability to protect or project force from Australia.¹⁴⁶

The Review's conceptual framework was built on three pillars: adequacy, efficiency, and reliability. Adequacy was evaluated to determine whether supply levels could meet demand and be transported to where they were needed. Efficiency was used to focus on the ability of market mechanisms to deliver fuel at the lowest possible cost. Reliability assessed the capacity of supply chains to absorb and adapt to disruptions. While this provides a somewhat logical structure, the Review's prioritisation showed a bias towards efficiency, explicitly warning that increased supply security would come with higher costs.¹⁴⁷ By prioritising price stability, the framework effectively rendered resilience a secondary concern, even though contested environments inherently make secure supply more costly but also strategically crucial.¹⁴⁸

Applying this framework to national fuel use patterns without fully integrating Defence requirements led the Review to emphasise diesel as the country's most critical fuel.¹⁴⁹ Diesel's extensive use does highlight its vital role in supporting freight, agriculture, mining, and maritime operations. However, it excluded Defence fuel patterns from the analysis, which would have shown that jet fuel accounts for around 70 per cent of Defence fuel use, and meant the review did not consider the operational and geographical needs that influence Australia's national capability during crises.¹⁵⁰ Moreover, this omission limited its ability to recommend measures to address vulnerabilities in the northern and north-western supply networks, which are essential for force projection and regional security.¹⁵¹

The scenarios used to test Australia's fuel system resilience mainly simulated short-term

¹⁴³ Department of Industry, Science, Energy and Resources, *Liquid Fuel Security Review—Final Report*, 18.

¹⁴⁴ Department of Industry, Science, Energy and Resources, *Liquid Fuel Security Review—Final Report*, 6.

¹⁴⁵ Department of Industry, Science, Energy and Resources, *Liquid Fuel Security Review—Final Report*, 15.

¹⁴⁶ Lockhorst, "The urgent need for a strategic overhaul."

¹⁴⁷ Australian Government, Department of Industry, Science, Energy and Resources, "Liquid Fuel Security Review - Final Report," October 2020, 20.

¹⁴⁸ Blackburn, "Australia's Liquid Fuel Security."

¹⁴⁹ Department of Industry, Science, Energy and Resources, *Liquid Fuel Security Review—Final Report*, 11.

¹⁵⁰ Benjamin Cole, "Decreasing Reliance on Fossil Fuels to Increase Defence Capability," Air & Space Power Centre, Australian Air Force, December 2022, 2, <https://airpower.airforce.gov.au/sites/default/files/2022-12/Decreasing%20Reliance%20On%20Fossil%20Fuels%20To%20Increase%20Defence%20Capability.pdf>.

¹⁵¹ Department of Defence, *Defence Strategic Review 2023*.

market disruptions, assuming global supply availability and rapid recovery.¹⁵² They did not consider more severe or lasting disruptions caused by geopolitical conflict, regional blockades, or sustained cyberattacks, risks recognised by independent assessments as plausible and strategically significant.¹⁵³ Reports such as "Over a Barrel" and the NRMA's "Australia's Liquid Fuel Security" criticised this limited scenario design, noting that it underestimates vulnerability and results in an overly optimistic view of resilience.¹⁵⁴ By prioritising assumptions of rapid adaptation and ongoing market access, the Review favoured incremental measures over comprehensive, preparedness-focused reforms that would be necessary to manage high-impact contingencies.

3.2 Policy and Legislative Outcomes

The Liquid Fuel Security Review nonetheless marked a significant improvement after years of limited government attention to fuel security.¹⁵⁵ Its structured analysis, evidence base, and direct link to concrete policy measures reintroduced the issue into the national policy debate. It enhanced awareness of supply chain risks, prompted reforms such as increased stockpiling, and supported targeted investments in critical infrastructure.¹⁵⁶ However, these strengths were counterbalanced by notable limitations, including the exclusion of Defence requirements, a focus on efficiency over resilience, and a reliance on short-term, recoverable disruption scenarios, which constrained the scope of policy options.¹⁵⁷ This approach made the Review better equipped to handle market volatility than to prepare for strategically aimed or long-duration supply shocks.¹⁵⁸



Image: Dept of Climate Change, Energy, the Environment and Water

The Liquid Fuel Security Act of 2024 formalised the conceptual boundaries set by the Review into law.¹⁵⁹ The Act introduced stockholding obligations, mandatory reporting, and ministerial powers to modify requirements during declared fuel emergencies, enhancing

¹⁵² Department of Industry, Science, Energy and Resources, *Liquid Fuel Security Review—Final Report*, 75.

¹⁵³ Swann, "Submission: Interim Report."

¹⁵⁴ Grudnoff, *Over a Barrel*, 16; Blackburn, "Australia's Liquid Fuel Security."

¹⁵⁵ Neil Greet, "Enabling energy security in a profoundly changing world," Accelerating Energy Transition Series, Engineers Australia, July 2024, 2.

¹⁵⁶ Department of Climate Change, Energy, the Environment and Water, "Liquid Fuel Security - Actions to Support Australia's Fuel Security," QB23-000039, January 2023, 3.

¹⁵⁷ Australian Government, Department of Industry, Science, Energy and Resources, "Liquid Fuel Security Review - Final Report," October 2020, 75.

¹⁵⁸ Swann, "Submission: Interim Report."

¹⁵⁹ *Fuel Security Act 2021* (Cth).

transparency and short-term resilience.¹⁶⁰ However, it preserved the Review's structural blind spots, notably excluding Defence requirements from its scope. No mechanisms were established for integrated civilian–Defence fuel planning or for setting preparedness benchmarks against prolonged, strategically motivated disruptions. In practice, the legislation reaffirmed the market approach and prioritised affordability and efficiency over a comprehensive resilience framework for the entire nation, leaving the fuel security architecture misaligned with Australia's deteriorating strategic environment.¹⁶¹

The government's broader post-Review policy framework included measures such as securing oil stocks in the US Strategic Petroleum Reserve¹⁶² expanding diesel storage capacity, upgrading refineries, modernising fuel legislation, and obtaining diesel exhaust fluid supplies.¹⁶³ However, the two measures that stand out as the most structurally important include the Fuel Security Services Payment (FSSP) and the Minimum Stockholding Obligation (MSO). The FSSP offers targeted financial support to domestic refiners, ensuring continued production of petrol, diesel, and jet fuel even during uneconomic market conditions, with funding available until mid-2027.¹⁶⁴ The MSO sets mandatory minimum on-shore stock levels for Diesel, improving transparency and strengthening short-term supply resilience.¹⁶⁵ These measures mark the most significant market-aligned interventions in decades, directly addressing vulnerabilities in refining viability and stock availability.

3.3 Strategic Vulnerabilities and Alternative Perspectives

Although both initiatives enhance immediate capacity to manage disruptions, their design remains fundamentally shaped by the Review's prioritisation of economic efficiency over resilience. This leaves Australia better equipped to manage routine market volatility, such as price swings or minor logistical interruptions, than to withstand long-term or strategically targeted disruptions. Such disruptions include blockades of maritime chokepoints, coercive export restrictions, or hostile cyberattacks intended to weaken Australia's economic stability, Defence preparedness, and national resilience during crises.¹⁶⁶

Perspectives from the NRMA, ASPI, and academic research present broader, alternative definitions of national fuel security. These focus on integrated Defence–civilian planning, redundancy in critical supply chains, and sovereign production capacity as vital, regardless of immediate cost considerations.¹⁶⁷ Unlike the LFSR, these analyses incorporate models of long-duration disruptions, contested logistics environments, and simultaneous crises affecting multiple fuel types.¹⁶⁸ NRMA's work has highlighted the importance of strategic stockholding aligned with Defence

¹⁶⁰ Ibid.

¹⁶¹ Grudnoff, *Over a Barrel*, 16–18.

¹⁶² Department of Climate Change, Energy, the Environment and Water, "Liquid Fuel Security - Actions to Support Australia's Fuel Security," QB23-000039, January 2023, 4.

¹⁶³ Department of Climate Change, Energy, the Environment and Water, "Australia's fuel security."

¹⁶⁴ Ibid.

¹⁶⁵ Ibid.

¹⁶⁶ "Australia's fuel insecurity is not hypothetical."

¹⁶⁷ John Blackburn, "Australia's Liquid Fuel Security Part 2," report for NRMA Motoring & Services, February 2014, 12.

¹⁶⁸ Ibid.

operational needs. The Australian Institute's 'Over a Barrel' emphasised the fragility of northern supply nodes, which are crucial for air and maritime operations.¹⁶⁹ Academics such as Yates and Greet's scholarship advocate for integrating fuel security into whole-of-nation capability planning rather than isolating it within market regulation frameworks.¹⁷⁰ Overall, these perspectives reveal that the LFSR underestimated the strategic importance of preparedness, restricting its ability to develop the integrated resilience framework needed for Australia's increasingly unstable strategic environment.¹⁷¹

¹⁶⁹ Grudnoff, *Over a Barrel*, 14.

¹⁷⁰ Athol Yates and Neil Greet, "Energy Security for Australia: Crafting a comprehensive energy security policy," Engineers Australia, 2014, 39.

¹⁷¹ Swann, "Submission: Interim Report."

Chapter 4: Finland and Japan's Fuel Resilience Measures

Australia is not alone in confronting fuel insecurity. Still, it is uncommon among advanced economies in its level of dependence on foreign fuel supply chains and the absence of a strategic safety net. Building on the previous chapter's analysis of Australia's policy framing and limitations, this chapter examines how Finland and Japan have institutionalised liquid fuels as a national capability. In contrast to Australia, countries like Finland and Japan, which have experienced energy shocks and risks of disruption,¹⁷² have established institutionalised systems to ensure the supply of liquid fuels during crises.¹⁷³ Although the strategic contexts of these countries differ, both view liquid fuels as a vital element of national capability.¹⁷⁴ While their methods for enabling this are not necessarily those Australia should follow, they demonstrate how nations can integrate fuel resilience into national planning.¹⁷⁵ Both countries have clear legal mandates,¹⁷⁶ empowered institutions,¹⁷⁷ and prioritise assurance over efficiency.¹⁷⁸

4.1 Finland's Comprehensive Security Model

Decades of proximity to an unpredictable Russia, combined with wartime scarcity and hybrid threats, have shaped Finland's deeply rooted culture of national preparedness.¹⁷⁹ Fuel security is regarded not as a market issue but as a vital foundation for its national resilience, demanding ongoing state attention and coordination.¹⁸⁰ This approach is institutionalised through the National Emergency Supply Agency (NESA), which manages strategic fuel reserves and organises logistics across critical sectors during crises.¹⁸¹ Unlike countries that depend on commercial supply chains, Finland has established a framework to ensure that this is both legally mandated¹⁸² and widely

¹⁷² International Energy Agency, "How Japan Thinks About Energy Security," CSIS, accessed July 28, 2025, <https://www.csis.org/analysis/how-japan-thinks-about-energy-security>.

¹⁷³ National Emergency Supply Agency, "The National Emergency Supply Agency," Huoltovarmuuskeskus, accessed July 28, 2025, <https://www.huoltovarmuuskeskus.fi/en/organisation/the-national-emergency-supply-agency>.

¹⁷⁴ Government of Finland, Security Strategy for Society, 2017, 20, <https://helda.helsinki.fi/server/api/core/bitstreams/1a7333a5-8480-4241-92dc-660037193aca/content>.

¹⁷⁵ Ministry of Economy, Trade and Industry, Strategic Energy Plan, April 2014, 28, https://www.enecho.meti.go.jp/en/category/others/basic_plan/pdf/4th_strategic_energy_plan.pdf.

¹⁷⁶ International Energy Agency, "Finland's Legislation on Oil Security," IEA, accessed July 28, 2025, <https://www.iea.org/articles/finland-s-legislation-on-oil-security>.

¹⁷⁷ National Emergency Supply Agency, "The National Emergency Supply Agency."

¹⁷⁸ Government of Finland, Security Strategy for Society, 2017, 20.

¹⁷⁹ Hanna Smith, "Hybrid Operations and the Importance of Resilience: Lessons From Recent Finnish History," Carnegie Endowment for International Peace, February 2018, <https://carnegieendowment.org/research/2018/02/hybrid-operations-and-the-importance-of-resilience-lessons-from-recent-finnish-history?lang=en>.

¹⁸⁰ Government of Finland, Security Strategy for Society, 2017, 20.

¹⁸¹ National Emergency Supply Agency, "The National Emergency Supply Agency."

¹⁸² International Energy Agency, "Finland's Legislation on Oil Security."

accepted by the public.¹⁸³

This system is based on a dual-track model that combines state reserves with private sector obligations.¹⁸⁴ Under the Security of Supply Act and the Act on the Obligatory Stockpiling of Imported Fuels, importers are required to hold two to three months' worth of fuel.¹⁸⁵ Simultaneously, the NESA maintains government-controlled reserves in secure, undisclosed depots across the country.¹⁸⁶ This layered structure ensures that strategic fuel stocks are not only available but also diversified among stakeholders, thereby reducing the risk of single points of failure during disruptions. Instead of relying on market responses, Finland integrates fuel requirements as a key element of national planning, ensuring it is incorporated into national strategies as a vital component of its sovereign resilience.¹⁸⁷

Finland's legal framework supports this through coordinated efforts among the state, industry, and essential services. NESA organises sector-specific working groups, including the Oil Pool and the Energy Supply Sector, to create detailed response plans for maintaining supply during disruptions.¹⁸⁸ These groups unite public agencies, infrastructure operators, and private firms to coordinate roles and set allocation protocols for critical sectors. Private operators are contracted in advance to ensure preparedness, enabling supplies to be directed quickly to priority users during a national emergency.¹⁸⁹ This approach aligns with Finland's broader Comprehensive Security Model, which views national resilience as a civic obligation shared across society, rather than solely a government function.¹⁹⁰

The depth of Finland's fuel system has also been tested through multiple crises, reinforcing its value as a foundation of national continuity and capability. In 2022, NESA released oil reserves in response to Russia's invasion of Ukraine, confirming its capacity to manage external shocks with agility.¹⁹¹ Earlier activations during the COVID-19 pandemic and poor harvest seasons showed that fuel stockpiles can stabilise supply chains beyond the energy sector.¹⁹² These practical demonstrations highlight how deeply fuel resilience is integrated into Finland's crisis planning and operational readiness across society. While Australia has not faced similar tests, Finland's experience does show that long-term resilience can be designed proactively, rather than being recovered after failure.¹⁹³

¹⁸³ Government of Finland, *Security Strategy for Society*, 2017, 20.

¹⁸⁴ Finnish Government, "Finland releases 369,000 barrels of crude oil to the market from its emergency stockpiles," *Valtioneuvosto.fi*, April 8, 2022, <https://valtioneuvosto.fi/en/-/1410877/finland-releases-369-000-barrels-of-crude-oil-to-the-market-from-its-emergency-stockpiles>.

¹⁸⁵ International Energy Agency, "Finland's Legislation on Oil Security."

¹⁸⁶ Ministry of Economic Affairs and Employment, "Reserve stocks and preparedness planning secure energy supply," *tem.fi*, accessed July 28, 2025, <https://tem.fi/en/security-of-energy-supply>.

¹⁸⁷ Government of Finland, *Security Strategy for Society*, 2017, 20.

¹⁸⁸ Ministry of Economic Affairs and Employment, "Reserve stocks and preparedness planning."

¹⁸⁹ National Emergency Supply Agency, "The National Emergency Supply Agency."

¹⁹⁰ Government of Finland, *Security Strategy for Society*, 2017, 20.

¹⁹¹ Finnish Government, "Finland releases 369,000 barrels of crude oil."

¹⁹² National Emergency Supply Agency, "The National Emergency Supply Agency."

¹⁹³ Smith, "Hybrid Operations."

4.2 Japan's Strategic Energy Framework

Despite an increasingly volatile regional environment underscored by North Korea's weapons programme, China's assertiveness, and tensions in the Taiwan Strait, Japan's approach to fuel security is actually shaped by its past energy shocks. The 1973 oil embargo was a turning point, triggering economic disruption and prompting a national reckoning over energy dependence and systemic fragility.¹⁹⁴ In response, Japan established a legal and institutional framework in the hope of preventing fuel shortages from ever again threatening national stability or economic continuity.¹⁹⁵ Unlike Finland, where security evolved from territorial threat, Japan's system emerged from economic trauma, making energy resilience a permanent strategic priority. Japan's experience reinforced a core principle, whereby physical reserves, legal authority, and coordinated institutions are essential to sustaining national capability under pressure.¹⁹⁶

Japan's fuel security framework is anchored by its Oil Stockpiling Act of 1975, which mandates substantial reserves across both public and private sectors. As of 2022, Japan maintained over 199 days of oil reserves, significantly exceeding the International Energy Agency's 90-day requirement for net importers. These reserves are split between government-managed stocks and industry commitments, with companies required to keep fuel inventories at specified domestic terminals. The Japan Organization for Metals and Energy Security (JOGMEC) manages state reserves and offers financial support to private operators via loans and subsidies.¹⁹⁷ This hybrid model guarantees national control over the reserves while utilising private infrastructure and sharing the costs and responsibility for maintaining fuel security.¹⁹⁸

Japan's fuel security extends beyond stockpiling to encompass detailed crisis planning, distribution logistics, and integrated civil–military coordination during national emergencies. The government maintains prioritisation protocols that ensure fuel is swiftly allocated to defence, emergency services, and critical infrastructure during times of disruption.¹⁹⁹ During the 2011 Great East Japan Earthquake, fuel reserves enabled the Self-Defense Forces to mobilise swiftly and assist communities affected by power and transportation failures.²⁰⁰ The crisis emphasised the importance of decentralised supply, backup systems, and regular drills to test coordination across national, regional, and local levels.²⁰¹ Resilience in Japan is not defined solely by passive reserves; it is

¹⁹⁴ International Energy Agency, "How Japan Thinks About Energy Security."

¹⁹⁵ "Oil Stockpiling Act (Act No. 96 of 1975)," Japanese Law Translation, accessed July 28, 2025, <https://www.japaneselawtranslation.go.jp/en/laws/view/3000/en>.

¹⁹⁶ International Energy Agency, "How Japan Thinks About Energy Security."

¹⁹⁷ International Energy Agency, "Japan Oil Security Policy – Analysis," IEA, accessed July 28, 2025, <https://www.iea.org/articles/japan-oil-security-policy>; International Energy Agency, "Oil Stocks of IEA Countries," IEA Data and Statistics, accessed July 28, 2025, <https://www.iea.org/data-and-statistics/data-tools/oil-stocks-of-iea-countries>.

¹⁹⁸ International Energy Agency, "Japan Oil Security Policy – Analysis."

¹⁹⁹ Ministry of Economy, Trade and Industry, Strategic Energy Plan, 28.

²⁰⁰ Noboru Shimodaira, "The JMSDF's Resilient Power for Civil Society: Lessons from the Great East Japan Earthquake," *Naval War College Review* 65, no. 1 (2012): 108, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1221&context=nwc-review>.

²⁰¹ Basalla, Berger, and Abbot, "The Great East Japan Earthquake: A Case Study in Civil-Military Coordination," *Joint Force Quarterly* 68 (2013): 25, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-68/JFQ-68_25-31_Basalla-Berger-Abbot.pdf.

demonstrated through simulation, planning, and the expectation that disruption will inevitably happen again.

Japan's approach to fuel security is based on the principle that resilience should be established before disruption occurs, rather than hurriedly constructed once systems start to fail. Although the global energy landscape is changing, Japan continues to invest in physical reserves, considering fuel vital for national defence and economic stability. Its guiding energy policy, S+3E, balances Security, Economic Efficiency, Environment, and Safety, but always prioritises assured access to fuel at the strategic core.²⁰² While diversification through renewables and hydrogen continues, planners accept that liquid fuels will remain essential to aviation, transport, and the military for the foreseeable future.²⁰³ This mindset presents a notable contrast to Australia, where assumptions of availability persist despite increasing geopolitical risks and a decline in sovereign control over supply chains.

4.3 Comparative Insights and Implications for Australia

Finland and Japan view fuel resilience as vital, recognising that the cost of disruption greatly outweighs the investment required to establish secure supply systems. Both nations employ hybrid stockpiling models²⁰⁴ coordinate closely with private operators²⁰⁵ and regard fuel as a vital enabler of national continuity and crisis response. Their systems develop through experience, supported by legislation,²⁰⁶ tested by emergencies,²⁰⁷ and continuously improved through planning and simulation.²⁰⁸ In contrast, Australia remains dependent on highly vulnerable and lean maritime supply chains and market assumptions, with limited sovereign control mechanisms to assure access during times of stress. Until Australia repositions fuel security as a strategic imperative, it will remain exposed to shocks that others have systematically prepared to absorb.

²⁰² Edelman Global Advisory, "Japan's Seventh Strategic Energy Plan," EdelmanGlobalAdvisory.com, January 7, 2025,

<https://www.edelmanglobaladvisory.com/japans-seventh-strategic-energy-plan>.

²⁰³ Ashurst, "Japan's New Energy Plan," Ashurst.com, accessed July 28, 2025, <https://www.ashurst.com/en/insights/japans-new-energy-plan/>.

²⁰⁴ Finnish Government, "Finland releases 369,000 barrels of crude oil to the market from its emergency stockpiles"; Reina Maeda, "Japan maintains LPG stockpile levels on trade concerns," Argus Media, July 15, 2025, <https://www.argusmedia.com/en/news-and-insights/latest-market-news/2710429-japan-maintains-lpg-stockpile-levels-on-trade-concerns>.

²⁰⁵ Ministry of Economic Affairs and Employment, "Reserve stocks and preparedness planning"; Ministry of Economy, Trade and Industry, *Strategic Energy Plan*, 28.

²⁰⁶ International Energy Agency, "Finland's Legislation on Oil Security"; "Oil Stockpiling Act."

²⁰⁷ Finnish Government, "Finland releases 369,000 barrels of crude oil to the market from its emergency stockpiles"; Shimodaira, "The JMSDF's Resilient Power for Civil Society," 108.

²⁰⁸ Ministry of Economy, Trade and Industry, *Strategic Energy Plan*, 28; Government of Finland, *Security Strategy for Society*, 2017, 20.

Chapter 5: Stockpiles to Sovereignty, Low-Carbon Liquid Fuels as a Strategic Capability

The comparative analysis of Finland and Japan revealed that both countries embed resilience through strategic stockpiling, utilising mandated reserves and government authority to maintain continuity during disruptions. The Liquid Fuel Security Review also emphasised the importance of stockpiling but limited its scope to a market stabilisation measure, excluding broader strategic needs and sovereign production capacity.²⁰⁹ These insights illustrate that stockpiling is only one component of resilience, as Australia remains vulnerable to coercion, contested supply chains, and prolonged disruptions in the absence of domestic refining capacity.²¹⁰

This chapter posits that low-carbon liquid fuels offer a sovereign production pathway that can complement an increase in stockpiles while supporting resilience, economic sovereignty, and decarbonisation goals.²¹¹ However, their adoption is debated, as critics highlight high costs, feedstock limitations, and regulatory uncertainty, which raise questions about scalability and affordability.²¹² By examining these viewpoints, the chapter demonstrates that despite these challenges, LCLFs remain a strategically aligned solution that enhances resilience, improves sovereign industrial capacity, and produces measurable decarbonisation benefits. In doing so, the chapter directly targets Australia's policymaking fragmentation, showing how security, economic, and environmental objectives can be aligned through a coherent national fuel strategy.²¹³

5.1 Strategic Value and Emerging Debates

Where stockpiling offers temporary security, LCLFs provide a lasting capability by establishing sovereign production capacity, thereby reducing dependence on contested overseas imports and enhancing national resilience.²¹⁴ Their strategic importance goes beyond emissions reduction, ensuring the continuity of Defence, freight, agriculture, and emergency services across Australia's economy.²¹⁵ Defence is especially vulnerable

²⁰⁹ Government of Finland, *Security Strategy for Society*; Swann, "Submission: Interim Report."

²¹⁰ Australian Workers' Union, "Submission to the 'Unlocking Australia's low carbon liquid fuel opportunity' consultation paper," July 2024, <https://www.infrastructure.gov.au/sites/default/files/documents/lclf2024-australian-workers-union.pdf>

²¹¹ Clean Energy Finance Corporation and Deloitte, *Refined Ambitions*.

²¹² Grattan Institute, *The next industrial revolution: Transforming Australia to flourish in a net-zero world* (Melbourne, VIC: Grattan Institute, 2022), <https://grattan.edu.au/report/next-industrial-revolution/>

²¹³ CSIRO, *Opportunities and Priorities for a Low Carbon Liquid Fuel Industry in Australia* (Canberra, ACT: CSIRO, 2025), <https://www.csiro.au/-/media/Missions/TNZ/Opportunities-and-priorities-for-a-Low-Carbon-Liquid-Fuel-Industry.pdf>

²¹⁴ Australian Industrial Transformation Institute, *Australian sovereign capability and supply chain resilience* (Adelaide, SA: Flinders University, 2021), <https://www.aph.gov.au/DocumentStore.ashx?id=bbf63058-99e8-4d20-8dd0-ea9ce41f79db&subId=715388>

²¹⁵ Deloitte, *Securing our Fuel Future: Resilience Through Low Carbon Liquid Fuels*, Report for Bioenergy Australia (Sydney, NSW: Deloitte, 2025), https://impact-on-sustainable-aviation.org/shared-files/2730/?Australia_Deloitte_Resilience%20through%20low%20carbon%20liquid

since jet fuel accounts for around 75 per cent of its total use, with no scalable substitutes available for air or maritime platforms.²¹⁶ This reliance makes interoperability with allies equally crucial, as the United States, Japan, and the European Union are all progressing with sustainable aviation fuel mandates.²¹⁷ Without sovereign LCLF capacity, Australia risks falling behind these partners, compromising interoperability, operational credibility and increasing exposure to contested supply chains.²¹⁸

5.2 Critiques and Counterarguments

Critics, including analysts at the Grattan Institute, warn that the higher costs of LCLFs could burden consumers and subsidise inefficiency, cautioning against governments “picking winners.”²¹⁹ Grattan has consistently argued that large-scale subsidies distort energy markets, increase consumer prices, and delay more cost-effective transition pathways, such as electrification or the use of hydrogen.²²⁰ Conversely, organisations focused on security, such as ASPI and NRMA, argue that resilience entails unavoidable costs, viewing LCLFs as strategic insurance against coercion, contested chokepoints, and extended disruptions.²²¹ For these analysts, affordability in peacetime matters less than guaranteed availability during a crisis, when price becomes irrelevant compared with the continuity of national capability.²²² The Government’s Future Made in Australia agenda reflects this tension, cautiously supporting industry development while balancing fiscal discipline with the recognition of LCLFs as both an industrial opportunity and a sovereign necessity.²²³

Concerns about feedstock availability further drive the scepticism. Environmental groups argue that biofuels risk repeating earlier “food versus fuel” controversies, as they compete with agriculture and raise questions about sustainability.²²⁴ Critics have emphasised that Australia’s domestic residues may be insufficient to boost production, leading to reliance on imported inputs that could weaken sovereignty.²²⁵ However,

%20fuels.pdf&download=1.

²¹⁶ Raelene Lockhorst, “Australia must boost investment to ensure strategic fuel security,” *The Strategist*, Australian Strategic Policy Institute, October 20, 2022, <https://www.aspistrategist.org.au/australia-must-boost-investment-to-ensure-strategic-fuel-security/>.

²¹⁷ Airlines for Australia and New Zealand, “Submission to the ‘Unlocking Australia’s low carbon liquid fuel opportunity’ consultation paper,” July 2024, <https://www.infrastructure.gov.au/sites/default/files/documents/lclf2024-airlines-for-australia-and-new-zealand.pdf>.

²¹⁸ Australian Workers’ Union, “Submission.”

²¹⁹ Grattan Institute, *The next industrial revolution*.

²²⁰ Ibid.

²²¹ “Australia’s fuel insecurity is not hypothetical”; Blackburn, “Australia’s Liquid Fuel Security.”

²²² “Australia’s fuel insecurity is not hypothetical.”

²²³ Australian Government, *A Future Made in Australia Fact Sheet*, Budget 2024-25 (Canberra, ACT: The Treasury, 2024), <https://archive.budget.gov.au/2024-25/factsheets/download/factsheet-fmia.pdf>.

²²⁴ Clean Energy Finance Corporation, “Biofuels and Transport: An Australian opportunity,” Submission to the Senate, Rural and Regional Affairs and Transport References Committee, Inquiry into the Adequacy of Australia’s Biosecurity Measures and Response Preparedness, n.d., https://www.aph.gov.au/-/media/Estimates/ec/supp2324/DCCEEW/Senator_Van_CEFC_Biofuels_and_Tra nsports.pdf.

²²⁵ CSIRO, *Opportunities and Priorities*.

Bioenergy Australia's 2025 report counters this pessimism by highlighting substantial untapped potential in tallow, waste oils, crop residues, and advanced synthetic pathways.²²⁶ They argue that the fundamental constraint is policy coordination, as many domestic feedstocks are exported cheaply overseas and re-imported later as higher-cost refined products.²²⁷ By redirecting these resources into local production, Australia could strengthen its sovereign capability while gaining significant economic value currently lost offshore.²²⁸

Infrastructure and scalability are also often subject to criticism. Analysts emphasise that Australia's limited refining capacity and underdeveloped biorefinery infrastructure restrict feasible options for increasing production.²²⁹ Building a new LCLF facility



requires an investment of \$200–400 million, which critics see as a significant obstacle in an uncertain policy environment.²³⁰ However, CSIRO and the Clean Energy Finance Corporation have demonstrated that these costs are comparable to those of hydrogen hubs, which already benefit from concessional finance and federal

funding.²³¹ Strategic procurement can also mitigate risks in development, with Defence acting as a guaranteed early procurer, underwriting capacity that can later be leveraged in commercial aviation and freight markets.²³² This approach positions sovereign production of LCLFs as a staged investment in resilience, rather than an inefficient subsidy for marginal technologies.²³³

5.3 Capability, Credibility, and Policy Pathways

LCLFs include renewable diesel, sustainable aviation fuel, and emerging synthetic fuels that match the energy density and performance of traditional petroleum products.²³⁴

²²⁶ Bioenergy Australia, "Submission to the 'Unlocking Australia's low carbon liquid fuel opportunity' consultation paper," July 2024, <https://www.infrastructure.gov.au/sites/default/files/documents/lclf2024-bioenergy.pdf>.

²²⁷ Clean Energy Finance Corporation and Deloitte, *Refined Ambitions*.

²²⁸ Australian Industrial Transformation Institute, *Australian sovereign capability*.

²²⁹ CSIRO, *Opportunities and Priorities*.

²³⁰ "Biofuels Boost Australia's Economy: The Growing Impact of Energy Crops," Biomass Producer, accessed September 4, 2025, <https://biomassproducer.com.au/agricultural-and-resource-management/biofuels-boost-australias-economy-the-growing-impact-of-energy-crops/>.

²³¹ Clean Energy Finance Corporation and Deloitte, *Refined Ambitions*.

²³² Tyson Sara, "Australia should grow its own fuel," *The Strategist*, March 18, 2024, <https://www.aspistragist.org.au/australia-should-grow-its-own-fuel/>.

²³³ Ibid.

²³⁴ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *A Future Made in Australia: Unlocking Australia's low carbon liquid fuel opportunity - Consultation Paper* (Canberra, ACT:

Unlike early-generation biofuels, they meet international drop-in standards, allowing for immediate replacement in existing fleets, distribution systems, and Defence platforms.²³⁵ This compatibility is strategically important because it avoids costly infrastructure duplication, reduces transition risks, and enables rapid integration without requiring operational redesign.²³⁶ Their lifecycle emissions reductions, often between 60 and 90 per cent, are recognised under international accounting frameworks, including CORSIA and the European Union Renewable Energy Directive.²³⁷ By embedding measurable abatement within aviation, freight, and Defence supply chains, LCLFs would strengthen Australia's climate diplomacy, signalling credibility to its regional partners at a time when environmental performance increasingly influences strategic alignment and cohesion.²³⁸

The dimension of economic sovereignty further reinforces the argument, as critics contend that subsidies will create fiscal burdens while diverting resources away from more cost-effective energy technologies.²³⁹ They assert that LCLFs offer limited value relative to their cost, primarily when Australia already imports fuels efficiently from global markets.²⁴⁰ Yet, Bioenergy Australia projects a \$36 billion industry by 2050, creating up to 28,000 jobs by 2030, with many of these jobs located in regional and rural communities.²⁴¹ The capacity to refine waste oils, residues, and agricultural by-products locally helps avoid the current paradox where Australia exports feedstocks at a low cost, only to re-import refined products at a higher price.²⁴² Sovereign production, therefore, represents not only resilience but also value-adding domestic industry, distributing growth into regions while insulating the economy against external shocks.²⁴³

Defence again highlights strategic necessity, since unlike civilian transport with partial electrification options, its platforms are built to operate for decades and cannot abandon the use of liquid fuels.²⁴⁴ Fighter jets, amphibious ships, and heavy armoured vehicles require dense, portable fuels that offer flexibility in contested areas and theatres.²⁴⁵ LCLFs provide this without the need for fleet redesigns, ensuring operational continuity while supporting decarbonisation.²⁴⁶ Interoperability is also crucial as allied militaries are increasingly using sustainable aviation fuels, and joint operations will eventually

Commonwealth of Australia, 2024), <https://www.infrastructure.gov.au/sites/default/files/documents/low-carbon-liquid-fuels-consultation-paper.pdf>.

²³⁵ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *A Future Made in Australia: Consultation Paper*.

²³⁶ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *A Future Made in Australia: Consultation Paper*.

²³⁷ Airlines for Australia and New Zealand, "Submission."

²³⁸ Griffith Asia Institute, *Future made in Australia? Evaluating Australia's 2024 green energy related policies and its potential impact on Asia* (Brisbane, QLD: Griffith University, 2024), https://www.griffith.edu.au/_data/assets/pdf_file/0031/1967143/Future-made-in-Australia-policy-brief.pdf.

²³⁹ Grattan Institute, *The next industrial revolution*.

²⁴⁰ Ibid.

²⁴¹ Deloitte, *Securing our Fuel Future*.

²⁴² Clean Energy Finance Corporation and Deloitte, *Refined Ambitions*.

²⁴³ Australian Industrial Transformation Institute, *Australian sovereign capability*.

²⁴⁴ Garside, *The Australian Defence Force and its future energy requirements*.

²⁴⁵ Ibid.

²⁴⁶ "Energy resilience, emissions targets in Defence sights," Department of Defence, October 28, 2024, <https://www.defence.gov.au/news-events/news/2024-10-28/energy-resilience-emissions-targets-defence-sights>.

require compatible supplies.²⁴⁷ Without sovereign capacity, Australia risks relying on allies for supplies during crises, which undermines its credibility as a security partner.²⁴⁸ Framing LCLFs as Defence assurance thus strengthens the counterargument to cost critiques: these fuels are vital enablers of strategic capability, not mere luxuries.²⁴⁹

Climate diplomacy adds a new layer. Pacific Island nations often see climate credibility as a test of partnership, linking emissions reductions with strategic trust.²⁵⁰ Including LCLFs in Australia's national strategy demonstrates that resilience and decarbonisation can advance together, countering the notion of neglect.²⁵¹ Globally, participation in schemes like CORSIA requires verified reductions in aviation emissions. Without LCLFs, Australia risks becoming isolated from international compliance frameworks, weakening both trade competitiveness and alliance unity.²⁵² Therefore, LCLFs are not just technical substitutes; they serve as credibility tools in regional diplomacy and international negotiations, aligning environmental responsibility with strategic influence.²⁵³

Expanding LCLFs will require deliberate statecraft, as markets alone cannot sustain higher costs or develop sovereign production capacity.²⁵⁴ Therefore, policy design is crucial. Demand-side measures such as blending mandates can create predictable markets but must be carefully sequenced with domestic supply to avoid sudden cost spikes.²⁵⁵ Defence procurement can act as a market-shaping tool, supporting early demand and signalling credibility to encourage wider private investment. On the supply side, concessional finance, targeted subsidies, and ARENA-style grants can reduce capital barriers, while production credits based on hydrogen incentives could lower per-litre costs.²⁵⁶ Governance measures such as certification frameworks aligned with CORSIA and EU standards, alongside expanded Guarantee of Origin schemes, would ensure credibility and attract international partners.²⁵⁷

These mechanisms collectively demonstrate that costs can be managed through strategic design, reframing subsidies not as inefficiencies but as premiums for resilience and sovereignty.²⁵⁸ Critics who warn against "picking losers" overlook that governments

²⁴⁷ Garside, *The Australian Defence Force and its future energy requirements*.

²⁴⁸ "Australia's fuel insecurity is not hypothetical."

²⁴⁹ Air and Space Power Centre, "Decreasing reliance on fossil fuels to increase defence capability," Royal Australian Air Force, December 5, 2022, <https://airpower.airforce.gov.au/sites/default/files/2022-12/Decreasing%20Reliance%20On%20Fossil%20Fuels%20To%20Increase%20Defence%20Capability.pdf>.

²⁵⁰ Griffith Asia Institute, *Future made in Australia?*

²⁵¹ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *A Future Made in Australia: Consultation Paper*.

²⁵² Airlines for Australia and New Zealand, "Submission to the 'Unlocking Australia's low carbon liquid fuel opportunity' consultation paper," July 2024, <https://www.infrastructure.gov.au/sites/default/files/documents/lclf2024-airlines-for-australia-and-new-zealand.pdf>.

²⁵³ Griffith Asia Institute, *Future made in Australia?*

²⁵⁴ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *A Future Made in Australia: Consultation Paper*.

²⁵⁵ Airlines for Australia and New Zealand, "Submission."

²⁵⁶ Clean Energy Finance Corporation and Deloitte, *Refined Ambitions*.

²⁵⁷ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *A Future Made in Australia: Consultation Paper*.

²⁵⁸ Deloitte, *Securing our Fuel Future*.

have historically shaped strategic industries, from refining and telecommunications to shipbuilding and critical minerals. By including targeted support, Australia can position LCLFs as the sovereign production complement to stockpiling, thus establishing twin pillars of resilience.²⁵⁹

A unified national fuel strategy integrating LCLFs would strengthen national capability, decrease reliance on contested imports, and align decarbonisation with security priorities.²⁶⁰ The argument presented here is clear and decisive, demonstrating that stockpiling results only in redundancy, while sovereign production using low-carbon fuels establishes lasting resilience.

²⁵⁹ CSIRO, *Opportunities and Priorities*.

²⁶⁰ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *A Future Made in Australia: Consultation Paper*.

Conclusion

This thesis has demonstrated that Australia's heavy dependence on imported liquid fuels represents one of the country's most profound structural risks, weakening its national resilience, economic stability, and Defence readiness. Accounting for over half of Australia's energy consumption, fuel enables the function of heavy freight, aviation, agriculture, mining, the military and emergency services, all of which lack scalable alternatives. Decades of deregulation and market orthodoxy have entrenched a national fuel system that prioritises cost efficiency, but one that is dangerously lacking in redundancy and sovereign control. These structural weaknesses have been highlighted by the dismantling of refining capacity, declining stockpiles, and increased reliance on overseas imports, making the national fuel system fragile to disruption. Moreover, this approach was institutionalised in the Liquid Fuel Security Review, which prioritised efficiency as the primary measure, relegating resilience to a secondary concern, and emphasising that secure supply inevitably involves an increase in supply costs.

The implications of this structural weakness are profound, as Defence's fuel needs were entirely excluded from the Review's framework, leaving its surge demands excluded from national planning despite their vital role in supporting a key aspect of Australia's national power. Meanwhile, billions have been allocated under the National Defence Strategy to deliver a deterrence-by-denial posture that is essentially rendered ineffective without assured access to liquid fuels. Without them, new capabilities risk paralysis in a contested environment. In contrast, the case studies of Finland and Japan show an alternative approach, where resilience is a deliberate choice, implemented through statutory design, empowered institutions, and public acceptance of higher costs as essential insurance against disruption. These examples highlight that resilience always comes at a price, but they also recognise that a far greater cost could be borne if their nations remained unprepared.

Delivering fuel resilience is also a question of climate credibility as Australia's pledge to achieve net zero by 2050 places its fuel policies under regional and international scrutiny, particularly among Pacific partners for whom climate action is central to their survival. Fuel resilience and how it is delivered, therefore, serve as a gauge of Australia's credibility as a reliable partner in addressing climate change. A sovereign low-carbon liquid fuels sector provides the only feasible way to expand Australia's refining capacity, balance resilience with decarbonisation commitments for hard-to-abate sectors and thus uphold climate credibility with its regional partners. Developing low-carbon liquid fuels domestically would ensure that military preparedness, economic stability, and environmental responsibility become interconnected pillars of a cohesive national fuel strategy.

Beyond a basic uplift in Australia's stockholdings, a logical early step is to conduct a comprehensive analysis of fuel demands across critical sectors, mapped geographically throughout Australia. This would identify the structural blind spots that leave the economy vulnerable to cascading failures during disruptions. Moreover, such an analysis must model long-duration disruptions, contested logistics environments, and simultaneous crises affecting multiple fuel types to identify where surge requirements are concentrated and where stockholding mandates can create redundancy in the areas most vital to national resilience. This process should be benchmarked against the International Energy Agency's stockholding requirements at a minimum, so that national obligations reflect not only compliance but also genuine preparedness for potential crises. Without granular demand mapping, stocks may accumulate in commercially convenient hubs, creating an illusion of redundancy while leaving areas, such as the northern and regional networks, dangerously exposed.

Distribution infrastructure requires a similarly comprehensive investigation, as resilience depends not only on the volume of fuels available but also on the ability to deliver them swiftly and where needed. The strategy of denial, outlined in the National Defence Strategy, increases pressure on northern and north-western networks, where secure access is vital for force projection. However, the infrastructure in these areas remains vulnerable. Critical modes, such as pipelines, sovereign-flagged coastal shipping, rail corridors, and the availability of truck drivers, must be prioritised, as disruption in these areas would affect both national defence and sectors like mining, which support the broader economy. Without targeted investment in these distribution links, even expanding the nation's stockholding or sovereign production will not provide the redundancy necessary to keep the network resilient enough to respond effectively in contested environments.

Creating a unified national fuel strategy, therefore, requires collaborative planning, as no single portfolio or industry player is responsible for delivering the resilience Australia urgently needs. Addressing this challenge demands a deliberate, phased approach that outlines the long-term end-state of national fuel resilience and then sequences the necessary reforms to address current vulnerabilities. By organising measures across long, medium, and short-term time horizons, Australia can recognise the interconnectedness of immediate stabilisation, systematic investigation, and lasting structural reform. Such planning must acknowledge that fuel prices impact every Australian, emphasising that efficiency is a priority while also ensuring that resilience and effectiveness are not consistently compromised. The goal is not to abandon efficiency but to balance it against the costs of fragility, reframing increases in fuel prices as an insurance premium for sovereignty and national preparedness. Collaboration must therefore include Defence surge requirements, freight continuity, geographic vulnerabilities across the north, and climate commitments to build regional climate credibility. Consideration should also be given to distribution infrastructure and workforce sustainability. Fragmented approaches have repeatedly failed to deliver a network fit for purpose in our current environment. A comprehensive national fuel strategy, which balances efficiency with resilience and grounds sovereign preparedness in an era of contested supply chains, is urgently needed to address Australia's fuel vulnerability.

Long-term measures

Enduring resilience cannot be achieved through stockpiling or investment in distribution alone, as these measures would stabilise but not transform Australia's structural dependence on contested imports. A sovereign low-carbon liquid fuels industry offers the only practical pathway to expand Australia's refining capacity, deliver enduring redundancy, and reconcile fuel resilience with Australia's decarbonisation commitments. Developing this capability requires a dual approach, where demand-side policies, such as blending mandates and government procurement mandates, including for Defence, must be paired with supply-side incentives, including concessional finance and certification frameworks. The right balance of these mechanisms would incentivise domestic production, ensuring that critical sectors receive certified LCLFs while positioning Australia as a credible climate partner within the region. Sovereign production would reduce exposure to maritime chokepoints, generate regional economic renewal, and align national security with climate commitments. Long-term measures must, therefore, transform fuel from a vulnerability into a sovereign capability, embedding preparedness as the foundation of national strategy for decades to come.

Medium-term measures

Stabilisation of the national fuel network alone is insufficient without also addressing the structural blind spots that continue to expose Australia's economy to the cascading failures that would be experienced during prolonged disruption. Stockholding mandates only create real resilience if stocks are positioned where surge requirements and strategic industries are most vulnerable to disruption. A comprehensive demand analysis across Defence, freight, agriculture, and emergency services, mapped geographically, is therefore essential to identify priority nodes and avoid merely providing a perception of redundancy. Benchmarking this analysis against International Energy Agency requirements would, at the very least, align national commitments with genuine preparedness rather than merely meeting minimal compliance standards. Distribution infrastructure also requires systematic investigation, as pipelines, rail networks, sovereign-flagged shipping, and road haulage could provide the arteries through which resilience flows. Without prioritised investment in these links, even expanded stocks would remain inert, unable to sustain operations in contested environments. Medium-term measures must therefore seek to connect evidence-based planning with targeted infrastructure development to convert redundancy into practical sovereign preparedness.

Short-term measures

Liquid fuels are, and will continue to be, a fundamental pillar of the Australian economy and a vital enabler of military power for the foreseeable future. Without redundancy, Defence surge requirements and critical services could be paralysed within days, undermining both national resilience and economic stability simultaneously. Stabilising this must begin with measures that immediately buffer the system against foreseeable shocks, creating space to plan deeper reforms. Mandating increased diesel and jet fuel stockholdings under the Liquid Fuel Security Act is straightforward when supported by transparent reporting and compliance mechanisms to ensure physical redundancy. Extending targeted support for the remaining refineries until alternative capacity is secured is equally straightforward and essential, ensuring that Australia's minimal sovereign production capability is maintained. These measures will not resolve structural dependency, but they will provide crucial insurance against cascading failures that may occur during crises, anchoring short-term stability within a longer-term reform pathway.

Towards a Unified National Fuel Strategy

Taken in isolation, none of the prescribed measures will address the depth of Australia's fuel vulnerability, which is structural, embedded, and multidimensional. Stockholding uplifts would deliver crucial buffers but cannot mitigate against Australia's structural dependency; while distribution upgrades could resolve bottlenecks, they fail to reduce Australia's import dependence. Domestic LCLF production would provide a sovereign supply solution but requires time, investment, and social approval. Only by integrating these aspects within a national fuel strategy can preparedness, economic stability, and climate responsibility be truly aligned as inseparable priorities. Such a strategy would balance immediate stabilisation with systematic investigation and long-term structural reform, creating coherence across Australia's Defence needs, economic security, and emissions commitments. The alternative is to continue with fragmented interventions, or to do nothing, leaving Australia vulnerable to cascading failures when contested environments inevitably challenge the longstanding assumptions about our market-based approach. Therefore, this integration is not merely a policy preference but a crucial condition for Australia's national resilience in an era of increasing sovereign risk.

Australia's heavy reliance on imported liquid fuels, essential for the country's operations, should be regarded as a sovereign capability issue rather than leaving it to commercial markets to resolve. A unified national fuel strategy could embed resilience into legislation, strengthen institutions, and coordinate policies across different national priorities, ensuring that no critical sector is unprepared for national emergencies. In this way, Defence's deterrence-by-denial strategy would be supported by reliable fuel supplies, economic stability would be preserved through resilient freight, mining, and agricultural networks, and environmental objectives would be advanced via sovereign low-carbon fuel production. This analysis shows that without an integrated national fuel strategy, Australia remains dangerously vulnerable; however, with such a strategy, fuel can become a fundamental part of the nation's capability and capacity. Developing this strategy is both urgent and feasible, requiring a clear framework that balances national security, economic stability, and environmental responsibility as interconnected priorities to foster long-term national resilience.

Bibliography

Airlines for Australia and New Zealand. "Submission to the 'Unlocking Australia's low carbon liquid fuel opportunity' consultation paper." July 2024. <https://www.infrastructure.gov.au/sites/default/files/documents/lclf2024-airlines-for-australia-and-new-zealand.pdf>.

Air and Space Power Centre. "Decreasing reliance on fossil fuels to increase defence capability." Royal Australian Air Force, December 5, 2022. <https://airpower.airforce.gov.au/sites/default/files/2022-12/Decreasing%20Reliance%20On%20Fossil%20Fuels%20To%20Increase%20Defence%20Capability.pdf>.

Ashurst. "Japan's New Energy Plan." Ashurst.com. Accessed July 28, 2025. <https://www.ashurst.com/en/insights/japans-new-energy-plan/>.

Austrade. "Australia looks to sustainable fuels to secure energy future." Australian Trade and Investment Commission, 2025. [https://international.austrade.gov.au/en/news-and-analysis/news/austrade.gov.au/en/news-and-analysis/news/australia-looks-to-sustainable-fuels-to-secure-energy-future](https://international.austrade.gov.au/en/news-and-analysis/news/australia-looks-to-sustainable-fuels-to-secure-energy-future).

Australian Energy Producers. "AEP Key Statistics 2024." June 2024. https://energyproducers.au/wp-content/uploads/2024/06/AEP_KS24_Web2.pdf.

Australian Government. A Future Made in Australia Fact Sheet. Budget 2024-25. Canberra, ACT: The Treasury, 2024. <https://archive.budget.gov.au/2024-25/factsheets/download/factsheet-fmia.pdf>.

Australian Industrial Transformation Institute. Australian sovereign capability and supply chain resilience. Adelaide, SA: Flinders University, 2021. <https://www.aph.gov.au/DocumentStore.ashx?id=bbf63058-99e8-4d20-8dd0-ea9ce41f79db&subId=715388>.

Australian Institute of Petroleum. Report on Australia's oil refinery industry. Submission to the House of Representatives Standing Committee on Economics. Melbourne, VIC: AIP, September 2017. <https://www.aip.com.au/sites/default/files/download-files/2017-09/APH%20Economics%20Committee%20Report%20-%20Oil%20Refining%20Industry.pdf>.

Australian Parliament House. Fuel Security Bill 2021. Bills Digest No. 81, 2020–21. Canberra, ACT: Parliamentary Library, June 17, 2021. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/FlagPost/2021/June/Fuel_Security_Bill_2021.

Australian Strategic Policy Institute. The trade routes vital to Australia's economic security. Special Report 203.

Canberra: ASPI, 2024. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2024-03/SR203%20Trade%20routes%20vital%20to%20Australia's%20economic%20security_1.pdf.

Australian Workers' Union. "Submission to the 'Unlocking Australia's low carbon liquid fuel opportunity' consultation paper." July 2024. <https://www.infrastructure.gov.au/sites/default/files/documents/lclf2024-australian->

workers-union.pdf.

Basalla, Michael, Brett Berger, and David Abbot. "The Great East Japan Earthquake: A Case Study in Civil-Military Coordination." *Joint Force Quarterly* 68 (2013): 25–31. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-68/JFQ-68_25-31_Basalla-Berger-Abbot.pdf.

Beaver, Wilson. "When the tank's empty: Australia's impoverished energy security." *The Interpreter*. Lowy Institute, June 21, 2022. <https://www.lowyinstitute.org/the-interpreter/when-tank-s-empty-australia-s-impoverished-energy-security>.

Bioenergy Australia. "Submission to the 'Unlocking Australia's low carbon liquid fuel opportunity' consultation paper." July 2024. <https://www.infrastructure.gov.au/sites/default/files/documents/lclf2024-bioenergy.pdf>.

"Biofuels Boost Australia's Economy: The Growing Impact of Energy Crops." *Biomass Producer*. Accessed September 4, 2025. <https://biomassproducer.com.au/agricultural-and-resource-management/biofuels-boost-australias-economy-the-growing-impact-of-energy-crops/>.

Blackburn, John. *Australia's Liquid Fuel Security*. Report for NRMA Motoring and Services. February 2013. <https://www.aph.gov.au/DocumentStore.ashx?id=86e8dfbc-1467-47fe-ad1e-bc635407ecf8&subId=301736>.

Blackburn, John. *Australia's Liquid Fuel Security Part 2*. Report for NRMA Motoring & Services. February 2014. <https://www.aph.gov.au/DocumentStore.ashx?id=677ff8dd-ce35-40ee-9af8-bfec1e43d125&subId=301736>.

Bureau of Infrastructure and Transport Research Economics. *Australian aggregate freight forecasts – 2022 update*. Research Report 154. Canberra: Commonwealth of Australia, 2022. https://www.bitre.gov.au/sites/default/files/documents/bitre_rr154.pdf.

Bureau of Infrastructure and Transport Research Economics. "Transport Energy and Environment." In *Australian Infrastructure and Transport Statistics Yearbook 2024*. Canberra: Commonwealth of Australia, 2024. <https://www.bitre.gov.au/publications/2024/australian-infrastructure-and-transport-statistics-yearbook-2024/transport-energy-environment>.

Campbell, Rod. "Fuel security in Australia and the International Energy Agency's 10-point plan." *The Australia Institute*, October 1, 2024. <https://australiainstitute.org.au/report/fuel-security-in-australia-and-the-international-energy-agencys-10-point-plan/>.

"Chapter 4. Threats to Australia's liquid fuel security." *Parliament of Australia*. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Rural_and_Regional_Affairs_and_Transport/Transport_energy_resilience/Report/c04.

Clean Energy Finance Corporation. "Biofuels and Transport: An Australian opportunity." *Submission to the Senate, Rural and Regional Affairs and Transport References Committee*. n.d. <https://www.aph.gov.au/->

[/media/Estimates/ec/supp2324/DCCEEW/Senator_Van_CEFC_Biofuels_and_Transports.pdf](#).

Clean Energy Finance Corporation and Deloitte. Refined Ambitions: Exploring Australia's Low Carbon Liquid Fuel Potential. Sydney, NSW: Clean Energy Finance Corporation, 2025. <https://www.cefc.com.au/media/jh3gvm14/refined-ambitions-exploring-australia-s-low-carbon-liquid-fuel-potential.pdf>.

Cole, Benjamin. "Decreasing Reliance on Fossil Fuels to Increase Defence Capability." Air & Space Power Centre, Australian Air Force, December 2022. <https://airpower.airforce.gov.au/sites/default/files/2022-12/Decreasing%20Reliance%20On%20Fossil%20Fuels%20To%20Increase%20Defence%20Capability.pdf>.

"A Conflict in the Pacific Could Prompt a Fight Over the Strait of Malacca." The Maritime Executive, July 2, 2023. <https://maritime-executive.com/editorials/a-conflict-in-pacific-could-prompt-a-fight-over-strait-of-malacca>.

CSIRO. Opportunities and Priorities for a Low Carbon Liquid Fuel Industry in Australia. Canberra, ACT: CSIRO, 2025. <https://www.csiro.au/-/media/Missions/TNZ/Opportunities-and-priorities-for-a-Low-Carbon-Liquid-Fuel-Industry.pdf>.

Deloitte. Securing our Fuel Future: Resilience Through Low Carbon Liquid Fuels. Report for Bioenergy Australia. Sydney, NSW: Deloitte, 2025. https://impact-on-sustainable-aviation.org/shared-files/2730/?Australia_Deloitte_Resilience%20through%20low%20carbon%20liquid%20fuels.pdf&download=1.

Department of Climate Change, Energy, the Environment and Water. "Australia's fuel security." DCCEEW. Accessed August 14, 2025. <https://www.dcceew.gov.au/energy/security/australias-fuel-security>.

Department of Climate Change, Energy, the Environment and Water. "IEA Programme and Treaty." DCCEEW. <https://www.dcceew.gov.au/energy/international-activity/iea-program-treaty>.

Department of Climate Change, Energy, the Environment and Water. "Liquid Fuel Security - Actions to Support Australia's Fuel Security." QB23-000039. January 2023.

Department of Climate Change, Energy, the Environment and Water. Liquid Fuel Security Review—Final Report. Canberra, ACT: DCCEEW, October 2020. <https://www.dcceew.gov.au/sites/default/files/documents/72895-1.pdf>.

Department of Climate Change, Energy, the Environment and Water. Liquid Fuel Security Review—Interim Report. Canberra, ACT: DCCEEW, April 2019. <https://www.dcceew.gov.au/sites/default/files/documents/liquid-fuel-security-review-interim-report.pdf>.

Department of Defence. Defence Strategic Review 2023: National Defence. Canberra: Commonwealth of Australia, 2023. <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>.

Department of Defence. "Energy resilience, emissions targets in Defence sights." October 28, 2024. <https://www.defence.gov.au/news-events/news/2024-10-28/energy-resilience-emissions-targets-defence-sights>.

Department of Infrastructure, Transport, Regional Development, Communications, and the Arts. "Establishing a Strategic Maritime Fleet of Australian Vessels." Submission, 2023. <https://www.infrastructure.gov.au/sites/default/files/documents/establishing-a-strategic-maritime-fleet-of-australian-vessels-aip.pdf>.

Department of Infrastructure, Transport, Regional Development, Communications, and the Arts. A Future Made in Australia: Unlocking Australia's low carbon liquid fuel opportunity - Consultation Paper. Canberra, ACT: Commonwealth of Australia, 2024. <https://www.infrastructure.gov.au/sites/default/files/documents/low-carbon-liquid-fuels-consultation-paper.pdf>.

Dossor, Rob. "Australian oil refineries and fuel security." FlagPost (blog). Parliamentary Library, Parliament of Australia, December 10, 2020. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/FlagPost/2020/December/Oil_refineries_and_fuel_security.

Edelman Global Advisory. "Japan's Seventh Strategic Energy Plan." EdelmanGlobalAdvisory.com, January 7, 2025. <https://www.edelmanglobaladvisory.com/japans-seventh-strategic-energy-plan>.

"Falling well short: FOI documents reveal shocking state of nation's fuel security preparedness." Defence Connect, January 14, 2025. <https://www.defenceconnect.com.au/geopolitics-and-policy/15357-falling-well-short-foi-documents-reveal-shocking-state-of-nations-fuel-security-preparedness>.

Finnish Government. "Finland releases 369,000 barrels of crude oil to the market from its emergency stockpiles." Media release. Valtioneuvosto.fi, April 8, 2022. <https://valtioneuvosto.fi/en/-/1410877/finland-releases-369-000-barrels-of-crude-oil-to-the-market-from-its-emergency-stockpiles>.

Floyd, Nicholas. "Just in Time: Logistics and Legislative Preparedness in Strategic Competition." The Cove, October 21, 2021. <https://cove.army.gov.au/article/just-time-logistics-and-legislative-preparedness-strategic-competition>.

Fuel Security Act 2021 (Cth). Compilation No. 2, October 17, 2024. <https://www.legislation.gov.au/F2024C00676/latest/text>.

Future Battery Industries CRC. An overview of Australia's mining vehicle and mining equipment electrification.

Report, November 2023. https://fbicrc.com.au/wp-content/uploads/2023/11/FBICRC_Mobile-Mine-Report-VFINAL.pdf.

Garside, Ben. The Australian Defence Force and its future energy requirements. Special Report Issue 187.

Canberra, ACT: Australian Strategic Policy Institute, 2022. <https://www.aspi.org.au/report/australian-defence-force-and-its-future-energy-requirements>.

Government of Finland. Security Strategy for Society. Helsinki: Prime Minister's Office,

2017. <https://helda.helsinki.fi/server/api/core/bitstreams/1a7333a5-8480-4241-92dc-660037193aca/content>.

Grattan Institute. The next industrial revolution: Transforming Australia to flourish in a net-zero world.

Melbourne, VIC: Grattan Institute, 2022. <https://grattan.edu.au/report/next-industrial-revolution/>.

Greet, Neil. "Enabling energy security in a profoundly changing world." Accelerating Energy Transition Series.

Engineers Australia, July 2024.

Griffith Asia Institute. Future made in Australia? Evaluating Australia's 2024 green energy related policies and its potential impact on Asia. Brisbane, QLD: Griffith University, 2024.

https://www.griffith.edu.au/data/assets/pdf_file/0031/1967143/Future-made-in-Australia-policy-brief.pdf.

Grudnoff, Matt. Over a barrel: A review of Australia's liquid fuel security. Discussion Paper. Canberra, ACT: The Australia Institute, April 2022. https://australiainstitute.org.au/wp-content/uploads/2022/04/P1036-Over-a-barrel_liquid-fuel-security-WEB.pdf.

Infrastructure Australia. A Pathway to Infrastructure Resilience. Advisory Paper 1. Canberra: Commonwealth of Australia, 2021. [https://www.infrastructureaustralia.gov.au/sites/default/files/2021-08/Advisory%20Paper%201%20-](https://www.infrastructureaustralia.gov.au/sites/default/files/2021-08/Advisory%20Paper%201%20-%20A%20pathway%20to%20Infrastructure%20Resilience%20FINAL.pdf)

[%20A%20pathway%20to%20Infrastructure%20Resilience%20FINAL.pdf](https://www.infrastructureaustralia.gov.au/sites/default/files/2021-08/Advisory%20Paper%201%20-%20A%20pathway%20to%20Infrastructure%20Resilience%20FINAL.pdf).

International Energy Agency. "Finland's Legislation on Oil Security." IEA. Accessed July 28, 2025. <https://www.iea.org/articles/finland-s-legislation-on-oil-security>.

International Energy Agency. "How Japan Thinks About Energy Security." Center for Strategic and International Studies, 2020. <https://www.csis.org/analysis/how-japan-thinks-about-energy-security>.

International Energy Agency. "Japan Oil Security Policy – Analysis." IEA. Accessed July 28, 2025. <https://www.iea.org/articles/japan-oil-security-policy>.

International Energy Agency. "Oil Stocks of IEA Countries." IEA Data and Statistics. Accessed July 28, 2025. <https://www.iea.org/data-and-statistics/data-tools/oil-stocks-of-iea-countries>.

Joint Standing Committee on Foreign Affairs, Defence and Trade. Inquiry into the Defence Annual Report 2019–20. Canberra: Commonwealth of Australia, 2021. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/DefenceARreport19-20/Report.

King, Catherine. "Have your say on a future made in Australia: unlocking Australia's low carbon liquid fuel opportunity." Media release. Department of Infrastructure, Transport,

Regional Development and Local Government, 2024. <https://minister.infrastructure.gov.au/c-king/media-release/have-your-say-future-made-australia-unlocking-australias-low-carbon-liquid-fuel-opportunity>.

Lockhorst, Raelene. "Australia must boost investment to ensure strategic fuel security." *The Strategist*, October 20, 2022. <https://www.aspistrategist.org.au/australia-must-boost-investment-to-ensure-strategic-fuel-security/>.

Lockhorst, Raelene. "The urgent need for a strategic overhaul in Australia's Defence approach to fuel resilience." *The Strategist (ASPI)*, September 19, 2024. <https://www.aspistragist.org.au/the-urgent-need-for-a-strategic-overhaul-in-australias-defence-approach-to-fuel-resilience/>.

Maeda, Reina. "Japan maintains LPG stockpile levels on trade concerns." *Argus Media*, July 15, 2025. <https://www.argusmedia.com/en/news-and-insights/latest-market-news/2710429-japan-maintains-lpg-stockpile-levels-on-trade-concerns>.

Ministry of Economic Affairs and Employment. "Reserve stocks and preparedness planning secure energy supply." *tem.fi*. Accessed July 28, 2025. <https://tem.fi/en/security-of-energy-supply>.

Ministry of Economy, Trade and Industry. *Strategic Energy Plan*. Tokyo: METI, April 2014. https://www.enecho.meti.go.jp/en/category/others/basic_plan/pdf/4th_strategic_energy_plan.pdf.

National Emergency Supply Agency. "The National Emergency Supply Agency." *Huoltovarmuuskus*.

Accessed July 28, 2025. <https://www.huoltovarmuuskus.fi/en/organisation/the-national-emergency-supply-agency>.

NSW Department of Primary Industries. *Diesel Use in NSW Agriculture and Opportunities to Support Net Zero*. Report, 2021. https://www.dpi.nsw.gov.au/data/assets/pdf_file/0011/1321796/mov3ment-diesel-use-in-ag.pdf.

Observer Research Foundation. "Securing Sea Lines of Communication in Asia." October 15, 2024. <https://www.orfonline.org/research/securing-sea-lines-of-communication-in-asia>.

Office of Impact Analysis. *Regulation Impact Statement: Securing Australia's Domestic Fuel Stocks and Refining Capability*. Canberra, ACT: Department of the Prime Minister and Cabinet, May 2021.

<https://oia.pmc.gov.au/sites/default/files/posts/2021/08/Fuel%20Security%20RIS%20-%20Securing%20Australia%E2%80%99s%20Domestic%20Fuel%20Stocks%20and%20Refini.pdf>.

Oil & Gas Journal. "BP to close Kwinana oil refinery." 2020. <https://www.ogj.com/refining-processing/refining/operations/article/14186463/bp-to-close>.

"Oil Stockpiling Act (Act No. 96 of 1975)." *Japanese Law Translation*. Accessed July 28, 2025. <https://www.japaneselawtranslation.go.jp/en/laws/view/3000/en>.

Pantges, Strati. "Fuel Security and Minimum Stockholding Obligations: What it means for you and your business." McCullough Robertson, September 30, 2024. <https://mccullough.com.au/2024/09/30/fuel-security-and-minimum-stockholding-obligations-what-it-means-for-you-and-your-business/>.

Regional Australia Institute. "Towards Net Zero - Fossil Fuel Dependency in Regional Australia." Report, 2025. <https://regionalaustralia.org.au/common/Uploaded%20files/Files/2025/ISIP/Sustainability/Embargoed>

%20Fossil%20Fuel%20Dependency%20in%20Regional%20Australia.pdf. Sara, Tyson. "Australia should grow its own fuel." The Strategist, March 18, 2024. <https://www.aspistragist.org.au/australia-should-grow-its-own-fuel/>.

Shimodaira, Noboru. "The JMSDF's Resilient Power for Civil Society: Lessons from the Great East Japan Earthquake." Naval War College Review 65, no. 1 (2012): 101–15. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1221&context=nwc-review>.

Shoebridge, Michael. "Australia's fuel insecurity is not hypothetical." The Strategist, August 2, 2023. <https://www.aspistragist.org.au/australias-fuel-insecurity-is-not-hypothetical/>.

Smith, Hanna. "Hybrid Operations and the Importance of Resilience: Lessons From Recent Finnish History." Carnegie Endowment for International Peace, February 2018. <https://carnegieendowment.org/research/2018/02/hybrid-operations-and-the-importance-of-resilience-lessons-from-recent-finnish-history?lang=en>.

Swann, Tom. "Submission: Interim Report on the Liquid Fuel Security Review." The Australia Institute, July 2019. https://australiainstitute.org.au/wp-content/uploads/2020/12/P739-Liquid-Fuel-Security-Submission-WEB_0.pdf.

Yates, Athol, and Neil Greet. "Energy Security for Australia: Crafting a comprehensive energy security policy." Engineers Australia, 2014.

This page is intentionally blank



What is the ‘International Rules-based Order’? Does the use of this terminology advance Australia’s foreign policy interests?

Mr Cary Scott-Kemmis

About the Author



Mr Cary Scott-Kemmis has almost two decades of experience across multiple Commonwealth portfolios. In 2023, he was selected to attend the Defence and Strategic Studies Course (DSSC) at the Australian War College—an appointment reserved for leaders assessed as having the potential to influence defence and national security policy both domestically and at the international level. During the course, Cary focused on strategic risk, Indo-Pacific security dynamics, and whole-of-government approaches to complex crises. Cary graduated from DSSC with a Master of National Security and Strategy from Deakin University. While attending the DSSC, he received the Geddes Gavel Award for academic achievement.

Summary

This paper argues that for Australia to defend the 'rules-based order', but, most critically, to convince others to do so, it is essential to have clarity about what the 'rules-based order' is and how it is perceived. This paper addresses two principal questions. First, what is the 'rules-based international order' frequently invoked by Australia and other States? Second, does Australia's use of 'rules-based order' terminology support Australia's foreign policy interests? To answer these questions, this paper will consider and examine: the emergence of 'rules-based order' terminology; the intersection between the 'rules-based order' and other frameworks, such as the 'liberal international order' and international law; the narratives regarding the order's content, its emergence, and attacks on the order; and who is employing 'rules based-order' terminology. This paper will demonstrate that this term is unfit for use as a tool by Australia to mobilise international action, particularly in the Indo-Pacific, in line with Australia's foreign and security policy interests. This paper offers recommendations for how Australia should seek to characterise how a 'rules-based order', or an international 'rule of law', should operate to support Australia's international interests. It concludes with a summary of the paper's findings and ideas for possible future research.



Image: British Institute of International and Comparative Law

Introduction

References to the ‘international rules-based order’ have become a ubiquitous feature of Australia’s foreign and security policy over the last fifteen years. These references have often been accompanied by assertions that this order is a critical national interest, it is under threat and that Australia and other States must defend it.

For instance, the 2023 Defence Strategic Review found that working with partners to defend the “global rules-based order” ranked alongside the “defen[ce] of Australia” as one of the Defence Force’s five top priorities.¹ In July 2016, Australia’s Foreign Minister, Julie Bishop, emphasised that all South China Sea claimants “[had] benefited enormously from the rules-based international order.”² Two years later, Bishop told a La Trobe University gathering that “the test of our generation” was whether “we defended and strengthened [the] rules-based order”.³ Australia’s Prime Minister, Anthony Albanese, said in October 2023 that it was the “responsibility of every nation that has benefitted from the stability and prosperity of the international rules-based order to work together and protect it”.⁴

While Australia and other States clearly imbue this ‘order’ with considerable importance, it is less clear precisely how it functions and what its rules are. In a lengthy study, Sellars observed that “the more we discuss [the rules-based order], the more elusive it becomes.”⁵ Chalmers remarked that “[UK] official documents and speeches rarely define what [the order is] as if it is widely recognised.”⁶ For Porter, describing it is akin to “wrestling with fog.”⁷ Two years after characterising the order’s defence as the acid test of a generation, Bishop conceded that the concept was, in fact, something of a “semantic innovation”.⁸

Some, such as Singapore’s Kausikan, insist that a lack of definitional clarity is

¹ ‘National Defence: Defence Strategic Review 2023’, Department of Defence, page 6, accessed 2 June 2023, www.defence.gov.au/about/reviews-inquiries/defence-strategic-review.

² “Australia Supports Peaceful Dispute Resolution in the South China Sea”, Australian Government Department of Foreign Affairs and Trade, last modified 12 July 2016, <https://www.foreignminister.gov.au/minister/julie-bishop/media-release/australia-supports-peaceful-dispute-resolution-south-china-sea>.

³ “La Trobe University Lecture and Conversation”, Australian Government Department of Foreign Affairs and Trade, last modified 11 April 2018, <https://www.foreignminister.gov.au/minister/julie-bishop/speech/la-trobe-university-lecture-and-conversation>.

⁴ Prime Minister, Anthony Albanese (@albomp), Instagram photo, 28 October 2023.

⁵ ‘Australia and the Rules-Based International Order’, Australian Institute of International Affairs, Tyler, Gyngell and Wakefield, page 9, accessed 27 July 2023, <https://www.internationalaffairs.org.au/publication/australia-and-the-rules-based-international-order/>.

⁶ ‘Which Rules? Why There Is No Single “Rules-Based International System”’, Royal United Services Institute, Malcolm Chalmers, accessed 12 August 2023, 1, www.rusi.org/explore-our-research/publications/occasional-papers/which-rules-why-there-no-single-rules-based-international-system.

⁷ ‘Wrestling with Fog: On the Elusiveness of Liberal Order’, War on the Rocks, Patrick Porter, last modified 15 July 2020, <http://warontherocks.com/2020/07/wrestling-with-fog-on-the-elusiveness-of-liberal-order/>.

⁸ ‘Rules-Based Order - Lowy Institute’, Lowy Institute, 18 September 2023, <https://interactives.loyyinstitute.org/features/rules-based-order/>.

immaterial. The term is a harmless bromide, or 'Rashōmon term', with its value rooted in its ambiguity.⁹ Others contest that perspective and view the term as politicised. China's Ambassador told the UN Security Council in 2023 that the term was an "ambiguous formulation", distinct from international law, which served as a "back door to double standards and exceptionalism."¹⁰

This paper argues that for Australia to defend the 'rules-based order', but, most critically, to convince others to do so, it is essential to have clarity about what the 'rules-based order' is and how it is perceived. This paper, therefore, addresses two principal questions. First, what is the 'rules-based international order' so frequently invoked by Australia and others? Second, does Australia's use of 'rules-based order' terminology support Australia's foreign policy interests?

To answer these questions, this paper will consider the emergence, use and academic and political narratives surrounding the 'rules-based international order'¹¹ to demonstrate that this term is unfit for use as a tool by Australia to mobilise international action, particularly in the Indo-Pacific, in line with Australia's foreign and security policy interests.

This paper will show that while users of 'rules-based international order' terminology typically describe an order with roots in the international institutions and architecture developed in the immediate aftermath of the Second World War, the term itself, or synonyms thereof, were not used by the Australian Government until the late 2000s. Further, its initial usage at the political level in Australia was in the context of an alleged breach of the 'order' by Australia itself, weakening the credibility of Australia's purported fidelity to the order (*Chapter One*). The 'rules-based international order' is treated, particularly in the US and Australia, as synonymous with the 'liberal international order'. This latter concept has a longer history, with consistent usage dating back to the 1970s. The core tenets of this order include the promotion of 'liberal' values, including liberal democracy, human rights, and the hegemony of the United States ('US'). This risks the perception that when Australia invokes 'rules-based order' terminology, it argues for the right to promote liberal democracy, a privileged role for liberal democracies within the order and the US' right to hegemony (*Chapter Two*).

Conceptions of the 'order's' content, scope, operation, and temporal emergence are varying and often irreconcilable, weakening the coherence and appeal of the terminology (*Chapter Three*). In contrast, the narrative of the order's fraying reveals an emphasis, by Australia and others, on liberal conceptions of the order, such as US hegemony and liberal democracy promotion that are unlikely to resonate globally (*Chapter Four*). An exploration of the relationship between international law and the 'order' highlights that an overemphasis on references to alleged breaches of the order, as opposed to international law, politicises such claims and may be perceived as designed to mask the shortcomings of accusing States in adhering to international law (*Chapter Five*). In contrast, an exploration of the States that are using the 'rules-based

⁹ 'Perspectives: What (and Whose) Rules Based Order (RBO)?', Asialink, University of Melbourne, Bilahari Kausikan, last modified 17 August 2021, <https://asialink.unimelb.edu.au/insights/what-and-whose-rules-based-order-rbo>.

¹⁰ 'Research Guides: UN Security Council Meetings & Outcomes Tables: 2023 (S/RES/2672-)', United Nations. Dag Hammarskjöld Library, accessed 26 August 2023, <https://research.un.org/en/docs/sc/quick/meetings/2023>.

¹¹ There are several key synonyms for this term, including: the 'global rules-based order', the 'rules-based global order' and the 'rules-based international order'. These are captured in **Table 1**.

order' terminology supports the conclusion that the term is viewed in political terms and is of less appeal to States beyond the West (*Chapter Six*). This paper concludes with recommendations for how Australia should seek to characterise how a 'rules-based order', or an international 'rule of law', should operate to support Australia's international interests (*Chapter Seven*) and a summary of the paper's findings and ideas for possible future research (*Conclusion*).

Research for this paper has been limited to English-language official and academic sources. As a result, while this paper's assessment of the reception of 'rules-based order' terminology in non-English speaking States does draw on some perspectives of individuals from these countries, this has been limited to authors who have published in English. As a result, this paper places greater emphasis on the likely perception of the use of this terminology.

This page is intentionally blank

Chapter 1: The emergence of 'rules-based international order' terminology

This Chapter will demonstrate that 'rules-based order' terminology emerged internationally in the 1990s and was first used by the Australian Government fifteen years ago. Its emergence at the political level in Australia was in the context of allegations that Australia was contributing to the order's destruction. These factors impact Australia's credibility, particularly when it seeks to rally others to defend the 'order'.

The study of, and attempts to define, 'international order' has long been a pursuit of scholars. As with many terms, its meaning is contested. Through a synthesis of the common features of definitions advanced by Brands and Ikenberry, 'international order' can be viewed as a set of commonly understood 'rules, norms, principles, and institutions' that govern relations between States on the international plane.¹² In *World Order*, Kissinger defined 'international order' as 'a set of commonly accepted rules that define the limits of permissible action and a balance of power that enforces restraint when rules break down, preventing one political unit from subjugating all others.' In this regard, 'rules', in one form or another, are envisaged as at the core of any international order.¹³

Emergence of the term globally

The term 'the rules-based international order', however, has a shorter history. While many academic and official accounts identify the intensive international institution building that followed the Second World War as the origin point of the rules and institutions at the 'rules-based order's' core, the *term itself* only began to gain traction within academic and public policy discourse in the 1990s. In one example of an early reference, Sarty, writing in 1993 in *Foreign Affairs*, referred to Canada's "promotion since 1945 of an open, stable, rules-based international order", thus situating post-war institutions at the order's core.¹⁴ Similarly, in 1994, Wang queried what the UN Security Council's failure to resolve the Iraq-Iraq conflict of the 1980s would portend for the "prospects for a rules-based international order."¹⁵

Governments' consistent usage of the term can also be traced to the mid-1990s. Canada's 1995 '*Canada in the World*' foreign policy statement observed that international institutions are "crucial to ... a rules-based global governance system".¹⁶ At the 1995 Nuclear Non-Proliferation Treaty conference, Ireland observed that "a rules-based international order and strong international institutions [are] of fundamental

¹² 'Understanding the Current International Order', RAND Corporation, Michael J. Mazarr et al, last modified 19 October 2016, 7, www.rand.org/pubs/research_reports/RR1598.html.

¹³ Henry Kissinger, *World Order*, (Penguin Books, 2014), page 9.

¹⁴ Leigh Sarty, "Sunset Boulevard Revisited - Canadian Internationalism after the Cold War," *International Journal* 48, no. 4 (Autumn 1993): 749-777.

¹⁵ Erik B. Wang, "The Iran-Iraq War Revisited: Some Reflections on the Role of International Law," *Canadian Yearbook of International Law* 32 (1994): 83-110.

¹⁶ 'Canada in the World: Canadian Foreign Policy Review 1995', Canadian Government, Department of Foreign Affairs and International Trade, accessed 17 July 2023, http://www.dfait-maeci.gc.ca/foreign_policy/cnd-world/menu-en.asp

importance".¹⁷

Google Ngram¹⁸ searches for the use of the term, and minor variations thereof, provide support for the above conclusions regarding the terminology's emergence.

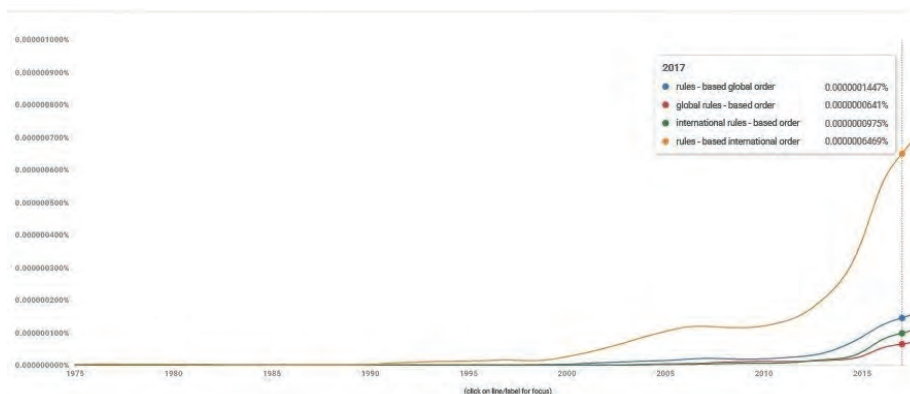


Table 1: Rules-based global order v international rules-based order – comparison of frequency of mentions in all English-language sources between 1975 and 2019 (Source: Google Ngram Viewer).

As **Table 1** indicates, consistent usage of the 'rules-based international order' began in the 1990s, with usage increasing exponentially from the late 1990s. Inflection points of usage are identifiable in the early 2000s and from approximately 2011/12 onwards.

Table 2 (below) shows that the term 'liberal international order' – which Chapter 2 demonstrates is largely employed as a synonym for the 'rules-based international order' in Australia and the US – began to gain prominence almost three decades earlier. The use of the 'liberal international order' and the 'rules-based international order' have increased in tandem. However, the former term, which enjoys greater prominence in official policy and academic literature in the US, is used more frequently, and its usage is increasing at a greater exponential rate than the 'rules-based order'.

¹⁷ Vylegzhanin, Alexander and Magomedova, Olga, 'The Term "Rules-Based International Order" in International Legal Discourses', *Moscow Journal of International Law*, July 2021, 40, <https://doi.org/DOI: 10.24833/0869-0049-2021-2-35-60>.

¹⁸ *Google Ngram* is a search function that displays a graph showing how specific phrases have occurred in a corpus of books over selected years. Further information is available at: <https://books.google.com/ngrams/info>

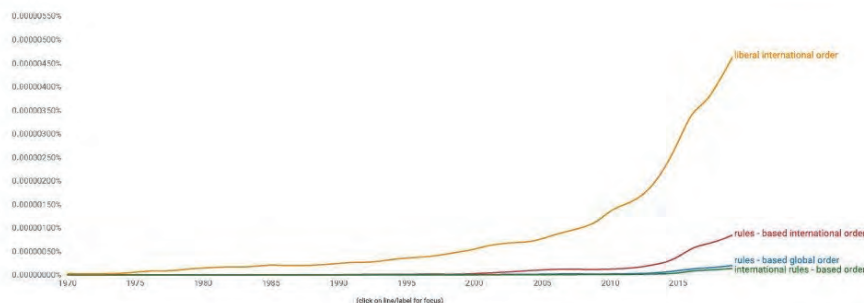


Table 2: Rules-based international order v liberal international order – comparison of the frequency of mentions in all English-language sources between 1970 and 2019 (Source: Google Ngram Viewer).

Emergence in Australia

In Australia, the ‘rules-based international order’ terminology experienced an unorthodox rise for a concept considered by both major parties to be at the core of Australia’s contemporary foreign policy interests. In 2003, when setting out the core tenets of the opposition’s foreign policy, then foreign affairs spokesperson, Kevin Rudd, outlined that “an international rules-based system based on the [UN]” represented one of three pillars of Labor’s foreign policy, alongside the US alliance and engagement with Asia.¹⁹

In contrast, Rudd charged that the Howard Government had “effectively junk[ed]” the rules-based order in place “for more than half a century” through its participation in the 2003 US-led invasion of Iraq. Rudd’s approach mirrored a similar rhetorical pattern in the US, with Democrats charging that the Bush Administration had breached a core rule of this ‘order’, the prohibition on aggressive war enshrined in Article 2(4) of the UN Charter, by invading Iraq.²⁰ While in opposition, Rudd consistently employed ‘rules-based order’ terminology, including in international engagements in China and elsewhere.²¹

In 2008, then-Prime Minister Rudd told the Brookings Institution that global harmony would depend on China “[participating] and acting in accordance with the rules of that ... global and regional rules-based order”.²² This was the first identifiable occasion of an Australian Government official using the term. Similarly, the 2009 Defence White

¹⁹ Australian Labor Party, ‘Kevin Rudd - The Three Pillars of Labor’s National Security Policy’, Bibliothek der Friedrich-Ebert-Stiftung, 15 October 2003, <https://library.fes.de/aussies/2003/1003/20006086.html>.

²⁰ Peter Beinart, ‘The Vacuous Phrase at the Core of Biden’s Foreign Policy’, *The New York Times*, 22 June 2021, <https://www.nytimes.com/2021/06/22/opinion/biden-foreign-policy.html>.

²¹ ‘Australia and China: A Strong and Stable Partnership for the 21st Century’, Embassy of the Republic of China in Australia, 26 January 2005, <https://web.archive.org/web/20050126165251/http://au.china-embassy.org/eng/zagx/t142076.htm>.

²² ‘A Conversation with the Prime Minister of Australia, the Hon. Kevin Rudd MP’, The Brookings Institution, accessed 19 September 2023, <https://www.brookings.edu/events/a-conversation-with-the-prime-minister-of-australia-the-hon-kevin-rudd-mp/>.

Paper was the first official high-level policy document to refer to the 'order' that could be identified.²³ This document and the 2013 White Paper that followed it accorded the term significant prominence, describing it as one of Australia's primary 'strategic interests'.^{24 25}

Australia's 2016 Defence White Paper, which made 56 references to the 'rules-based global order', claimed that this order's stability was "essential for Australia's security and prosperity".²⁶ However, the term or similar could not be identified in any Defence White Papers before 2009.²⁷

References to 'order' and 'rules' in official material prior to 2009 provides no sense of a broader 'rules-based order' concept. For instance, the 2000 White Paper referred to a 'global security order', which the US played a 'major role' in maintaining.²⁸ Australia's 2017 Foreign Policy White Paper insisted that "determined diplomacy and strong partnerships" were required to "strengthen the rules-based international order", alongside 15 other references.²⁹ In contrast, Australia's 2003 Foreign Policy White Paper, the most immediate previous iteration, contained no references to the term nor any conceivable synonyms. Its references to 'order', for instance, included an assertion that States would need to organise "military coalitions" to deal swiftly and decisively with threats to "international order", an apparent and problematic reference to Iraq.³⁰ The thirty-two references to 'rules' emphasised the importance of specific international legal rules, including on trade and non-proliferation.

The 1997 Foreign Policy White Paper, which preceded the 2003 version, did not employ the term 'international rules-based order' either. The document made 13 references to 'rules', all of which related to specific international trade rules.³¹ The two references to 'order' referred to ASEAN's role in the "emerging regional order" and Japan's anticipated

²³ This conclusion is supported by research conducted by the Australian Institute for International Affairs and the Australian Committee of the Council for Security Cooperation in the Asia Pacific. See page 22, *'Australia and the Rules-Based International Order'*, Australian Institute of International Affairs, Tyler, Gyngell and Wakefield, accessed 27 July 2023, www.internationalaffairs.org.au/publication/australia-and-the-rules-based-international-order/.

²⁴ "Defence White Paper", Australian Government, Department of Defence, accessed 15 September 2023, <https://www.defence.gov.au/about/strategic-planning/defence-white-paper>.

²⁵ Department of Defence, "Defence White Paper".

²⁶ Department of Defence, "Defence White Paper".

²⁷ Department of Defence, "Defence White Paper".

²⁸ Department of Defence, "Defence White Paper".

²⁹ '2017 Foreign Policy White Paper' Australian Government, Department of Foreign Affairs and Trade, last modified 24 April 2020, page 2, www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/index.html.

³⁰ 'Advancing the National Interest: Australia's Foreign Policy and Trade White Paper 2003', Department of Foreign Affairs and Trade, Australia, accessed on 17 July 2023, page 46, <https://catalogue.nla.gov.au/catalog/2324418>

³¹ 'Advancing the National Interest: Australia's Foreign Policy and Trade White Paper 1997', Department of Foreign Affairs and Trade, Australia, accessed on 17 July 2023, <https://catalogue.nla.gov.au/catalog/2324418>

use of its diplomatic influence to “underpin the regional and global order”.³² A similar pattern is evident in the US and UK’s foreign policy and strategic literature. While the US’ 2010 National Security Strategy, released under President Obama, mentioned the term,³³ strategies released in 1994 and 2000 did not refer to the ‘rules-based order’ or similar formulations. In the UK, the term first appeared to gain traction in the 2008 National Security Strategy.³⁴

This analysis reveals two fundamental challenges for Australia. First, it is challenging to reconcile the importance of the order in contemporary Australian official statements and policy with the reality that the term has only entered the Government’s lexicon in the last fifteen years. Further, as an exploration of Foreign Policy and Defence White Papers, statements and documents released before 2009 has demonstrated, no synonymous terms are used. Rather, references to ‘rules’ tend to relate to specific and technical rules of international law. In contrast, references to ‘order’ tend to emphasise the leadership or hegemonic role of the US, seemingly independent of any broader international rules or architecture. It is challenging, therefore, for Australia to convince States in the Indo-Pacific, or indeed States generally, that the ‘rules-based order’, purportedly created in the ashes of the Second World War, is critical to all States’ national interests when Australia has only been articulating its importance over the last few decades.

The emergence of the term in the Australian political lexicon in the context of allegations that the Australian Government ‘junked’ the order through its participation in the US’ 2003 invasion of Iraq reinforces a perception that despite Australia’s (recent) promotion of the ‘rules-based order’ its track record in adhering to this order, as Australia itself defines it, is far from exemplary. As a result, Australia’s credibility is reduced when it seeks to rally support to defend or promote the ‘order’ or when it seeks to assert that other States, as later Chapters will explore, are seeking to overturn or erode the order, including by acting in violation of its core norms.

³² ‘Advancing the National Interest: Australia’s Foreign Policy and Trade White Paper 1997’, Department of Foreign Affairs and Trade, Australia, accessed on 17 July 2023, pages 29 and 66, <https://catalogue.nla.gov.au/catalog/2324418>

³³ ‘National Security Strategy – May 2010’, The White House, Washington, accessed on 1 September 2023, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

³⁴ ‘The National Security of the United Kingdom – Security in an interdependent world’, UK Cabinet Office, accessed 1 September 2023, <https://assets.publishing.service.gov.uk/media/5a7c68abed915d696ccfc92a/7291.pdf>

This page is intentionally blank

Chapter 2: The 'rules-based international order' v. the 'liberal international order'

While the 'rules-based international order' term emerged in the academic and official lexicon in the 1990s, a separate term, 'the liberal international order', had been used for many decades.³⁵ This Chapter will analyse the core elements of the 'liberal international order' and demonstrate that it and the 'rules-based international order' are effectively synonyms in Australia and the US. Accordingly, concepts such as US hegemony and the promotion of liberal democracy, which make up the liberal order and are explored in the first subsection of this Chapter, are imported into 'rules-based order' terminology, reducing its broader international appeal.

What is the 'liberal international order'?

Deudney and Ikenberry, two prominent academic authors on the 'liberal international order', explain that, at its heart, the 'post-war liberal order' is "aimed at 'making safe' liberal democracy in a world riven by tyranny, brutality, and intolerance".³⁶ This liberal order, they assert, has several essential features and norms.³⁷ The first is '**security co-binding**' between liberal States and the US, as hegemon. This is epitomised by mutual defence arrangements, such as the North Atlantic Treaty Organization ('NATO'), which ties certain regions and States to the US.³⁸ Chalmers incorporates a similar perspective, describing the 'Western system', embodied by security and integrative mechanisms, such as NATO, bilateral security agreements (such as ANZUS³⁹), the European Union and the Five Eyes intelligence-sharing arrangement, as a vital component of the order.⁴⁰

The second key feature of the liberal order, for Ikenberry, is the '**penetrated hegemony**' of the US. Ikenberry outlines that the 'liberal international order' or 'the American-centred Western order' (Ikenberry uses these terms interchangeably) differs from traditional hegemonic relations based on superordinate-subordinate relations. In contrast, the liberal order vests overall control with the US, while allowing Western states scope to contribute to "policymaking for the overall system". In this way, the order is an "empire by invitation."⁴¹ The US, as hegemon, is considered the "first citizen" of this order "providing hegemonic leadership—anchoring the alliances, stabilising the world economy, fostering cooperation and championing 'free world' values."⁴²

Similarly, Ho conceives of the 'liberal order' as one in which liberal, democratic States, especially the US, occupy positions of privilege. Non-liberal democracies like Vietnam

³⁵ Refer to **Table 2**.

³⁶ G.J Ikenberry, *A World Safe for Democracy: Liberal Internationalism and the Crises of Global Order* (New Haven, CT: Yale University Press, 2020), xii-xiii.

³⁷ G. John Ikenberry and Daniel Deudney, 'The Nature and Sources of Liberal International Order', *Review of International Studies* 25, no. 2 (April 1999): 176.

³⁸ Ikenberry and Deudney, 'The Nature and Sources of Liberal International Order', page 177.

³⁹ 'ANZUS' refers to the 'Australia, New Zealand and United States Security Treaty', which was agreed in 1951.

⁴⁰ Chalmers, Malcolm, 'Which Rules?', 4.

⁴¹ Ikenberry and Deudney, 'The Nature and Sources of Liberal International Order', page 185

⁴² G. John Ikenberry, 'The End of Liberal International Order?', *International Affairs* 94, page 7, no. 1 (1 January 2018): 7–23, <https://doi.org/10.1093/ia/iix241>.

may work within the liberal system, but only if they accept US primacy. Ho argues that during the Cold War, the liberal international order (comprising the US and its liberal democratic allies) operated in opposition to a communist-led order championed by the Soviet Union ('USSR') and China.⁴³ Within this paradigm, the USSR's collapse and the Cold War's culmination in 1991 represented the victory of the liberal international order over a communist order,⁴⁴ a line of reasoning that shares parallels with Fukuyama's 'end of history' thesis regarding the triumph of Western liberalism.⁴⁵

Sloss also views a hegemon as essential to the 'liberal international order', noting that its rules are "difficult to enforce without a dominant hegemon ... willing and able to exert its power to maintain a rules-based order."⁴⁶ Participants at a Chatham House conference in 2015 on 'challenges to the international rules-based order' adopted an equivalent position, agreeing that the rules-based international order was both embodied by Western liberal values and "enforced by the most powerful nations."⁴⁷

Western primacy or predominance also emerges as another core feature of the liberal order in other Australian and US narratives. Bisley has observed a growing sense in Canberra that diminished US and Western "primacy" has reduced the ability to enforce 'Western rules'.⁴⁸ Porter argued that the 'liberal democratic order' was naturally Western-led and that it was inherently resilient as "capitalist democracies" retained the "majority of global power". In contrast, rising powers would "never align into a cohesive, counter-hegemonic bloc."⁴⁹

Ikenberry suggested that the third key component of liberal order is '**civic identity**'. This covers norms and principles such as "political democracy, constitutional government, individual rights [and] private property-based economic systems."⁵⁰ Mazzar, in a US Government-sponsored study seeking to define the 'rule-based order',⁵¹ noted that the liberal elements of the order, such as democracy, are so firmly ingrained that "reducing the emphasis" on these elements could "unravel" the order itself. In addition, the "liberal character" of the order "implies ... a positive duty to defend other members of the liberal community" and to free people from "intolerable oppression" even if, it is implied, that might be in breach of principles of international law, such as state sovereignty. The US invasion of Iraq in 2003 and efforts to impose a

⁴³ Benjamin Tze Ern Ho, 'A Finely Fractured Consensus: American Motivations for Rules-Based Order', *The Washington Quarterly* 45, no. 4 (2 October 2022): 61, <https://doi.org/10.1080/0163660X.2022.2148506>.

⁴⁴ Ho, 'A Finely Fractured Consensus', page 61.

⁴⁵ Fukuyama, Francis. "The End of History?" *The National Interest*, no. 16 (1989): 3–18. <http://www.jstor.org/stable/24027184>.

⁴⁶ Sloss, David, *Is the International Legal Order Unraveling?* (Oxford University Press, 2022), 19.

⁴⁷ "Challenges to the Rules-based international order", *Chatham House*, accessed 3 September 2023, <https://www.chathamhouse.org/sites/default/files/London%20Conference%202015%20-%20Background%20Papers.pdf>.

⁴⁸ Australian Institute of International Affairs, '*Australia and the Rules-Based International Order*', page 308.

⁴⁹ Patrick Porter, 'Sorry, Folks. There Is No Rules-Based World Order.' *The National Interest*, 28 August 2016, 5, <https://nationalinterest.org/blog/the-skeptics/sorry-folks-there-no-rules-based-world-order-17497>.

⁵⁰ Ikenberry and Deudney, 'The Nature and Sources of Liberal International Order', page 192.

⁵¹ 'Understanding the Current International Order', RAND Corporation, page xiii.

democratic system, under this paradigm, were “not an insult to the liberal order” but rather the highest point in its development.⁵² Mazzar envisaged conflict and tension within this system, conceding that it was predictable that “illiberal states”, such as Russia and China, would take a stand against critical elements of the rules-based order, including liberal values, US alliances and hegemony.⁵³

‘Liberal international order’ and the ‘rules-based international order’ – separate or synonymous?

In government policy and academic literature in Australia and the US, the ‘liberal international order’ and the ‘rules-based international order’ are treated as broadly synonymous and interchangeable. Bilahari Kausikan, former head of Singapore’s foreign ministry, claims that for the vast majority of States, including those in the Indo-Pacific, the rules-based international order *means* the liberal international order, an order ‘led’ by the US.⁵⁴ Strating observes that the West tends to use the ‘rules-based international order’ as a “rhetorical proxy” for the maintenance of US hegemony under a ‘liberal international order’.⁵⁵ For Price, when Australian officials refer to the ‘rules-based order’, this is code for the “post-1945 Liberal International Order”, as described by Ikenberry.⁵⁶

Reinforcing this point, Bisley and Schreer assert that the Australian Government’s contemporary preference for the use of the ‘rules-based international order’ is not because it views this term as divergent from the ‘liberal international order’. On the contrary, this is because the ‘rules-based order’ formulation has greater appeal to the non-democratic, non-liberal States of the Indo-Pacific, such as Singapore and Vietnam, with which Australia seeks to enhance security and foreign policy cooperation.⁵⁷

In a recent study of US official and academic thinking concerning the content and scope of the ‘rules-based international order’, Ho found that most camps saw this order in liberal terms – that is, as a vehicle for the promotion of liberal economic and governance values and US hegemony. Ho concluded that thinking fell into three ‘schools’: idealists, internationalists, and instrumentalists.⁵⁸ Idealists viewed the order as being animated by the promotion of liberal values, such as democracy and human rights. The US was the *sine qua non* for the order and its exemplar. Instrumentalists viewed the order principally as focused on preserving Washington’s power and hegemony. Alternatively, internationalists considered the order was primarily about maximising international cooperation and stability. Ho found no overwhelming partisan alignment to any of these schools.

In terms of official narratives, the US, a regular invoker of ‘rules-based order’

⁵² ‘Understanding the Current International Order’, RAND Corporation, page 33.

⁵³ ‘Understanding the Current International Order’, RAND Corporation, page 33.

⁵⁴ Bilahari Kausikan, ‘Perspectives’, 17 August 2021.

⁵⁵ Dr. Bec Strating, ‘Perspectives: Preserving the “Rules-Based Order”’, Asialink, 17 August 2021, 1, <https://asialink.unimelb.edu.au/insights/perspectives-preserving-the-rules-based-order>.

⁵⁶ Price, Megan, ‘Norm Erosion and Australia’s Challenge to the Rules-Based Order’, *Australian Journal of International Affairs* 75, no. 2 (n.d.): 163, <https://doi.org/10.1080/10357718.2021.1875983>.

⁵⁷ Bisley, Nick and Schreer, Benjamin, ‘Australia and the Rules-Based Order in Asia’, *Asian Survey* 58, no. 2 (April 2018): 312.

⁵⁸ Ern Ho, ‘A Finely Fractured Consensus’.

terminology,⁵⁹ often refers to international order in a way that appears to confirm that it views its hegemony and primacy in rule-setting as a central principle. For example, in the 2016 State of the Union address, President Obama stated that “China does not set the rules [in the Indo-Pacific], we do.”⁶⁰ Similarly, the US’ 2018 Strategic Framework for the Indo-Pacific describes the maintenance of US “strategic primacy” as a key US regional objective.⁶¹ In an essay in *Foreign Affairs* in 2020, then-candidate Biden emphasised the role of US leadership in “forging the agreements, and animating the institutions” that bring global order.⁶²

In the Australian context, official documents and statements confirm, or at least create the perception, that Australia views the rules-based and liberal order concepts as synonymous, thus effectively incorporating liberal order norms into Australia’s interpretation of the order. For example, in the 2017 Fullerton lecture in Singapore, Foreign Minister Bishop used the terms ‘liberal international order’ and ‘rules-based international order’ interchangeably. Further, Bishop noted that US democracy and political values “reflect the liberal rules-based order ... we seek to preserve and defend.”⁶³ Australia’s 2017 Foreign Policy White Paper confirmed that Australia strongly supports “US global leadership” in the international system. Without US support, the Paper suggests, both the “effectiveness and the liberal character of the rules-based order will decline.”⁶⁴ Australia’s former Prime Minister Scott Morrison used both terms interchangeably, and, on occasion, combined the two, referring to the “liberal, rules-based order”.⁶⁵

Australia’s 2013 National Security Strategy described the US as the “critical underpinning” to the rules-based order.⁶⁶ In 2014, Prime Minister Abbot went further, describing Australia’s conception of the US as a guarantor whose role was to “keep the

⁵⁹ Beinart, ‘The Vacuous Phrase at the Core of Biden’s Foreign Policy’.

⁶⁰ ‘Remarks of President Barack Obama – State of the Union Address as Delivered’, White House, 13 January 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/01/12/remarks-president-barack-obama-%E2%80%93-prepared-delivery-state-union-address>.

⁶¹ ‘Statement from National Security Advisor Robert C. O’Brien’, The White House, accessed 21 September 2023, <https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-011221/>.

⁶² Joseph R. Biden and Jr, ‘Why America Must Lead Again’, *Foreign Affairs*, 23 January 2020, <https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again>.

⁶³ ‘Change and Uncertainty in the Indo-Pacific: Strategic Challenges and Opportunities: Speech to the 28th IISS Fullerton Lecture, Singapore’, accessed 21 September 2023, <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/5160178%22>.

⁶⁴ ‘2017 Foreign Policy White Paper’ Australian Government, Department of Foreign Affairs and Trade, last modified 24 April 2020, page 7, www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/index.html.

⁶⁵ ‘Rules-Based Order: What’s in a Name?’, Lowy Institute, accessed 29 September 2023, <https://www.lowyinstitute.org/the-interpreter/rules-based-order-what-s-name>.

⁶⁶ ‘Strong and Secure – A Strategy for Australia’s National Security’, Parliament House of Australia, accessed 25 June 2023, page 22, <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22library/lcatalog/00500351%22>.

peace and enforce the rules".⁶⁷ For Foreign Minister Bishop, the liberal elements of what was an order in which the West enjoyed primacy were critical. While non-democracies, like China, could "thrive" in the present order, "an essential pillar of our preferred order is a democratic community." Emphasising this point, Bishop suggested that only liberal democracies could be true 'citizens' of the rules-based international order and outlined that "domestic democratic habits" were essential to the resolving of disagreements according to international law and to allow States to achieve their full economic potential, citing the 'middle-income trap' thesis.⁶⁸

The perception that liberal democratic States, such as Australia, view the 'rules-based' and 'liberal' order as identical was reinforced by a 2017 Strategy Paper released by the 'D-10' forum of democracies.⁶⁹ This paper used the terms 'international rules-based order', 'rules-based democratic order' and 'liberal international order' interchangeably, describing this order as based on democratic governance and the protection of individual rights.⁷⁰

From the perspective of Australia's foreign policy, fundamental challenges for Australia's use of 'rules-based order' language as a tool to catalyse regional action arise from the perception that Australia views the 'rules-based' and 'liberal' international orders as synonymous. If a 'rules-based order' requires the promotion of liberal, democratic values as a guiding philosophy, or if 'true membership' requires that a State be a liberal democracy, this automatically excludes many States in the Indo-Pacific that are not liberal democracies or even basic democracies. In a 'liberal democracy index' prepared by *Our World in Data*, aside from Australia, New Zealand, and the US, only South Korea, Japan, Taiwan, and Vanuatu score above fifty per cent in the Indo-Pacific.⁷¹ Singapore has expressly rejected liberal democracy,⁷² while China and Vietnam are one-party, authoritarian states. Thailand is emerging from (another) period of military dictatorship. Indonesia, Bangladesh, and India are rated as only 'partly free' by *Freedom House* and Cambodia, Myanmar, and Laos are considered 'not free'.⁷³ As Milner and Smith observe, ASEAN members, with their divergent governance practices, do not wish to discriminate with respect to political systems and are wary of language that suggests order must be brought by a partnership of democracies.⁷⁴

⁶⁷ 'Rules-Based Order: What's in a Name?' Lowy Institute.

⁶⁸ 'Change and Uncertainty in the Indo-Pacific: Strategic Challenges and Opportunities: Speech to the 28th IISS Fullerton Lecture, Singapore'.

⁶⁹ The "Democracies 10" or "D-10" comprise Australia, Canada, France, Germany, Italy, Japan, South Korea, the UK, the US and the EU.
www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/global-strategy-initiative/democratic-order-initiative/d-10-strategy-forum/

⁷⁰ Romain Warnault, 'Strategy of "Constraint"', *Atlantic Council* (blog), 16 March 2017, 4, <https://www.atlanticcouncil.org/in-depth-research-reports/report/strategy-of-constraint/>.

⁷¹ 'Liberal Democracy Index', *Our World in Data*, accessed 27 October 2023, <https://ourworldindata.org/grapher/liberal-democracy-index>.

⁷² Dylan M H Loh, 'Singapore's Conception of the Liberal International Order as a Small State', *International Affairs* 99, no. 4 (3 July 2023): 1499–1518, <https://doi.org/10.1093/ia/iiaad161>.

⁷³ 'Countries and Territories – Freedom in the World Dataset', *Freedom House*, accessed 6 October 2023, <https://freedomhouse.org/countries/freedom-world/scores>.

⁷⁴ Tony Milner and Ric Smith, 'Rules-Based Order: What Does the Region Think?', *Asialink*, 17 August 2021, 3, <https://asialink.unimelb.edu.au/insights/rules-based-order-what-does-the-region-think>.

Further, if the 'rules-based order', as Mazarr has suggested, justifies the use of force against countries in the service of efforts to bring liberal democracy, such as in Iraq in 2003, this approach is antithetical to the perspectives of the vast majority of States in the Indo-Pacific region. The notion that the 'rules-based order' justifies efforts to spread liberal democracy, not just via proselytisation but also, where necessary, by force, has parallels with the 'civilising mission', an intellectual trend that took root in the nineteenth century and purported to justify European colonialism on the basis that "backward lands" would be 'civilised' in return for the exploitation of their economies.⁷⁵ To support this conclusion, we only need to look at the reaction of States in the Indo-Pacific region to the US' 2003 invasion of Iraq and the fact that Australia and the US were the only States in the Indo-Pacific that participated in the invasion. India opposed the US invasion of Iraq, maintaining that UN Security Council authorisation was required and that any move to change the regime in Baghdad "must come from within" and "not be imposed from outside."⁷⁶ China, Indonesia, Malaysia (speaking for the Non-Aligned Movement), New Zealand, Vietnam, and Bangladesh took similar positions.⁷⁷



The flags of the countries in the Association of Southeast Asian nations (ASEAN) are displayed.
Image: Shutterstock

Finally, the centrality of US hegemony to the 'liberal' and 'rules-based' orders establishes, at least in the Indo-Pacific, a binary between the US and China and could reasonably imply that support for this order requires support for US regional hegemony. This runs contrary to the position of many States in the region. As Singapore's Kausikan writes, the 'political-security' aspects of the 'rules-based order' effectively incorporate the norm of US primacy and, subsequently, the "hard containment" of China, something that ASEAN members do not support.⁷⁸ Further, as Singapore's Prime Minister underlined in 2022, countries in Southeast Asia – most of which are more economically reliant on trade with China than the US – do not wish to be forced to 'choose' between the US and China and believe that security is enhanced where these superpowers enjoy

⁷⁵ Kiernan, V.G., *The Lords of Human Kind: European Attitudes to Other Cultures in the Imperial Age* (Serif, 1995), 24.

⁷⁶ 'Statement on the Current Situation Related to Iraq', Ministry of External Affairs, India, accessed 11 October 2023, https://www.mea.gov.in/press-releases.htm?dtl/9209/Statement_on_the_current_situation_related_to_Iraq.

⁷⁷ See country statements recorded at: 'Security Council holds first debate on Iraq since start of military action: speakers call for halt to aggression, immediate withdrawal', UN Press, accessed 21 July 2023, <https://press.un.org/en/2003/sc7705.doc.htm>.

⁷⁸ Bilahari Kausikan, 'Perspectives', 17 August 2021, page 2.

“overlapping circles of friends.”⁷⁹

Anwar, an adviser to Indonesia's Vice President, underscores that the emphasis on 'rules-based international order' terminology by the US, Australia and others is perceived by China as “exclusive rather than inclusive” and a component of a “strategy to contain China”. ASEAN countries are at the coalface of US-China strategic competition and, Anwar highlights, have “no desire” to be driven to “take side[s]” and be divided by the superpowers, as occurred during the Cold War.⁸⁰

In addition, if US hegemony or primacy in the Indo-Pacific constitutes a part of the fabric of the rules-based order, the perception could be that support for this order equates to a willingness to back the US – militarily if necessary – should its primacy be challenged in the Indo-Pacific, or elsewhere. The resulting implications dampen the appeal of 'rules-based order' terminology. As Anwar and others outline, ASEAN states have been clear that they do not wish to 'choose', and the idea of backing the US militarily in a conflict with China, not least over 'primacy', appears inconceivable for many regional States.

⁷⁹ Chris Barrett, 'We Don't Want to Pick Sides: The View from South-East Asia as China Woos Pacific', *The Sydney Morning Herald*, 26 May 2022, www.smh.com.au/world/asia/we-don-t-want-to-pick-sides-the-view-from-south-east-asia-as-china-woos-pacific-20220526-p5aosj.html.

⁸⁰ Dewi Fortuna Anwar, 'A Rules-Based Order in the Indo-Pacific: A view from Jakarta', *Journal of Indo-Pacific Affairs*, 2020, 42-47, page 46.



Image: StockCake. Available at https://stockcake.com/i/vintage-adventure-atlas_2117268_1287771

Chapter 3: When was the ‘international rules-based order’ created, and what does it comprise?

This Chapter will demonstrate that the official and academic narrative regarding the creation of the rules-based order is incoherent; there is no consensus on what the rules and institutions that make up the ‘rules-based order’ are, or even whether the order exists or is merely aspirational. Individual accounts of the rules and institutions that comprise the order are also, in some instances, incoherent or internally contradictory. As a result, it is challenging for Australia to convince other States, in the region and beyond, to value the order and to act in its defence.

Emergence of the rules and institutions of the order

In temporal terms, the bulk of the official and academic literature suggests that the order was established in the aftermath of the Second World War and comprises, at its core, the UN and the Bretton Woods Institutions (i.e., the International Monetary Fund (‘IMF’) and the World Bank).⁸¹ However, some trace the origins of an international rules-based order to the Kellogg-Briand Pact of 1928⁸², a treaty that sought to outlaw aggressive war and served as a forerunner to Article 2(4) of the UN Charter, or even to the 1648 Treaty of Westphalia.⁸³

Australia’s 2016 Defence White Paper described the rules-based order as underpinned by “international governance ... developed since the end of the Second World War”, including the UN and international treaties.⁸⁴ Similarly, Australia’s 2017 Foreign Policy White Paper emphasised that the creation of “international institutions and rules to ... support economic growth, global security and human development” was one of the key features of the post-Second World War era.⁸⁵

However, the rules-based order is considered aspirational in some official and academic quarters. This perspective is informed by liberal conceptions of the order, suggesting that there can be no genuinely *global* ‘rules-based order’ until all, or perhaps the majority, of States are liberal democracies or accept liberal democracy’s hegemony. For example, Sloss argues that in the post-Cold War period, the US “attempted to create a rules-based order that was both liberal and global”. This order was typified by “military adventurism”, leveraging US military power to spread human rights and democracy internationally.⁸⁶ Mazarr submits that while a rules-based order was established in the

⁸¹ See, for example, Department of Defence, “Defence White Paper”, page 21 and ‘2017 Foreign Policy White Paper’ Australian Government, Department of Foreign Affairs and Trade, last modified 24 April 2020, page 79, www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/index.html and other sources explored in this Chapter.

⁸² ‘The Liberal Order of the Past 70 Years Is under Threat’, *The Economist*, accessed 29 September 2023, <https://www.economist.com/books-and-arts/2017/09/21/the-liberal-order-of-the-past-70-years-is-under-threat?giftId=9ee2a2a5-2e4c-4024-8a72-2c031f304e83>

⁸³ ‘Australia and the Rules-Based International Order’, Australian Institute of International Affairs, Tyler, Gyngell and Wakefield, page 17, accessed 27 July 2023, <https://www.internationalaffairs.org.au/publication/australia-and-the-rules-based-international-order/>.

⁸⁴ Department of Defence, “Defence White Paper”, page 21.

⁸⁵ ‘2017 Foreign Policy White Paper’ Australian Government, Department of Foreign Affairs and Trade, last modified 24 April 2020, page 79, www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/index.html.

⁸⁶ Sloss, David, *Is the International Legal Order Unravelling?*, page 22.

aftermath of the Second World War, membership was limited to the democratic West. Once the Soviet Union collapsed, the opportunity to participate in the order was extended more broadly, allowing States that accepted the order's core norms – US hegemony, democracy, and liberal values – to join.⁸⁷

Statements at the official level appear to confirm that similar perspectives are held by the US and Australian governments. In 2011 at APEC, then-Secretary of State, Hillary Clinton, noted that a “rules-based order” needed to be created to promote and protect freedom, openness and fairness.⁸⁸ In 2019, Australia's Defence Minister Reynolds articulated the need to establish a rules-based order that is “fit-for-purpose in the twenty-first century” and which can deliver “regional and global peace and also prosperity” as a “collective challenge”.⁸⁹ While Reynolds' statement is seemingly at odds with Government White Papers, at best it reduces the perceived coherence of Australia's conception of the ‘rules-based order’, negatively affecting the strength of Australia's case when it seeks to rally other States to defend the order. Further, there is a risk that Reynold's statement could be perceived as reinforcing liberal elements in Australia's conception of the order's operation, such as a privileged role for liberal democracies. As Chapter 2 has demonstrated, many States in the Indo-Pacific are not liberal democracies, rendering it less likely that Australia could convince these States to value and defend an order that Australia suggests they are not part – or are second-class citizens – of.

Content of the order

Official and academic efforts to capture the rules-based order's content, limits and core features diverge significantly, while individual conceptions often lack internal coherence. For instance, Hall and Heazle claim that the post-war rules-based order is, at its core, about global economic rules, maritime rules, and human rights standards. The principle of the ‘freedom of [maritime] navigation’ is portrayed as a key element of the order, though Hall and Heazle's work does not reconcile the fact that this international norm is enshrined in a treaty – the United Nations Convention on the Law of the Sea (‘UNCLOS’) – which the order's most powerful member, the US, is not a party to.⁹⁰ UNCLOS' deep sea-bed mining regime, popular in the developing world, is viewed by the US as inimical to its liberal, free market interests.⁹¹

Patrick maintains instead that the post-war order's guiding principles are openness, economic liberalism and de-colonisation and that fundamental norms of the order include self-determination, freedom of navigation, the use of force in self-defence, non-proliferation, human rights, and climate change.⁹² The UN is widely credited as playing

⁸⁷ ‘Understanding the Current International Order’, RAND Corporation, Michael J. Mazarr et al, last modified 19 October 2016, 32, www.rand.org/pubs/research_reports/RR1598.html.

⁸⁸ ‘America's Pacific Century’, remarks delivered at APEC 2011, U.S. Department of State, accessed 16 June 2023, [//2009-2017.state.gov/secretary/20092013clinton/rm/2011/11/176999.htm](https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/11/176999.htm).

⁸⁹ ‘Keynote Address, Hudson Institute, Washington DC’ *Department of Defence, Australia*, 2 November 2019, <https://www.minister.defence.gov.au/speeches/2019-11-02/keynote-address-hudson-institute-washington-dc>.

⁹⁰ ‘United Nations Treaty Collection’, accessed 27 October 2023, https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_en.

⁹¹ ‘Statement on United States Actions Concerning the Conference on the Law of the Sea’, Ronald Reagan Presidential Library, accessed 19 September 2023, www.reaganlibrary.gov/archives/speech/statement-united-states-actions-concerning-conference-law-sea

⁹² Stewart Patrick, ‘World Order: What, Exactly, are the Rules?’, *The Washington Quarterly*,

a pivotal role in catalysing and supporting the de-colonisation/self-determination process. The 1960 *Declaration on the Granting of Independence to Colonial Countries and Peoples* ('the Declaration') was the decision that initiated the UN's involvement in the de-colonisation process. Only nine States in the UN General Assembly did not support this Declaration, including Australia, the US, and the UK.⁹³ The Declaration itself was put forward by the Soviet Union. The Soviet leadership of this initiative and the lack of US support make it challenging to reconcile Patrick's conclusion that the order is a "post-1945 Western Order" that incorporates US "hegemony" with his separate finding that "self-determination" is one of the order's guiding principles.⁹⁴

While Patrick claims that non-proliferation norms are 'fundamental' to the post-war order, it is unclear how this can be reconciled with the fact that the most critical non-proliferation norms are contained in treaties that did not become binding for some decades after the Second World War. For instance, the Nuclear Non-Proliferation Treaty entered into force in 1970⁹⁵, whereas the Chemical Weapons Convention, prohibiting the possession of chemical weapons, entered into force only in 1997.⁹⁶

As explored in Chapter Two, official, and academic literature in the West often blurs or merges references to a rules-based international order with references to what Ikenberry and others have characterised as the liberal international order. Many of the narratives explored in this paper suggest that the 'rules-based order' is a Western order created in competition with a Soviet order. A widely cited 2016 RAND study, commissioned by the US Government, describes the order, at a structural level, as a post-war liberal order, established by the US, which includes "international economic institutions, bilateral" and "regional security organizations" (meaning US alliance structures) and "liberal political norms".⁹⁷ Citing, Ikenberry, Patrick and others, this study suggests that this rules-based order was "not global at first"; instead, it was incubated "within the global democratic community in competition with the Soviet bloc". Once the Soviet Union collapsed, the order was "extended globally", allowing States to participate, on the condition of adherence to the order's liberal norms and values. Ho also draws a similar distinction between a Western 'rules-based order' and a 'Soviet order', though the structures and rules of these orders and whether, or how, they overlap are given limited attention.⁹⁸ According to Mazarr, the order's core elements include "US power and sponsorship" and "a set of legitimate global institutions", such as the UN and the World Trade Organization ('WTO'), and "international legal conventions", such as arms control regimes.⁹⁹

These norms and institutions were created to advance "core principles", including "economic stability", "nonaggression", and "the advance of liberal values".¹⁰⁰ The rules-based order was built around "two architectures", reflecting key ideological points of consensus. The first is the liberal trade and investment regime – encompassing the

39:1, 2016, 7-27, page 11, DOI: 10.1080/0163660X.2016.1170477

⁹³ 'Declaration on the Granting of Independence to Colonial Countries and Peoples', United Nations Audiovisual Library, accessed 25 September 2023, <https://legal.un.org/avl/ha/dicc/dicc.html>.

⁹⁴ Stewart Patrick, World Order: What, Exactly, are the Rules?, *The Washington Quarterly*, 2016, 39:1, 7-27, page 12, DOI: 10.1080/0163660X.2016.1170477

⁹⁵ 'Treaty on the Non-Proliferation of Nuclear Weapons (NPT)', UN Office of Disarmament Affairs, accessed 3 October 2023, <https://disarmament.unoda.org/wmd/nuclear/npt/>.

⁹⁶ 'History', Organisation for the Prohibition of Chemical Weapons, accessed 3 October 2023, <https://www.opcw.org/about-us/history>.

⁹⁷ Mazarr et al., 'Understanding the Current International Order', 3.

⁹⁸ Ho, 'A Finely Fractured Consensus', page 61.

⁹⁹ Mazarr et al., 'Understanding the Current International Order', 12.

¹⁰⁰ Mazarr et al., 'Understanding the Current International Order', 13.

Bretton Woods Institutions and the General Agreement on Tariffs and Trade (later WTO). This regime was developed by a “core set of democratic trading states” that were so large that prosperity for other states required trade with them, and thus participation in the liberal order.

The second is the security architecture, designed to “obstruct large-scale aggression [and] also to shape the use of force.” In addition, the order “came to embrace goals of democratization and the protection of human rights”, such that these are “embedded” in the “global vision” for the order.¹⁰¹ From the perspective of the RAND study, it is unclear how the concept of a Western rules-based order competing with a Soviet order can be reconciled with the idea of the UN system and key global conventions, such as those on arms control, sitting within the ‘Western rules-based system’. After all, both the US and the USSR played an integral role in drafting the UN Charter. Indeed, it was the USSR that insisted on the inclusion of the veto power for permanent members of the UN Security Council, which included the USSR, as the price of its agreement to the Charter.¹⁰² It is also unclear precisely whether membership of this order, which includes, according to the RAND study and other authors, the UN, requires that a State be a liberal democracy. After all, this would not be consistent with the fact that many States that have been members of the UN since its inception,¹⁰³ including two-fifths of the permanent membership of the UN Security Council, are non-democracies, let alone liberal democracies.¹⁰⁴

Chalmers, adding further to the incoherence of the narrative surrounding the content of the order, claims that instead of thinking about a single ‘rules-based order’, it is necessary to conceive of the order as consisting of multiple orders with varying memberships, organised not geographically but thematically. These thematic orders include the ‘Universal Security System’, the ‘Western System’, the ‘Universal Economic System’, and ‘Major Power Relations’.¹⁰⁵ The former is governed by the principles of “self-determination and non-aggression”, under the UN system, and norms related to the use of nuclear and other weapons of mass destruction. The Western System enjoys the exclusive membership of “developed market democracies” in North America, Europe and the Asia-Pacific through security, integrative and cooperative mechanisms, such as the EU, NATO, bilateral security agreements, the G7, the OECD and the Five Eyes intelligence sharing arrangements. The Universal Economic System captures the international trade and investment architecture established by the IMF, the World Bank, and the WTO. The Major Power System includes the bloc structure and the division of Europe into mutually agreed spheres of influence and bilateral arms control agreements between the superpowers, such as the START treaty.¹⁰⁶

In terms of the content of the ‘rules-based order’, Australia’s official documents and statements tend towards the general over the specific. The 2016 Defence White Paper described the order as encompassing the UN system, a “shared commitment” to abide

¹⁰¹ Mazarr et al., ‘Understanding the Current International Order’, 15.

¹⁰² David L. Bosco, *Five to Rule Them All*, (Oxford University Press, 2009).

¹⁰³ Founding members of the United Nations included: Russia, China, Poland, Belarus, Venezuela, Iraq, Ethiopia, and South Africa. These States were not recognised as democracies at the point the UN was founded.

<https://research.un.org/en/unmembers/founders#:~:text=Founding%20Member%20States,51%20Founding%20Members%20in%201945>.

¹⁰⁴ The UN Security Council has five permanent members. This includes Russia and China, which are widely recognised as non-democratic States.

¹⁰⁵ Chalmers, Malcolm, ‘Which Rules?’, 4.

¹⁰⁶ ‘Strategic Arms Reduction Treaty’; Chalmers, Malcolm, ‘Which Rules?’, 4.

by international law and regional security architectures.¹⁰⁷ Prime Minister Morrison also reinforced the UN's centrality, describing it in 2019 as the "prime custodian" of the order, adding that the "UN and its norms" were key to a cooperative rules-based approach to global challenges. In a 2018 speech by Australia's Foreign Minister Bishop and in Australia's 2016 Defence White Paper, the UN architecture and "regional security architectures" – including bilateral mutual defence agreements, such as ANZUS, as well as ASEAN and other regional fora, such as the European Union – were described as core components of the 'rules-based order'.¹⁰⁸

As this analysis reveals, academic and official views diverge significantly with respect to the content and contours of the 'rules-based order'. As was explored in Chapter Two, many accounts emphasise liberal conceptions of the order, such as US hegemony and the promotion of liberal values, though they ignore the agency of non-Western actors in shaping key norms that regulate interaction between States, the temporal period in which norms were generated and the record of some Western States in terms of submitting themselves to treaties which many States consider contain norms critical to global order. Australia's narrative regarding the order is equally inconsistent. In one instance, the order is a post-war creation; in another, it is yet to be realised. In one case, the UN is at the very core of the order, then Australia speaks of the US setting and enforcing the rules and, in a move that suggests a profound lack of confidence in the UN, conducts an 'audit' of its multilateral institutions. Accordingly, this inability to paint a straightforward narrative leaves the neutral observer to conclude that 'liberal' norms are genuinely at the core of the rules-based order as these are the only elements clearly and consistently referenced across competing narratives. Beyond these liberal norms, it is hard to paint a clear and consistent picture of the order's norms, making it challenging for Australia to rally international efforts to maintain and defend the order.

¹⁰⁷ Department of Defence, "Defence White Paper".

¹⁰⁸ Department of Defence, "Defence White Paper", page 45; and "La Trobe University Lecture and Conversation", Department of Foreign Affairs and Trade, Australia, accessed on 5 October 2023, <https://www.foreignminister.gov.au/minister/julie-bishop/speech/la-trobe-university-lecture-and-conversation>.

This page is intentionally blank

Chapter 4: The rules-based international order is ‘under strain’

The suggestion that the rules-based order is in crisis, “disintegrating”, or even in its “death throes”,¹⁰⁹ is another central theme in academic and official discourse, including in Australia. Indeed, as Chapter One demonstrated, some of the earliest references at the political level in Australia to the ‘rules-based order’ were to characterise it as in jeopardy, in that instance because of Australia’s conduct.¹¹⁰ An exploration of the narratives related to the ‘strain’ on the order assists in illuminating how those who utilise this description view the norms and operation of the ‘rules-based order’. This Chapter will demonstrate that the narratives regarding the ‘stresses’ on the order, which are predominantly found among Western sources, are focused largely on the geopolitical challenges generated by Russia’s and China’s more assertive international posture. These narratives further reinforce that ‘liberal’ norms – such as US hegemony, the privileged status of the West as rule maker and enforcer, and the promotion of liberal democracy globally, including by force – sit at the very core of the mainstream conception of the ‘rules-based order’. As a result, the rallying and coordinating power of ‘rules-based order’ terminology is diminished.

A fraying order?

The narrative that the ‘rules-based international order’ is currently facing unprecedented pressure and challenge, particularly from China and Russia, is dominant in both Australian academic and official sources. For Tyler, the concept that some States are “uniquely or fundamentally challenging [it]” is a central theme of the order itself.¹¹¹ Maude, a former senior official in Australia’s foreign ministry, noted that we must “recognise the significance of the strains on the rules-based order” and that it is changing, with its liberal character weakening.¹¹² Australia’s 2017 Foreign Policy White Paper paints a similarly gloomy picture, emphasising that the order is “under significant challenge” with “forces of change ... buffeting this system”, citing “geo-political competition”, power shifts between states and globalisation as the primary centrifugal forces.¹¹³ Australia’s 2016 Defence White Paper described an order that was showing “signs of fragility” and was being contested by “competition between countries and major powers trying to promote their interests outside of the established rules [created over 70 years ago]”.¹¹⁴

¹⁰⁹ ‘The Rules-Based International Order Is Ending. What Will Replace It?’, The Hill, accessed 14 June 2023, <https://thehill.com/opinion/national-security/3736389-the-rules-based-international-order-is-ending-what-will-replace-it/>.

¹¹⁰ Mazarr et al., ‘Understanding the Current International Order’, 2.

¹¹¹ ‘Australia and the Rules-Based International Order’, Australian Institute of International Affairs, Tyler, Gyngell and Wakefield, page 9, accessed 27 July 2023, <https://www.internationalaffairs.org.au/publication/australia-and-the-rules-based-international-order/>.

¹¹² ‘Australia and the Rules-Based International Order’, Australian Institute of International Affairs, Tyler, Gyngell and Wakefield, page 45, accessed 27 July 2023, <https://www.internationalaffairs.org.au/publication/australia-and-the-rules-based-international-order/>.

¹¹³ ‘2017 Foreign Policy White Paper’ Australian Government, Department of Foreign Affairs and Trade, last modified 24 April 2020, page 79, www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/index.html.

¹¹⁴ Department of Defence, “Defence White Paper”.

Similar perspectives can be found elsewhere. In reference to Russia's invasion of Ukraine, German Foreign Minister, Heiko Maas, observed that some States were engaging in "power politics", undermining the order based on rules in favour of an order based on strength.¹¹⁵ Similarly, for Paikin, Russia's invasion of Ukraine has left the rules-based order "in crisis" and has "destroyed the European security architecture".¹¹⁶

Why and how is it fraying?

While a consistent theme in official and academic narratives centres on the pressures and strains on this order, accounts of how and why it is fraying differ markedly. Often, the 'fraying' narrative is underpinned by liberal conceptions of the order, with challenges coming from non-liberal States or even purely because of the failure of the 'liberal agenda' to gain traction internationally. As a pointed example, Mead cites the failures of US 'democracy building' interventions in Libya, under Obama, and in Iraq, under George W. Bush, as examples of the failure of liberal internationalism at the very core of the rules-based order.¹¹⁷



Image: Depositphotos

Another dominant theme in the 'fragility' narrative focuses less on the notion that the order's integrity is at risk due to breaches of fundamental tenets of its international legal norms, such as Russia's breach of the prohibition on aggression enshrined in Article 2(4) of the UN Charter through its invasion of Ukraine. Instead, the sources of 'disorder' are threats to US hegemony and dominance that

arise because of rising powers rejecting the premise of US primacy. For example, Haass, former President of the US Council on Foreign Relations, stresses that the current "disorder" in the rules-based system is a result of States and other actors acting with greater autonomy and "paying less heed to US interests and preferences".¹¹⁸

Similarly, for Mazarr, one of the critical risks to the order is that rising States perceive that elements of it are "designed to constrain their power and perpetuate U.S. hegemony."¹¹⁹ Bisley concludes that there is a growing sense among decision-making elites in Canberra that the post-war rules-based order is in 'disarray' since "Western primacy and the ability to enforce Western rules [which make up the 'Western rules-based order'] are declining." The critical question, for Bisley, is whether the US is willing to "act as the principal guarantor" for these rules.

¹¹⁵ Malcolm Jorgensen, 'The German National Security Strategy and International Legal Order's Contested Political Framing', *EJIL: Talk!* (blog), 5 July 2023, page 23, <https://www.ejiltalk.org/international-legal-orders-contested-political-framing/>.

¹¹⁶ 'Canada's Dilemma: China and the "Rules-Based International Order"', *The Institute for Peace and Diplomacy - l'Institut Pour La Paix et La Diplomatie*, 14 June 2022, page 1, <https://peacediplomacy.org/2022/06/14/canadas-dilemma-china-and-the-rules-based-international-order/>.

¹¹⁷ Walter Russell Mead, 'The End of the Wilsonian Era: Why Liberal Internationalism Failed', *Foreign Affairs* 100, no. 1 (February 2021): 136.

¹¹⁸ Richard N. Haass, 'The Unraveling: How to Respond to a Disordered World', *Foreign Affairs* 93, no. 6 (2014): 70.

¹¹⁹ Mazarr et al., 'Understanding the Current International Order', 3.

For Bisley, 'rules-based order' terminology is a subtle code for the desire of the US to retain 'primacy' in East Asia, which has been the "fundamental ordering principle in East Asia". Usage of the rules-based order formulation – which Bisley observes is largely by US allies – is a means for Canberra to "signal Australia's growing security alignment with Washington and its other Asian partners". Calling out China for breaches of the rules-based order is merely a subtle way to criticise China's "strategic actions" while minimising the risk of damage to the bilateral relationship.¹²⁰

Bisley's narrative is that China poses a threat to this 'Western rules-based order' on the basis that it has rejected overtures and socialisation efforts from the West to become a liberal democratic state.¹²¹ Under this paradigm, China challenges this order by building its own regional institutions – such as the Shanghai Cooperation Organization and the Asian Infrastructure Investment Bank. In addition, however, China's challenge to the order can also be seen in its "comprehensive military build-up ... designed to negate US naval supremacy in the Western Pacific." Thus, from Bisley's perspective, or at least the perception the reader is left with, US military supremacy in East Asia itself is a crucial component or norm of the 'rules-based order'.¹²²

As a corollary, China's challenge to the order and its desire, as Bisley puts it, to 'rewrite' the order, at least in East Asia, is not framed as China's desire to rewrite extant rules of international law, but rather to build the military power necessary to displace the US as East Asia's hegemon. According to Bisley, Australia must champion a coalition against China's 'revisionism' to resist this. Necessarily, this will require the involvement of democratic and non-democratic States. Accordingly, it will be necessary for Canberra to steer clear of the use of 'liberal international order' language (favouring instead the 'rules-based order'), so it is appealing to non-democratic States in Asia.

The concept that liberal democracies occupy a position of privilege also appears consistently in the 'fraying' narrative. Ikenberry acknowledges the threats to the rules-based order but is more sanguine about its prospects for survival. The order, Ikenberry contends, is a "liberal leviathan", reinforcing the centrality and supremacy of liberal democracies. Ikenberry argues that capitalist democracies retain the bulk of global power, and their 'first-mover advantage' means they have created a global order that is "easy to join" but "hard to overturn".¹²³ In Ikenberry's view, it is unlikely that rising powers would coalesce into a coherent "counter-hegemonic" bloc, given their differences in interests, histories, and political systems. In this regard, it is clear to Ikenberry that the rules-based order is designed to benefit capitalist democracies and has facilitated a period of hegemony for these States. Mazarr shares this view, noting that liberal democracies "ha[ve] always constituted the core of the modern order."¹²⁴

Sloss touches on some similar themes. For Sloss, the rise of China, 'democratic decline' globally, and the weakening of the US' power and leadership are among the order's principal threats. For Sloss, the latter threat is acute because the US plays a critical role in both maintaining and enforcing the order's "rules affecting peace, prosperity, and

¹²⁰ Bisley, Nick and Schreer, Benjamin, 'Australia and the Rules-Based Order in Asia', *Asian Survey* 58, no. 2 (April 2018): 311.

¹²¹ Bisley, Nick and Schreer, Benjamin, 312.

¹²² Bisley, Nick and Schreer, Benjamin, 'Australia and the Rules-Based Order in Asia', *Asian Survey* 58, no. 2 (April 2018): 313.

¹²³ G. John Ikenberry, 'Reflections on After Victory', *The British Journal of Politics and International Relations* 21, no. 1 (2019): 16.

¹²⁴ Mazarr et al., 3.

human rights".¹²⁵

Like others, Sloss links the integrity of the rules-based order to the health of democracy internationally. Sloss suggests that wise politicians in the West may be able to "exploit widespread fear of China" to reinvigorate liberal democracy, both domestically and globally. If this fails, the resulting "erosion of liberal democracy" will undermine the protection of human rights, a fundamental pillar, Sloss claims, of the rules-based order.

¹²⁶ Sloss emphasises the idea that liberal values are both at the heart of the rules-based order, but also that liberal democracies enjoy a form of exceptional standing within the rules-based order, or even that parts of this order are not genuinely universal but apply only to, or privilege, liberal democracies.

The challenge this narrative creates is two-fold. First, it underscores the perception that the rules-based order is being used as a synonym for the liberal international order and that concepts such as the promotion of liberal democracy, US hegemony and a privileged role for liberal democracies sit at the core of this order. The narrative that the rise of powers that are not liberal democracies threaten the order is unlikely to increase the attractive pull of the rules-based order for many States in Australia's region, given the number of countries in the Indo-Pacific that are not democracies (see Chapter 2). Second, it promotes the idea that US hegemony or primacy in the Indo-Pacific forms a pillar of the rule-based order. As Chapter 2 canvassed in detail, many States in the Indo-Pacific have been clear that they do not wish to be forced to choose between China and the US and do not support the concept of any State occupying a position of hegemony in the region.

¹²⁵ Sloss, David, *Is the International Legal Order Unravelling?*, page 21.

¹²⁶ Sloss, David, *Is the International Legal Order Unravelling?*, page 34.

Chapter 5: What is the distinction between the ‘order’ and international law?

In April 2020, Russia's Foreign Minister, Sergey Lavrov, observed that there is a trend in the West to:

*“make fewer references to international law or even remove it from the international lexicon altogether. Instead of the well-established term “international law” they are attempting to use a new expression, ‘a rules-based order.’ ”*¹²⁷

International law comprises rules of a legally binding character that set out the “responsibilities of States in their conduct with each other, and their treatment of individuals within States boundaries.”¹²⁸ As such, international law – as a set of legally binding rules applicable to States – may be expected to have considerable prominence within an order that is ‘rules-based’. In practice, as this Chapter will demonstrate, official and academic narratives on the ‘rules-based order’ in Australia and the US de-emphasise international law and its centrality as part of this order. This Chapter will argue that this de-emphasis weakens the appeal of ‘rules-based order’ terminology as rhetorical attacks against Russia and China for breaches of the ‘rules-based order’ risk being perceived as overly geopolitically motivated, particularly considering the track record of adherence to international law of accusing States.

From the perspective of some conceptions of the ‘rules-based order’, the reason for the distinction between ‘international law’ and the order is that the latter captures the full breadth of international rules, including those of a legally binding character and those that might best be described as political commitments. Germany, for example, advocates this approach. It considers that the order includes international law and “non-binding norms, standards and procedures in various international fora and negotiating processes.” After all, a significant portion of the norms and rules that govern relations between States are non-legally binding. These include the 1948 Universal Declaration of Human Rights,¹²⁹ which was a hortatory resolution of the UN General Assembly,¹³⁰ the 1993 Rio Declaration on the Environment and Development,¹³¹ and the 1960 UN General Assembly resolution on the Declaration on the Granting of Independence to Colonial Countries and Peoples (Resolution 1514).¹³²

¹²⁷ ‘Excerpts from Russian Foreign Minister Sergey Lavrov’s Remarks at a Roundtable Discussion with the Participants of the Gorchakov Public Diplomacy Fund’, *Permanent Mission of the Russian Federation to the European Union*, last modified 22 April 2020, <https://russiaeu.ru/en/news/excerpts-russian-foreign-minister-sergey-lavrovs-remarks-roundtable-discussion-participants>, archived at <<https://perma.cc/799K-M629>>. See generally Sergei V Lavrov, ‘On Law, Rights and Rules’ (2021) 19(3) *Russia in Global Affairs* 228.

¹²⁸ ‘Uphold International Law’, United Nations, accessed 10 October 2023, <https://www.un.org/en/our-work/uphold-international-law>.

¹²⁹ ‘Universal Declaration of Human Rights’, United Nations, accessed 27 October 2023, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

¹³⁰ ‘What Is the Universal Declaration on Human Rights?’, Australian Human Rights Commission, 31 December 2007, <https://humanrights.gov.au/our-work/projects/what-universal-declaration-human-rights>.

¹³¹ ‘Declaration of the United Nations Conference on the Human Environment’, United Nations, accessed 27 October 2023, <https://legal.un.org/avl/ha/dunche/dunche.html>.

¹³² ‘Declaration on the Granting of Independence to Colonial Countries and Peoples’.

However, Australia's emphasis on other norms, such as US security alliances and the US' unique role in the order, makes it clear that Australia's position diverges from Germany's. Australia's 2016 Defence White Paper claimed that the 'rules-based order' entails a common commitment between States to act in line with "agreed rules which evolve over time". It lists 'international law' as but one example of 'agreed rules' in an open list that includes "regional security arrangements". This is a notable juxtaposition, given that the bulk of regional security arrangements, such as the agreements that underpin NATO, ANZUS and the Five Power Defence Arrangements, are enshrined in treaties, meaning that the rules of these security arrangements are international law.¹³³ This juxtaposition reinforces the impression that Australia's conception of a rules-based international order includes the security frameworks that such agreements generate or acknowledge, including the concept of US primacy in the Indo-Pacific.

Australia's 2017 Foreign Policy White Paper reinforces this perception. It characterises 'international law' and the 'rules-based order' as distinct frameworks, noting that Australia's response to cyber-attacks will be consistent with "our support for the rules-based international order and our obligations under international law." In a paragraph exploring the core principles of the rules-based order that support Australia's interests and values, the White Paper identified "international law", "the articulation of universal rights and freedoms", and "US leadership [and] network of [alliances]" as well as the US military presence in Asia and Europe.¹³⁴

There is, therefore, a risk of the perception that the de-emphasis on international law, in favour of an emphasis on the 'rules-based order', is because users of the 'rules-based order' terminology wish to import a range of concepts as norms of this order – such as the hegemony of the US and liberal democracies – which are not enshrined in international law.

In addition, the emphasis on breaches of the 'rules-based order', an undefined concept, over specific rules of international law, has given rise to the perception that it allows certain States, principally the US but also Australia, to attack States with which they are in geopolitical competition while avoiding criticism of their own record of adherence to international legal standards.¹³⁵

An overwhelming majority of States consider Russia's 2022 invasion of Ukraine to be a fundamental breach of one of the most critical post-war norms of international law and one of the central pillars of the UN Charter – the legal prohibition on aggressive war enshrined in Article 2(4) of the UN Charter. On 2 March 2022, the UN General Assembly adopted resolution A/Res/ES-11/1, which "deplore[d] in the strongest terms the aggression by the Russian Federation against Ukraine in violation of Article 2(4) of the

¹³³ The sources of international law are authoritatively set out in Article 38 of the *Statute of the International Court of Justice*, which forms part of the *Charter of the United Nations*. Article 38(1)(a) outlines that international treaties and conventions between States are considered international law.

¹³⁴ '2017 Foreign Policy White Paper' Australian Government, Department of Foreign Affairs and Trade, last modified 24 April 2020, page 21, www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/index.html.

¹³⁵ John Dugard, 'The Choice before Us: International Law or a "Rules-Based International Order"?' *Leiden Journal of International Law*, 21 February 2023, 5, <https://doi.org/10.1017/S0922156523000043>.

Charter".¹³⁶ Nearly eighty per cent of States voted in favour of this resolution, with only North Korea, Syria, Belarus, Eritrea, and Russia voting against it. While this resolution was replete with references to the violation of international law, it contained no references to the 'rules-based order'. Singapore's Foreign Minister, in a statement in February 2022, condemned Russia's invasion of Ukraine as a breach of "fundamental norms of international law and the UN Charter that prohibit the use of force and acts of aggression against another sovereign State."¹³⁷ Again, no reference was made to the 'rules-based order'.

In contrast, in response to the same event, statements by the US and Australia are replete with references to the rules-based order. In March 2022, US President Biden labelled Russia's invasion of Ukraine a "direct challenge to the [post-war] rule-based international order".¹³⁸ In a New York Times op-ed in June 2022, Biden declared that Putin's aggression could spell the end for the 'rules-based international order' and "open the door" to aggression elsewhere.¹³⁹ At a NATO summit in June of that year, Biden, making a notable reference to the role of democracies, claimed that he told Putin that its invasion of Ukraine would "see democracies in the world stand up and oppose his aggression and defend the rules-based order."¹⁴⁰ Similarly, Australia's Foreign Minister labelled Russia's actions a breach of "bedrock principles ... of the rules-based order."¹⁴¹

Twenty years ago, however, another military intervention by a Permanent Member of the UN Security Council in another sovereign State prompted similar allegations from many quarters of a breach of Article 2(4) of the UN Charter – the US invasion of Iraq. It is here that one of the fundamental weaknesses of the emphasis on breaches of the 'rules-based order' over 'international law' lies in that the emphasis on claims that certain actions by Russia and China 'challenge' or 'destroy' this order exposes the proponents of this term, chiefly the US but also Australia, to charges of inconsistency or even hypocrisy.

¹³⁶ 'Research Guides: UN General Assembly Resolutions Tables: Emergency Special Sessions', United Nations, Dag Hammarskjöld Library, accessed 26 September 2023, <https://research.un.org/en/docs/ga/quick/emergency>.

¹³⁷ 'Minister for Foreign Affairs Dr Vivian Balakrishnan's Ministerial Statement on the Situation in Ukraine and Its Implications', Singapore Ministry of Foreign Affairs, accessed 26 September 2023, <http://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/02/20220228-Ministerial-Statement>.

¹³⁸ The White House, 'Remarks by President Biden on the United Efforts of the Free World to Support the People of Ukraine', The White House, 26 March 2022, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/26/remarks-by-president-biden-on-the-united-efforts-of-the-free-world-to-support-the-people-of-ukraine/>.

¹³⁹ Dugard, 'The Choice before Us', 1.

¹⁴⁰ 'Biden Says NATO Meets Challenges of Today, Prepares to Counter Threats of Tomorrow', U.S. Department of Defense, accessed 26 September 2023, <https://www.defense.gov/News/News-Stories/Article/Article/3080993/biden-says-nato-meets-challenges-of-today-prepares-to-counter-threats-of-tomorr/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F3080993%2Fbiden-says-nato-meets-challenges-of-today-prepares-to-counter-threats-of-tomorr%2F>.

¹⁴¹ 'Statement on Russia's Invasion of Ukraine', Australian Government Department of Foreign Affairs and Trade, 24 February 2022, <https://www.foreignminister.gov.au/minister/marise-payne/media-release/statement-russias-invasion-ukraine>.

As Professor Murphy, a former international lawyer in the US State Department, highlights, the US itself has a track record of violating Article 2(4) of the UN Charter through the illegal use of force in Kosovo (alongside other NATO members) and against Iraq in 2003.¹⁴² Australia was also a participant in the US 'coalition of the willing', an action for which, as observed previously, the Howard Government was treated to allegations from Kevin Rudd that it was 'junking' the rules-based order. Considering this, it can be difficult to unpack the logic behind assertions that Russia's actions in Ukraine – an unquestionably flagrant violation of perhaps the UN Charter's most critical obligation – pose an existential challenge to the 'rules-based order' whereas breaches of that same norm by the US and its like-minded partners do not. Indeed, Henry Kissinger, in the context of the Kosovo conflict, reflected that "the abrupt abandonment of the concept of national sovereignty" by the West risked grave consequences for global order.¹⁴³ In the context of Iraq, in addition to Rudd's critique explored in Chapter One, Elizabeth Wilmshurst, a long-serving UK Foreign Office lawyer, resigned in response to the UK's decision to invade in 2003 on the basis that the action was a "crime of aggression ... so detrimental to international order and the rule of law".¹⁴⁴

A similar dynamic is evident with respect to China. In 2016, US President Obama told China that the Arbitral Tribunal's ruling, which found China's nine-dash-line was not valid legally, was "binding" and that China should comply in order to "maintain the rules-based international order".¹⁴⁵ The US' record in terms of adherence to binding international judicial decisions has not been exemplary. In 1986, the International Court of Justice ('ICJ') – the UN's principal judicial body – found that the US' arming of the contra rebels and the mining of Nicaragua's harbours amounted to an illegal use of force and a violation of Nicaragua's sovereignty.¹⁴⁶ The US refused to accept the Court's ruling, which included calls for reparations for Nicaragua. The then US Ambassador to the UN claimed the Court was a "semi-legal" entity that "nations sometimes accept and sometimes don't." In fact, under Article 59 of the ICJ's Statute, ICJ rulings are binding on the parties to the dispute.¹⁴⁷ US attempts to withdraw from its recognition of the ICJ's jurisdiction in disputes brought against the US ('compulsory jurisdiction') in 1985 were found by the Court not to be applicable to the Nicaragua case.¹⁴⁸ The US had recognised the Court's compulsory jurisdiction since 1946.¹⁴⁹

¹⁴² Murphy, John F., *The United States and the Rule of Law in International Affairs* (Cambridge: Cambridge University Press, 2004), 350.

¹⁴³ Robert Kagan, "America's Crisis of Legitimacy," *Foreign Affairs* 83, no. 2 (March/April 2004): 65-87, page 75.

¹⁴⁴ Richard Norton-Taylor, "War resignation letter censored", *The Guardian*, 25 March 2005, <https://www.theguardian.com/politics/2005/mar/24/uk.iraq>.

¹⁴⁵ 'South China Sea: Obama Urges Beijing to Abide by Ruling', *BBC News*, 3 September 2016, <https://www.bbc.com/news/world-asia-china-37267372>.

¹⁴⁶ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, International Court of Justice, accessed 27 October 2023, <https://www.icj-cij.org/case/70/judgments>.

¹⁴⁷ 'How the Court works', *International Court of Justice*, accessed 27 September 2023, <https://www.icj-cij.org/how-the-court-works#:~:text=The%20judgment%20is%20final%2C%20binding,an%20opinion%20to%20the%20judgment>.

¹⁴⁸ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, International Court of Justice, accessed 27 October 2023, <https://www.icj-cij.org/case/70/judgments>.

¹⁴⁹ "Foreign relations of the United States, 1946", *US State Department*, accessed 25 October 2023,

In addition to instances where international law has been violated, the US has refused to subject itself to the very international standards that it demands others adhere to. For instance, and as discussed in Chapter Three, while the US, Australia and others criticise China for its failure to act consistent with its obligations under UNCLOS, the US remains one of the small number of States, most of which are developing, landlocked States, that are not party to UNCLOS.¹⁵⁰ US concerns that portions of UNCLOS related to deep sea-bed mining represent a form of socialism only serve to reinforce perceptions of US exceptionalism when it comes to being bound by international law.¹⁵¹

Murphy argues that the US struggles with the constraining effect of international law due to the US' "triumphalism" and "exceptionalism", as well as its "distrust of centralized power". As a result, the US prefers international institutions, such as the UN Security Council and the World Bank, where it enjoys substantial influence and control.¹⁵² Australia has echoed similar sentiments. Just weeks after describing the UN as the "prime custodian of the rules-based order", Prime Minister Morrison railed against 'negative globalism', the impositions of the 'borderless global community' and an 'unaccountable internationalist bureaucracy'.¹⁵³ In a demonstration of limited faith in the multilateral bodies he had just anointed the custodians of the 'rules-based order', Morrison announced a "comprehensive audit of global institutions and rule-making processes."¹⁵⁴

The emphasis on allegations of the breach of the 'rules-based order', as opposed to international law, risks further diminishing the appeal of 'rules-based order' terminology for three key reasons. First, there is a risk that the use of the term – which is used primarily by the US and its allies – is viewed by others as an insincere or cynical effort to simultaneously brand certain actors as malign, sometimes while avoiding specific charges, while masking past failures of the accusing State to act consistent with international rules. As Singapore's Mahbubani has pointed out in the context of the US invasion of Iraq, "how can the violators of UN principles also be their enforcers?"¹⁵⁵ Second, the characterisation of some States' breaches of international law as posing jeopardy to the 'rules-based order' itself, even in the context of similar past breaches by accusing States, risks highlighting a perception that some Western States consider themselves 'exceptional' or above the constraining effect of international law as a result

<https://history.state.gov/historicaldocuments/frus1946v01/d34#:~:text=The%20Declaration%20by%20the%20United,of%20August%2016%20by%20the>

¹⁵⁰ 'United Nations Treaty Collection', accessed 27 October 2023,

https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_en.

¹⁵¹ 'Hypocri-Sea: The United States' Failure to Join the UN Convention on the Law of the Sea', *Harvard International Review*, 31 October 2019, <https://hir.harvard.edu/hypocri-sea-the-united-states-failure-to-join-the-un-convention-on-the-law-of-the-sea-2/>.

¹⁵² Murphy, *The United States and the Rule of Law in International Affairs*, 354.

¹⁵³ Paul Karp, 'Scott Morrison Gave "negative Globalism" Speeches without Consulting Dfat', *The Guardian*, 24 October 2019, <https://www.theguardian.com/australia-news/2019/oct/25/scott-morrison-gave-negative-globalism-speeches-without-consulting-dfat>.

¹⁵⁴ Paul Karp, 'Scott Morrison Gave "negative Globalism" Speeches without Consulting Dfat', *The Guardian*, 24 October 2019, <https://www.theguardian.com/australia-news/2019/oct/25/scott-morrison-gave-negative-globalism-speeches-without-consulting-dfat>.

¹⁵⁵ Kishore Mahbubani, "The Case against the West - America and Europe in the Asian Century," *Foreign Affairs* 87, no. 3 (May/June 2008): 111-125, page 114.

of their hegemonic or privileged status within the 'rules-based order'.

Third, there is a risk that an overemphasis on breaches of the rules-based order can, in practice, dilute support for the criticism of flagrant violations of international law because of a perceived politicisation of the issue and importation of geopolitical and 'bloc' dynamics. This can already be seen in the context of the situation in Ukraine at the United Nations, where resolutions that call on Russia to withdraw its military forces from Crimea and end its occupation attracted predominantly Western support, with only 62 out of 193 UN members voting in favour.¹⁵⁶ The following Chapter explores this issue further.

¹⁵⁶ 'General Assembly Adopts 51 Resolutions, 13 Decisions Forwarded by Fourth, Sixth Committees', United Nations Press, accessed 25 August 2023, <https://press.un.org/en/2021/ga12394.doc.htm>.

Chapter 6: Who is using 'rules-based order' terminology? Who is not?

This Chapter reinforces this paper's conclusion that the 'rules-based order' terminology is of limited appeal beyond the West by demonstrating that while it is in favour in the West, and principally, in Australia, the US and the UK, it is explicitly rejected as a geopolitical construct by China and Russia and not typically utilised by other States in the Indo-Pacific. While Germany, as canvassed previously, Austria and others also use the formulation, these States tend to ascribe to it a more technical definition, focused on international law, norms of a non-legal character and norm-generating multilateral institutions, such as the UN and its dispute resolution tribunals and bodies.

For many Europeans, the rules-based order is more closely intertwined with international law and legal structures, such as the UN system, and less with power dynamics. As explored previously, for Germany, the order covers international law, but also "non-binding norms, standards and procedures in various international fora and negotiating processes."¹⁵⁷ Austria defines the 'rules-based order' as largely analogous to international law, describing it as "a system comprising international law, treaties, customary law as well as general principles of law as outlined in the Statute of the International Court of Justice (ICJ)." The order also required the "settlement of disputes by peaceful means", including through international judicial processes.¹⁵⁸

In contrast, Russia and China maintain that the 'rules-based order' formulation serves as a stalking horse for US and Western hegemony. Russia objects to the perceived lack of clarity regarding the order's content. Lavrov has stated that the West "shies away from spelling out the 'rules' it purports to follow" and accuses any State that acts against "the will of the West" of being a "rule breaker".¹⁵⁹ Lavrov criticises the West's claims to the universality and the inevitability of its liberal values and its democratic political systems, observing that there is more than simply one civilisation in the world.¹⁶⁰

Similarly, China considers it an 'ambiguous formulation' not found in the UN Charter or the UN's resolutions.¹⁶¹ It views the formulation as a vehicle to "impose [Western] standards and will on others" and as a "back door to double standards and exceptionalism." In 2022, Russia and China issued a joint statement that implicitly rejected the order in favour of an 'international law-based world order'.¹⁶²

Beyond the US and its allies in Western Europe and East Asia, the use of the 'rules-

¹⁵⁷ Stefan Talmon, 'Notable Statements on International Law during March 2020', *German Practice in International Law*, 12 May 2020, <https://gpil.jura.uni-bonn.de/2020/05/notable-statements-on-international-law-during-march-2020/>.

¹⁵⁸ 'UN General Assembly - Legal - Sixth Committee', United Nations, accessed 27 October 2023, https://www.un.org/en/ga/sixth/76/rule_of_law.shtml.

¹⁵⁹ Sebastiaan Van Severen, 'Lavrov's Lament: A Russian Take on the Rules-Based Global Order', *EJIL: Talk!* (blog), 16 July 2021, 1, <https://www.ejiltalk.org/lavrovs-lament-a-russian-take-on-the-rules-based-global-order/>.

¹⁶⁰ Van Severen, 1.

¹⁶¹ 'Research Guides: UN Security Council Meetings & Outcomes Tables: 2023 (S/RES/2672-)', United Nations. Dag Hammarskjöld Library, accessed 26 August 2023, <https://research.un.org/en/docs/sc/quick/meetings/2023>.

¹⁶² 'Russia-China Joint Statement on International Relations, February 4, 2022', US China Institute, accessed 1 October 2023, <https://china.usc.edu/russia-china-joint-statement-international-relations-february-4-2022>.

based order' formulation is more limited. While Australia's former Prime Minister Morrison dubbed the UN the "prime custodian" of the rules-based order,¹⁶³ the international organisation which enjoys the greatest universality and international legitimacy as a forum for international cooperation has largely eschewed the 'rules-based order' formulation in its statements and decisions.

While the US and others suggest that Russia's invasion of Ukraine threatened to shatter the very foundations of the 'rules-based order', the UN General Assembly's resolution in response to Russia's invasion contained no references to this formulation or to 'order', its eight references to 'rules' were to specific international legal rules.¹⁶⁴ On 21 September 2020, the UN General Assembly adopted a resolution to celebrate the 75th anniversary of the 1945 UN Charter, a treaty establishing an institution that is a core component of most conceptions of the 'rules-based order'. This resolution contained no references to the 'rules-based order'. In a 2023 UN Security Council open debate on the 'rule of law in the maintenance of international peace and security', the US and UK statements emphasised the importance of the 'rules-based order'. In contrast, Russia and China criticised the formulation in familiar terms. Malta was the only other State that employed the term. Malta's statement described this order as "enshrined in the UN Charter", an approach more in line with Germany's or Austria's characterisation.¹⁶⁵

Turning to the Indo-Pacific, the 'rules-based order' formulation is not typically employed in the language used by its regional institutions. The 2019 ASEAN 'Outlook on the Indo-Pacific' statement does not employ the phrase.¹⁶⁶ In contrast, the formulation receives significant prominence in statements and strategies on the Indo-Pacific from the US, Australia, and others. While it is common for the statements from Western liberal democracies to be replete with references to the rules-based order, statements from the last four ASEAN Leaders Summits contain only a single reference to 'rules-based order', which in that instance referred explicitly to legal cooperation between ASEAN members on an extradition treaty.¹⁶⁷

While ASEAN member states have not articulated a common position on the formulation, for some key thinkers in the region, it is evident that the 'rules-based order' formulation is perceived as intertwined with 'liberal and internationalist beliefs shared among political elites in Western countries' and is considered designed to 'counter assumed challenges' from non-Western States and blocs.¹⁶⁸ For others, it is seen as code for a 'US-led Western order', in which the core norms include the promotion of

¹⁶³ Lowy Institute, 'Rules Based Order'.

¹⁶⁴ 'A/RES/ES-11/1 : UN Documents : Security Council Report', accessed 27 October 2023, <https://www.securitycouncilreport.org/un-documents/document/a-res-es-11-1.php>.

¹⁶⁵ 'Research Guides: UN Security Council Meetings & Outcomes Tables: 2023 (S/RES/2672-)', United Nations. Dag Hammarskjöld Library, accessed 26 August 2023, <https://research.un.org/en/docs/sc/quick/meetings/2023>.

¹⁶⁶ 'ASEAN Outlook on the Indo-Pacific', ASEAN Main Portal, accessed 27 October 2023, <https://asean.org/speechandstatement/asean-outlook-on-the-indo-pacific/>.

¹⁶⁷ 'Statements Archives', ASEAN Main Portal, accessed 27 October 2023, <https://asean.org/category/statements-meetings/>.

¹⁶⁸ 'Rules-Based Order: What Does the Region Think?', *Asialink*, University of Melbourne, Ric Smith and Tony Milner, 17 August 2021, 3, <https://asialink.unimelb.edu.au/insights/rules-based-order-what-does-the-region-think>.

liberal democracy, free trade and universal human rights standards.¹⁶⁹

There is a perception in the region that the 'rules-based order' is an inherently political term, closely aligned with the US and its democratic system of government. Alignment with and use of this terminology could be viewed as being at odds with a strong desire in the region not to "discriminate against any political system" nor to choose between the US and China.¹⁷⁰ This may well explain why the rules-based order formulation enjoys limited prominence in the Indo-Pacific region, and where it is employed, it is typically not used in ways that align with Western conceptions of the term.

¹⁶⁹ 'Rules-Based Order: What Does the Region Think?', *Asialink*, University of Melbourne, Ric Smith and Tony Milner, 17 August 2021, 3, <https://asialink.unimelb.edu.au/insights/rules-based-order-what-does-the-region-think>.

¹⁷⁰ 'Rules-Based Order: What Does the Region Think?', *Asialink*, University of Melbourne, Ric Smith and Tony Milner, 17 August 2021, 3, <https://asialink.unimelb.edu.au/insights/rules-based-order-what-does-the-region-think>.



Images: Department of Defence

Chapter 7: Implications for Australia's foreign policy

As Australia's Foreign Minister, Penny Wong, has articulated, Australia's vision is for a region that "operates by rules ... where a larger country does not determine the fate of a smaller country".¹⁷¹ As this paper has demonstrated, there is a risk that the 'rules-based order' formulation is perceived as being at odds with Wong's statement, given the perception that Australia sees this order as encompassing US hegemony and a privileged role for liberal democracies.

This paper argues that Australia must articulate more clearly how it sees rules, rulemaking, and rule-adjudicating processes contributing to prosperity, order, and stability in the Indo-Pacific and beyond. Such a statement would benefit from the inclusion of the following five elements.

First, Australia should emphasise the importance of States, big and small, allies and competitors, adhering to international law. Recognising that States can only be bound by international law to which they consent, certain critical international agreements, including but not limited to the UN Charter, UNCLOS and the NPT, are critical guarantors of stability in the Indo-Pacific. Australia should articulate this point and strongly encourage all States to be party to these treaties. While adherence to all international legal obligations is important, it must be recognised that some international law norms are foundational and critical to regional order and stability and are deserving of greater emphasis, such as the obligations of States to refrain from the use of force, save in self-defence, and the obligation of non-interference and respect for the sovereignty of other States, norms which are enshrined in Article 2 of the UN Charter.

Second, Australia should emphasise the importance of States committing to the peaceful resolution of disputes, a core legal norm found also in Article 2 of the UN Charter. States should demonstrate this commitment by undertaking to resolve all disputes peacefully and in accordance with international law. Where disputes cannot be resolved bilaterally, these should be submitted to relevant global judicial and arbitral processes. In line with this, States should submit to the compulsory jurisdiction of the International Court of Justice, as Australia has done.¹⁷²

Third, acknowledging that rules, not power, should regulate interactions between States, States in the Indo-Pacific should make a joint commitment to negotiate new rules where it is necessary to deal with challenges requiring collective action or in situations where there is a particular risk of tension, such as in the context of border, territorial, or maritime disputes. Such rules may be global, regional, or even bilateral. Ideally, such rules would be legally binding, but in some instances, that may not be achievable, and instead, rules may be non-legally binding (sometimes referred to as 'less than treaty status instruments').¹⁷³

¹⁷¹ 'National Press Club Address, Australian Interests in a Regional Balance of Power', Australian Government, Department of Foreign Affairs and Trade, last modified 17 April 2023, <https://www.foreignminister.gov.au/minister/penny-wong/speech/national-press-club-address-australian-interests-regional-balance-power>.

¹⁷² 'Declarations Recognizing the Jurisdiction of the Court as Compulsory' International Court of Justice, accessed 27 October 2023, <https://www.icj-cij.org/declarations/au>.

¹⁷³ "Australia's practice for concluding less-than-treaty status instruments", Department of Foreign Affairs and Trade, Australian Government, accessed 11 October 2023, <https://www.dfat.gov.au/international-relations/treaties/australias-practice-concluding-less-than-treaty-status-instruments>.

Fourth, appreciating that existing rules and norms that States have agreed can be changed, but that this should be done within the existing frameworks for the amendment of those rules, or by creating, in some instances, new rules. In the process of rulemaking or amending, no States or exclusive collective of States have a unilateral right – unless they have been expressly granted such rights – to make, remove or enforce the rules. Fifth, the States in the Indo-Pacific must commit to open and regular dialogue between all States in the region as an essential pillar of their international relations and as a mechanism for building understanding and solving common problems.

Conclusion

As this paper has acknowledged, research has been limited to English-language sources. Thus, in drawing conclusions about the reaction of States in the Indo-Pacific to 'rules-based order' terminology, greater emphasis has been placed on the role of perception. Further research in this space could explore in more detail non-English sources to establish first-hand regional and international perspectives on the use of 'rules-based order' terminology. Additional research could also focus on the origins of the blending of the 'rules-based order' concept with the more overtly ideological 'liberal international order' terminology. The working hypothesis of this paper is that the 'rules-based order' first originated as a term designed to intertwine global order more closely with international law and law-making and enforcing multilateral institutions, as was demonstrated in its early usage including in the context of the 2003 Iraq war. Though, ultimately, the 'rules-based order' terminology began to be infused rhetorically, at least in Australia and the US, with the norms of the 'liberal international order'. In recent decades, the term 'the rules-based international order' has assumed a central position in Australia's foreign and security policy. While Australia places considerable stock in this order, it also claims that all States in the Indo-Pacific – friends, competitors, and foes alike – have benefited from this framework and have a stake in its defence. Given the criticality that Australia ascribes to this order, both for itself and for the region and beyond, and given the absence of any concrete and substantive definitions for this 'order,' this paper has sought to explore how the rules-based order is defined and whether it is a suitable term to employ as a central principle of Australia's foreign and security policy.

This paper finds that while the 'rules-based order' itself is typically said to have been created post World War Two, the term itself only entered the political lexicon in Australia in the last twenty years. The term is primarily spoken about in Australia, the US and elsewhere as being synonymous with the 'liberal international order', sending the signal that Australia and others view US hegemony and the 'civilising mission' of overseas democracy promotion, sometimes, as Mead suggested in the context of the Iraq invasion in 2003, via the barrel of a gun as core ideals of the order. While the norms of the 'liberal international order' bring some coherence to the concept of a rules-based order, broader efforts to encapsulate the content and even the origins of the order tend to be disparate and incoherent.

Contemporary use of 'rules-based order' language by Australia and the US, particularly given the 'liberal' elements these States have imported to the term, risk framing attacks on significant violators of international law – such as Russia's invasion of Ukraine – through the lens of strategic competition where there is an implicit request to 'choose sides'. Further, the use of 'rules-based order' terminology can be perceived as a cynical effort to mask or downplay past violations, or rejection, of international law by user States, including based on claims to exceptionalism. Accordingly, this paper concludes that Australia's use of 'rules-based order' terminology to rally international action in support of Australia's interests should be rethought.

As this paper has acknowledged, research has been limited to English-language sources. Thus, in drawing conclusions about the reaction of States in the Indo-Pacific to 'rules-based order' terminology, greater emphasis has been placed on the role of perception. Further research in this space could explore in more detail non-English sources to establish first-hand regional and international perspectives on the use of 'rules-based order' terminology. Additional research could also focus on the origins of the blending of the 'rules-based order' concept with the more overtly ideological 'liberal international order' terminology. The working hypothesis of this paper is that the 'rules-

based order' first originated as a term designed to intertwine global order more closely with international law and law-making and enforcing multilateral institutions, as was demonstrated in its early usage including in the context of the 2003 Iraq war. Though, ultimately, the 'rules-based order' terminology began to be infused rhetorically, at least in Australia and the US, with the norms of the 'liberal international order'.

Bibliography

Anwar, Dewi Fortuna. 'A Rules-Based Order in the Indo-Pacific: A view from Jakarta', *Journal of Indo-Pacific Affairs*, 2020, 42-47, page 46.

Association of Southeast Asian Nations - Secretariat. 'ASEAN Outlook on the Indo-Pacific'. Accessed 27 October 2023. <https://asean.org/speechandstatement/asean-outlook-on-the-indo-pacific/>.

Association of Southeast Asian Nations - Secretariat. 'Statements Archives'. Accessed 27 October 2023. <https://asean.org/category/statements-meetings/>.

Commonwealth of Australia, Department of Defence. 'Defence White Paper'. Accessed 19 September 2023. <https://www.defence.gov.au/about/strategic-planning/defence-white-paper>.

Commonwealth of Australia, Department of Defence. 'National Defence: Defence Strategic Review 2023'. Accessed 14 June 2023. <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>.

Australian Government, Department of Foreign Affairs and Trade. 'Australia Supports Peaceful Dispute Resolution in the South China Sea'. Last modified 12 July 2016. <https://www.foreignminister.gov.au/minister/julie-bishop/media-release/australia-supports-peaceful-dispute-resolution-south-china-sea>.

Australian Government, Department of Foreign Affairs and Trade. 'La Trobe University Lecture and Conversation'. Last modified 11 April 2018. <https://www.foreignminister.gov.au/minister/julie-bishop/speech/la-trobe-university-lecture-and-conversation>.

Australian Government, Department of Foreign Affairs and Trade. 'National Press Club Address, Australian Interests in a Regional Balance of Power'. Last modified 17 April 2023. <https://www.foreignminister.gov.au/minister/penny-wong/speech/national-press-club-address-australian-interests-regional-balance-power>.

Australian Government, Department of Foreign Affairs and Trade. 'Statement on Russia's Invasion of Ukraine'. Last modified 24 February 2022. <https://www.foreignminister.gov.au/minister/marise-payne/media-release/statement-russias-invasion-ukraine>.

Barrett, Chris. "We Don't Want to Pick Sides: The View from South-East Asia as China Woos Pacific." *The Sydney Morning Herald*, 26 May 2022. <https://www.smh.com.au/world/asia/we-don-t-want-to-pick-sides-the-view-from-south-east-asia-as-china-woos-pacific-20220526-p5aosj.html>.

'South China Sea: Obama Urges Beijing to Abide by Ruling'. *BBC News*. Last modified 3 September 2016, <https://www.bbc.com/news/world-asia-china-37267372>.

Beinart, Peter. 'The Vacuous Phrase at the Core of Biden's Foreign Policy'. *The New York Times*, 22 June 2021. <https://www.nytimes.com/2021/06/22/opinion/biden-foreign-policy.html>.

Biden, Joseph R. 'Why America Must Lead Again'. *Foreign Affairs*. Last modified 23 January 2020. <https://www.foreignaffairs.com/articles/united-states/2020-01-23/why->

america-must-lead-again.

Bisley, Nick, and Schreer, Benjamin. "Australia and the Rules-Based Order in Asia". *Asian Survey* 58, no. 2 (April 2018): 302–19.

The Brookings Institution. 'A Conversation with the Prime Minister of Australia, the Hon. Kevin Rudd MP'. Accessed 19 September 2023. <https://www.brookings.edu/events/a-conversation-with-the-prime-minister-of-australia-the-hon-kevin-rudd-mp/>.

Bosco, David L. *Five to Rule Them All*. Oxford University Press, 2009.

Bull, Hedley. *The Anarchical Society: A Study of Order in World Politics*. New York: Palgrave, 1977.

Chalmers, Malcolm. 'Which Rules? Why There Is No Single "Rules-Based International System"'. Accessed 21 July 2023. <https://www.rusi.org>.

Chatham House. "Challenges to the Rules-based international order", accessed 3 September 2023, <https://www.chathamhouse.org/sites/default/files/London%20Conference%202015%20-%20Background%20Papers.pdf>.

China Daily. 'Rules-Based Order: Hypocrisy Masquerading as Principle'. Accessed 24 April 2023. <https://s.chinadailyhk.com/mUF3Af>.

Embassy of the People's Republic of China, Australia. 'Australia and China: A Strong and Stable Partnership for the 21st Century'. Last modified 6 January 2005. <https://web.archive.org/web/20050126165251/http://au.china-embassy.org/eng/zagx/t142076.htm>.

United Nations. 'Declaration of the United Nations Conference on the Human Environment'. Accessed 11 October 2023. <https://legal.un.org/avl/ha/dunche/dunche.html>.

United Nations. 'Declaration on the Granting of Independence to Colonial Countries and Peoples'. Accessed 25 October 2023. <https://legal.un.org/avl/ha/dicc/dicc.html>.

International Court of Justice. 'Declarations Recognizing the Jurisdiction of the Court as Compulsory'. Accessed 27 October 2023. <https://www.icj-cij.org/declarations/au>.

Dugard, John. 'The Choice before Us: International Law or a "Rules-Based International Order"?'. *Leiden Journal of International Law*, 21 February 2023, 1–10. <https://doi.org/10.1017/S0922156523000043>.

Falk, Richard A., "Kosovo, World Order, and the Future of International Law." *The American Journal of International Law*, No. 4 (Oct., 1999), pp. 847-85.

Ern Ho, Benjamin Tze. 'A Finely Fractured Consensus: American Motivations for Rules-Based Order'. *The Washington Quarterly* 45, no. 4 (2 October 2022): 61–76. <https://doi.org/10.1080/0163660X.2022.2148506>.

United Nations. 'General Assembly Adopts 51 Resolutions, 13 Decisions Forwarded by Fourth, Sixth Committees | UN Press'. Accessed 7 October 2023.

<https://press.un.org/en/2021/ga12394.doc.htm>.

Haass, Richard N. 'The Unraveling: How to Respond to a Disordered World'. *Foreign Affairs* 93, no. 6 (2014): 70–79.

Harvard International Review. 'Hypocri-Sea: The United States' Failure to Join the UN Convention on the Law of the Sea'. Last modified 31 October 2019.
<https://hir.harvard.edu/hypocri-sea-the-united-states-failure-to-join-the-un-convention-on-the-law-of-the-sea-2/>.

The White House. 'Remarks by President Biden on the United Efforts of the Free World to Support the People of Ukraine'. Last modified 26 March 2022.
<https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/26/remarks-by-president-biden-on-the-united-efforts-of-the-free-world-to-support-the-people-of-ukraine/>.

Ikenberry, G. John. 'Reflections on After Victory'. *The British Journal of Politics and International Relations* 21, no. 1 (2019): 5–19.

Ikenberry, G. John. 'The End of Liberal International Order?' *International Affairs* 94, no. 1 (1 January 2018): 7–23. <https://doi.org/10.1093/ia/iix241>.

Ikenberry, G. John, and Daniel Deudney. 'The Nature and Sources of Liberal International Order'. *Review of International Studies* 25, no. 2 (April 1999): 179–96.

Jorgensen, Malcolm. 'The German National Security Strategy and International Legal Order's Contested Political Framing'. *EJIL: Talk!* (blog). Accessed 5 July 2023.
<https://www.ejiltalk.org/international-legal-orders-contested-political-framing/>.

Kagan, Robert. "America's Crisis of Legitimacy," *Foreign Affairs* 83, no. 2 (March/April 2004): 65-87

Karp, Paul. 'Scott Morrison Gave "Negative Globalism" Speeches without Consulting DFAT'. *The Guardian*. Last modified 24 October 2019.
<https://www.theguardian.com/australia-news/2019/oct/25/scott-morrison-gave-negative-globalism-speeches-without-consulting-dfat>.

Kausikan, Bilahari. 'Perspectives: What (and Whose) Rules-Based Order (RBO)?' *Asialink*. Last modified 17 August 2021. <https://asialink.unimelb.edu.au/insights/what-and-whose-rules-based-order-rbo>.

Australian Government, Department of Defence. 'Keynote Address, Hudson Institute, Washington DC'. Last modified 2 November 2019.
<https://www.minister.defence.gov.au/speeches/2019-11-02/keynote-address-hudson-institute-washington-dc>.

Kiernan, V.G. *The Lords of Human Kind : European Attitudes to Other Cultures in the Imperial Age*. Serif, 1995.

United Nations, Dag Hammarskjöld Library. 'Research Guides: UN General Assembly Resolutions Tables: Emergency Special Sessions'. Accessed 26 September 2023.
<https://research.un.org/en/docs/ga/quick/emergency>.

United Nations. 'Research Guides: UN Security Council Meetings & Outcomes Tables:

2023 (S/RES/2672-)'. Accessed 26 October 2023.
<https://research.un.org/en/docs/sc/quick/meetings/2023>.

Latham, Andrew. 'The Rules-Based International Order Is Ending. What Will Replace It?'. Accessed 14 June 2023. <https://thehill.com/opinion/national-security/3736389-the-rules-based-international-order-is-ending-what-will-replace-it/>.

Loh, Dylan M. H. 'Singapore's Conception of the Liberal International Order as a Small State', *International Affairs* 99, no. 4 (3 July 2023): 1499–1518,
<https://doi.org/10.1093/ia/iad161>.

Lowy Institute. 'Rules Based Order - Lowy Institute'. Accessed 18 September 2023.
<https://interactives.lowyinstitute.org/features/rules-based-order/>.

Lowy Institute. 'Rules-Based Order: What's in a Name?' Accessed 29 September 2023. <https://www.lowyinstitute.org/the-interpreter/rules-based-order-what-s-name>.

Mahbubani, Kishore. "The Case against the West - America and Europe in the Asian Century," *Foreign Affairs* 87, no. 3 (May/June 2008): 111-125

Mazarr, Michael J., Miranda Priebe, Andrew Radin, and Astrid Stuth Cevallos. 'Understanding the Current International Order'. *RAND Corporation*. Last modified 19 October 2016. https://www.rand.org/pubs/research_reports/RR1598.html.

Mead, Walter Russell. 'The End of the Wilsonian Era: Why Liberal Internationalism Failed', *Foreign Affairs* 100, no. 1 (February 2021): 123–37.

Singapore, Ministry of Foreign Affairs. 'Minister for Foreign Affairs Dr Vivian Balakrishnan's Ministerial Statement on the Situation in Ukraine and Its Implications'. Accessed 26 September 2023. <http://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/02/20220228-Ministerial-Statement>.

Murphy, John F. *The United States and the Rule of Law in International Affairs*. Cambridge: Cambridge University Press, 2004.

Norton-Taylor, Richard. "War resignation letter censored", *The Guardian*, 25 March 2005, <https://www.theguardian.com/politics/2005/mar/24/uk.iraq>.

United Nations. 'Universal Declaration of Human Rights'. Accessed 11 October 2023. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

United Nations. 'Uphold International Law'. Accessed 10 October 2023. <https://www.un.org/en/our-work/uphold-international-law>.

International Court of Justice. 'Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)'. Accessed 27 October 2023. <https://www.icj-cij.org/case/70/judgments>.

Organisation for the Prohibition of Chemical Weapons. 'History'. Accessed 3 October 2023. <https://www.opcw.org/about-us/history>.

Our World in Data. 'Liberal Democracy Index'. Accessed 2 October 2023. <https://ourworldindata.org/grapher/liberal-democracy-index>.

Department of Foreign Affairs and Trade, Australian Government. 'Foreign Policy White Paper - 2017'. Last modified 24 April 2020. <https://www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/index.html>.

Parliament House, Commonwealth of Australia. 'ParlInfo - Change and Uncertainty in the IndoPacific: Strategic Challenges and Opportunities: Speech to the 28th IISS Fullerton Lecture, Singapore'. Accessed 21 September 2023. <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pre-srel/5160178%22>.

Parliament House, Commonwealth of Australia. "Strong and Secure – A Strategy for Australia's National Security", accessed 25 June 2023, <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22library/lcatalog/00500351%22>.

Australian Labor Party. 'Kevin Rudd - The Three Pillars Of Labor's National Security Policy'. *Bibliothek der Friedrich-Ebert-Stiftung*. Last modified 15 October 2003. <https://library.fes.de/aussies/2003/1003/20006086.html>.

Patrick, Stewart, "World Order: What, Exactly, are the Rules?", *The Washington Quarterly*, 39:1, 7-27, DOI: 10.1080/0163660X.2016.1170477

Porter, Patrick. 'Sorry, Folks. There Is No Rules-Based World Order.' *The Center for the National Interest*. 28 August 2016. <https://nationalinterest.org/blog/the-skeptics/sorry-folks-there-no-rules-based-world-order-17497>.

Porter, Patrick. 'Wrestling with Fog: On the Elusiveness of Liberal Order'. *War on the Rocks*. Last modified 15 July 2020. <http://warontherocks.com/2020/07/wrestling-with-fog-on-the-elusiveness-of-liberal-order/>.

Price, Megan. 'Norm Erosion and Australia's Challenge to the Rules-Based Order'. *Australian Journal of International Affairs* 75, no. 2, January 2021: 161–77. <https://doi.org/10.1080/10357718.2021.1875983>.

US-China Institute. 'Russia-China Joint Statement on International Relations, February 4, 2022'. Accessed 25 October 2023. <https://china.usc.edu/russia-china-joint-statement-international-relations-february-4-2022>.

United Nations. 'Security Council holds first debate on Iraq since start of military action; speakers call for halt to aggression, immediate withdrawal'. Accessed 25 October 2023. <https://press.un.org/en/2003/sc7705.doc.htm>.

Sloss, David. *Is the International Legal Order Unraveling?* Oxford University Press, 2022.

The White House. 'Statement from National Security Advisor Robert C. O'Brien – The White House'. Accessed 21 September 2023. <https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-011221/>.

Government of India, Ministry of External Affairs. 'Statement on the Current Situation Related to Iraq'. Accessed 11 October 2023. https://www.mea.gov.in/press-releases.htm?dtl/9209/Statement_on_the_current_situation_related_to_Iraq.

Talmon, Stefan. 'Notable Statements on International Law during March 2020'. *German Practice in International Law*. Last modified 12 May 2020. <https://gpil.jura.uni-bonn.de/2020/05/notable-statements-on-international-law-during-march-2020/>.

'The Liberal Order of the Past 70 Years Is under Threat'. *The Economist*. Accessed 29 September 2023. <https://www.economist.com/books-and-arts/2017/09/21/the-liberal-order-of-the-past-70-years-is-under-threat?giftId=9ee2a2a5-2e4c-4024-8a72-2c031f304e83>.

The Institute for Peace and Diplomacy. 'Canada's Dilemma: China and the "Rules-Based International Order"'. Last modified 14 June 2022. <https://peacediplomacy.org/2022/06/14/canadas-dilemma-china-and-the-rules-based-international-order/>.

'The Rules-Based International Order Is Ending. What Will Replace It?'. *The Hill*. Accessed 14 June 2023. <https://thehill.com/opinion/national-security/3736389-the-rules-based-international-order-is-ending-what-will-replace-it/>.

United Nations. 'Treaty on the Non-Proliferation of Nuclear Weapons (NPT)'. Accessed 3 October 2023. <https://disarmament.unoda.org/wmd/nuclear/npt/>.

United Nations. 'UN General Assembly - Legal - Sixth Committee'. Accessed 7 October 2023. https://www.un.org/en/ga/sixth/76/rule_of_law.shtml.

United Nations. 'United Nations Treaty Collection'. Accessed 1 October 2023. https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_en.

U.S. Department of Defense. 'Biden Says NATO Meets Challenges of Today, Prepares to Counter Threats of Tomorrow'. Accessed 26 September 2023. <https://www.defense.gov/News/News-Stories/Article/Article/3080993/biden-says-nato-meets-challenges-of-today-prepares-to-counter-threats-of-tomorr/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F3080993%2Fbiden-says-nato-meets-challenges-of-today-prepares-to-counter-threats-of-tomorr%2F>.

U.S. Department of State. 'America's Pacific Century'. Accessed 16 June 2023. <https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/11/176999.htm>.

Tyler, Melissa Conley, Allan Gyngell and Bryce Wakefield. 'Australia and the Rules-Based International Order'. *Australian Institute of International Affairs*. Accessed 27 July 2023. <https://www.internationalaffairs.org.au/publication/australia-and-the-rules-based-international-order/>.

Strating, Dr Bec. 'Perspectives: Preserving the "Rules-Based Order"'. *Asialink*. Last modified 17 August 2021. <https://asialink.unimelb.edu.au/insights/perspectives-preserving-the-rules-based-order>.

Smith, Ric and Tony Milner. 'Rules-Based Order: What Does the Region Think?' *Asialink*. Last modified 17 August 2021. <https://asialink.unimelb.edu.au/insights/rules-based-order-what-does-the-region-think>.

Van Severen, Sebastiaan. 'Lavrov's Lament: A Russian Take on the Rules-Based Global Order'. *EJIL: Talk!* Last modified 16 July 2021. <https://www.ejiltalk.org/lavrovs->

lament-a-russian-take-on-the-rules-based-global-order/.

Vylegzhanin, Alexander, and Magomedova, Olga. 'The Term "Rules-Based International Order" in International Legal Discourses'. *Moscow Journal of International Law*, July 2021, 35–60. <https://doi.org/DOI: 10.24833/0869-0049-2021-2-35-60>.

Warnault, Romain. 'Strategy of "Constrainment"'. *Atlantic Council*, 16 March 2017. <https://www.atlanticcouncil.org/in-depth-research-reports/report/strategy-of-constraintment/>.

United Nations. 'What Is the Universal Declaration on Human Rights?'. Last modified 31 December 2007. <https://humanrights.gov.au/our-work/projects/what-universal-declaration-human-rights>.

The White House. 'Remarks by the Vice President at the US-Japan-South Korea Trilateral Meeting'. Last modified 14 July 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/07/14/remarks-vice-president-us-japan-south-korea-trilateral-meeting>.

The White House. 'Remarks of President Barack Obama – State of the Union Address As Delivered'. Last modified 13 January 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/01/12/remarks-president-barack-obama-%E2%80%93-prepared-delivery-state-union-address>.

Zakaria, Fareed. 'Putin Is Invading Ukraine Because It's a Liberal Democracy'. *The Washington Post*. Accessed 14 June 2023. <https://www.washingtonpost.com/opinions/2022/02/24/putin-invasion-ukraine-shows-why-liberal-democracy-worth-defending/>.



Images: Department of Defence



Autonomy and Artificial Intelligence in Hydrography: Royal Australian Navy's Future Workforce

Commodore Darryn Mullins, RAN



About the Author



Commodore Mullins is currently serving as the Hydrographer of Australia, and the Director General Maritime Geospatial.

Prior to joining the Royal Australian Navy as a Maritime Warfare Officer in 1995, he studied law.

After training in HMA Ships *Torrens*, *Darwin*, *Tarakan*, *Bendigo*, and *Flinders*, he sub-specialised as a Maritime Geospatial Officer – Hydrographic. He then served in HMA Ships *Leeuwin*, *Mermaid*, and *Melville*, participating in operations in Timor Leste and Bougainville. As Officer in Charge of the Deployable Geospatial Support Team, he deployed to Banda Aceh, Indonesia to assist in the response to the devastation of the 2004 Boxing Day tsunami.

Commodore Mullins was recognised as a dual specialist Maritime Warfare Officer/Legal Officer in 1999. He subsequently served as Commanding Officer of HMA Ship *Shepparton*. In his legal capacity, Commodore Mullins has held numerous senior operational and strategic legal positions including Director Navy Legal Service and Director Legal, Headquarters Joint Operations Command (J06).

Summary

This thesis addresses the question:

How would the integration of autonomous systems and artificial intelligence (AI) in the Royal Australian Navy's (RAN) hydrographic capability impact workforce transformation?

Driven by the strategic imperatives of the 2023 Defence Strategic Review (DSR) for a 'Strategy of Denial' in the Indo-Pacific, the RAN is shifting from traditional crewed survey ships to a future capability reliant on uncrewed systems and AI-driven data analysis. The thesis argues that this technological leap necessitates a profound and disruptive workforce transformation that extends beyond mere retraining.

This transformation involves a fundamental shift in the professional identity of the hydrographic specialist from a traditional mariner to a technologist, which is, a systems operator and data analyst skilled in robotics and AI interpretation. This evolution creates significant challenges in skill acquisition, training, recruitment, and retention. Success is contingent on the RAN's ability to create new career pathways, foster a culture that values technical mastery, develop new operational concepts for Human-Machine Teaming, and align naval doctrine with this new reality. Ultimately, the thesis concludes that successfully navigating this change is a prerequisite for realising the full operational potential of an autonomy-enabled hydrographic capability.



Image: Department of Defence

Introduction

The strategic landscape of the Indo-Pacific region is characterised by increasing complexity and contestation, demanding that the Australian Defence Force (ADF), and specifically the Royal Australian Navy (RAN), leverage technological advancements to maintain a capability edge.¹ The 2023 *Defence Strategic Review* (DSR) and the subsequent 2024 *National Defence Strategy* (NDS) unequivocally mandate the adoption of disruptive technologies, with Robotics, Autonomous Systems, and Artificial Intelligence (RAS-AI)² identified as a critical priority to support a 'Strategy of Denial'.³ Within this broad strategic directive, the modernisation of the RAN's hydrographic capability (i.e. the science of measuring and describing the physical features of oceans, seas, coastal areas, lakes, and rivers⁴), emerges as a foundational enabler for maritime operations and national security. This thesis confronts the pivotal challenge accompanying this technological leap: the profound impact on the RAN's specialist hydrographic workforce.

The core research question guiding this inquiry is: **How would the integration of autonomous systems and artificial intelligence (AI) in the Royal Australian Navy's hydrographic capability impact workforce transformation?** The central argument presented is that the introduction of Autonomous Underwater Vehicles (AUVs), Uncrewed Surface Vessels (USVs), and AI-driven data analytics into the Navy's hydrographic survey missions and data processing—a direction already set by strategic guidance and capability development plans⁵—necessitates a fundamental and potentially disruptive transformation of the RAN's workforce. The RAN's own *RAS-AI Strategy 2040* and its accompanying *RAS-AI Campaign Plan 2025* articulate a vision for harnessing these technologies across the fleet, including for hydrographic and geospatial support functions.⁶ This transformation extends beyond mere technical retraining; it involves a shift in roles, responsibilities, career pathways, and the very

¹ The Indo-Pacific in this context is currently ill-defined but generally understood to span from the west coast of the United States of America (US) to the east coast of Africa.

² The RAN Robotics, Autonomous Systems & Artificial Intelligence (RAS-AI) *Campaign Plan 2025* defines autonomous system as: 'A system that determines how to perform the tasks necessary to achieve a defined goal. Autonomous systems respond to stimuli in a probabilistic manner but can be regulated by deterministic controls so that it can perform their tasks or functions without further human input.'

³ Australian Government, Department of Defence, *Defence Strategic Review* (Canberra: Department of Defence, 2023), 19, 66, see:

<https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>

accessed 8 April 2025; Australian Government, Department of Defence, 2024 *National Defence Strategy* (Canberra: Department of Defence, 2024), 4, 35, see:

<https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program> accessed 8 May 2025.

⁴ What is Hydrography? - Australian Hydrographic Office, accessed April 11, 2025, <https://www.hydro.gov.au/aboutus/what.htm>. For history see: 'Admiralty Manual of Hydrographic Surveying', Vol 1 1965, pgs 1-5.

⁵ See Royal Australian Navy, Robotics, Autonomous Systems & Artificial Intelligence (RAS-AI) *Strategy 2040* (Canberra: Department of Defence, 2020), see:

<https://www.navy.gov.au/sites/default/files/2024-02/RASAI-Strategy-2040.pdf>

accessed 8 April 2025; Royal Australian Navy, *RAS-AI Campaign Plan 2025*

(Canberra: Department of Defence, 2024), see:

<https://www.navy.gov.au/sites/default/files/2024-02/RAS-AI-Campaign-Plan-2025.pdf>

accessed 11 April 2025.

⁶ Royal Australian Navy, *RAS-AI Strategy 2040*; Royal Australian Navy, *RAS-AI Campaign Plan 2025*.

conceptualisation of hydrographic expertise within a naval context. The level of detail required to address and operationalise such matters will not be dealt with in this thesis however, broad principles and themes will.

Hydrography, traditionally a discipline reliant on crewed survey vessels and meticulous manual data collection and processing, provides the essential geospatial intelligence for safe navigation, maritime trade, resource management, disaster relief, and, critically for Defence, the geospatial intelligence enabling naval operations. As the Australian Hydrographic Office (AHO) notes, 'hydrographic information underpins every activity that occurs on, under or over the sea.'⁷ The accuracy and timeliness of hydrographic data are paramount for anti-submarine warfare, amphibious operations, mine countermeasures, and ensuring access for naval forces. However, traditional methods are often resource-intensive, time-consuming, and can expose personnel to risk in contested or hazardous environments.

The allure of autonomous systems⁸ and AI in this domain is compelling; in fact, autonomous hydrographic and mine-counter-measure systems acquisition (Project SEA 1905) was underway until it was cancelled due to competing funding pressures.⁹ AUVs and USVs offer the potential for persistent, wide-area surveillance, rapid data acquisition in denied or dangerous waters, and reduced personnel exposure. AI and machine learning (ML) algorithms promise to accelerate data processing, identify anomalies, and potentially automate aspects of chart production, thereby compressing the 'data acquisition to user' timeline and enhancing decision support.

However, any transition from established, human-centric methodologies to an autonomy-enabled hydrographic capability has its challenges, particularly concerning the workforce. This thesis posits that the successful integration of these advanced technologies is not merely a matter of procurement and technical implementation. Instead, successful integration would hinge on the RAN's ability to effectively manage

⁷ Australian Hydrographic Office, 'Our Role', see:

<https://www.hydro.gov.au/aboutus/what.htm> accessed 30 May 2025; for history see: 'Admiralty Manual of Hydrographic Surveying', Vol 1 1965, pgs 1-5.

⁸ The United States Department of Defense defines autonomy as follows: 'Autonomy is a capability (or a set of capabilities) that enables a particular action of a system to be automatic or, within programmed boundaries, self-governing.' US Department of Defense, 'DoD Directive No. 3000.09: Autonomy in Weapons Systems' (21 November 2012), see:

<https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf> accessed 1 April 2025. The RAN, Remote Autonomous Systems-Artificial Intelligence (RAS-AI) Campaign Plan 2025 defines autonomy as 'the ability of a machine, whether hardware or software, to perform a task without human input.'

⁹ Projects such as SEA 1905 (Maritime Mine Countermeasures and Hydrographic Capability – now discontinued) and SEA 1770 (Rapid Environmental Assessment – which has been serviced) provide tangible evidence of the Navy's trajectory to an autonomy-enabled future, even as the precise path of future autonomous acquisitions evolve. While Phase 1 of SEA 1905 was cancelled in April 2024, the underlying requirement for a modern, deployable mine countermeasures and hydrographic capability, utilising a combination of crewed and uncrewed surface vessels paired with remote and autonomous underwater vehicles, persists. See: 'Australian defence programmes,' Asian Military Review, June 2025, <https://www.asianmilitaryreview.com/2025/06/australian-defence-programmes/> accessed 8 June 2025. This development, while a setback for the original program structure, highlights the dynamic and often complex nature of acquiring cutting-edge, multi-system capabilities, and underscores an enduring commitment to uncrewed systems for these critical maritime tasks.

a complex workforce transformation. It would involve shifting hydrographic personnel from traditional hands-on surveying roles to new functions centred on remote system supervision, mission planning for autonomous assets, advanced data analysis, interpretation of AI-generated outputs, and the maintenance of complex software-intensive systems.

Several corollary questions flow from the central research question. How effectively can the RAN manage the transition from legacy platforms, such as the recently decommissioned *Leeuwin* and *Paluma* class survey vessels,¹⁰ to a more distributed and (in the future) autonomous system-based capability, given current workforce structures, training pipelines, and skill demographics? How does the increasing reliance on industry partnerships, exemplified by the Hydrographic Industry Partnership Program (HIPP), impact the development and retention of sovereign military hydrographic expertise and the overall workforce composition? Furthermore, while this thesis will focus primarily on workforce transformation due to word constraints, it acknowledges the interconnectedness of policy, doctrine, and regulatory frameworks: are these existing structures sufficiently agile and aligned to support this rapid technological shift and the new operational concepts it enables?

Research Method

This thesis employs a qualitative research methodology, utilising a combination of document analysis, and comparative case studies of allied experiences. This approach is well-suited to exploring the complex, multifaceted nature of workforce transformation in a technologically evolving military organisation.

To address gaps in understanding within the existing policy and academic scholarship, this thesis synthesises insights from primary and secondary sources, including strategic policy documents,¹¹ legal sources,¹² technical literature,¹³ academic journals,¹⁴ reports and publications from defence research institutions and think tanks.¹⁵ It will also draw upon publicly accessible statements and information released by Defence and industry stakeholders,¹⁶ including reports from parliamentary committees and the Australian National Audit Office (ANAO) as well as publications from national and international

¹⁰ Jonathan Nally, 'Navy now has only one hydrographic survey ship.' *Spatial Source*, 12 August 2024, see: <https://www.spatialsource.com.au/navy-now-has-only-one-hydrographic-survey-ship/> accessed 1 June 2025; Australian Defence Magazine, 'HMAS *Melville* to be decommissioned,' 22 July 2024, see: [https://www.australiandefence.com.au/news/news/hmas-melville-to-be-decommissioned#:~:text=HMAS%20Melville%20\(A%202426\)%20will.2000%20as%20hydrographic%20survey%20ships](https://www.australiandefence.com.au/news/news/hmas-melville-to-be-decommissioned#:~:text=HMAS%20Melville%20(A%202426)%20will.2000%20as%20hydrographic%20survey%20ships) accessed 1 June 2025.

¹¹ For example, Defence Strategic Review (2023), National Defence Strategy (2024), Integrated Investment Program (IIP), and the 2020 Defence Strategic Update.

¹² For example, the *Navigation Act 2012 (Cth)* and the *Marine Safety (Domestic Commercial Vessel) National Law Act 2012 (Cth)*.

¹³ For example, RAS-AI Strategy 2040, RAS-AI Campaign Plan 2025, and Australian Maritime Doctrine.

¹⁴ Focusing on maritime studies, defence technology, strategic studies, and human resources.

¹⁵ Such as the Australian Strategic Policy Institute (ASPI), the Defence Science and Technology Group (DSTG), and the Trusted Autonomous Systems Defence Cooperative Research Centre (TAS DCRC).

¹⁶ For example, the Hydro International and the Australian Defence Magazine.

hydrographic bodies.¹⁷ These insights are then combined with empirical and theoretical insights derived from the experiences of allied countries and organisational theory to illuminate the path ahead.

With respect to the comparative case study, this is undertaken later in Chapter 4 and will focus on the experiences of key allied navies, specifically the United Kingdom's Royal Navy (RN) and the United States Navy (USN). These two navies were selected because they are significantly investing in autonomous systems for hydrographic and related mine countermeasures (MCM) capabilities. Examining their approaches to workforce adaptation, training reforms, integration challenges, and lessons learned can, therefore, provide valuable insights and potential best practices relevant to the RAN's context.

A few caveats are worth noting here. First, this research relies almost entirely on publicly accessible information. While this presents a limitation in terms of accessing classified or commercially sensitive internal Defence planning documents, the wealth of available public information, including detailed strategic guidance and reports on technological advancements (including in the commercial hydrographic surveying industry), provides a robust foundation for this thesis's inquiry. Second, the rapidly evolving nature of autonomous systems technology and the dynamic strategic environment mean that this analysis will necessarily represent a snapshot in time, current as of October 2025. Engaging in an accurate assessment of the long-term effectiveness of initiatives like HIPP is also constrained by their relative novelty and associated commercial sensitivities. Finally, this thesis's scope is deliberately focused on the RAN's hydrographic capability and its associated workforce transformation. It excludes detailed technical analysis of specific autonomous platforms or the broader complexities of international maritime law governing autonomous vessels, beyond their contextual relevance to workforce roles and training.

Aims and significance

This research aims to provide a holistic analysis of the complex workforce transition needed to coordinate and align people, processes and technology for future strategic readiness. It seeks to move beyond a purely technological or strategic assessment to explore the human dimension of hydrographic modernisation. The significance of this thesis lies in its direct relevance to current Defence priorities and its potential to inform policy and practice within the Royal Australian Navy (RAN). The workforce implications of the Navy's shift from traditional hydrographic platforms to deployable capabilities, managed by small teams known as Deployable Geospatial Support Teams (DGSTs), have been substantial. Utilizing equipment and capabilities acquired through Project SEA 1770 (Rapid Environmental Assessment (REA)), understanding these workforce implications is crucial to avoiding capability gaps and ensuring the full realization of the promised benefits of autonomy. Regarding the acquisition and use of future autonomous capabilities, such as those under potential future projects like the cancelled Project SEA 1905 - Maritime Mine Countermeasures and Hydrographic Capability, understanding the workforce implications will become even more critical to prevent capability gaps and ensure the promised benefits of autonomy are fully realized.

This thesis's originality further lies in its specific focus on the RAN's hydrographic workforce transformation within the broader context of autonomy and AI adoption. While existing the literature (as reviewed in Chapter 1) often addresses the technological aspects of AUVs/USVs or the strategic implications of RAS-AI, a comprehensive

¹⁷ For example, the Australian Hydrographic Office (AHO) reports and International Hydrographic Organization (IHO) standards and publications (e.g., S-100 Universal Hydrographic Data Model).

analysis of the human capital challenges confronting a specialised branch like hydrography in the RAN remains significantly less developed. Practically, the findings of this research aim to be of value to Defence planners, capability managers, human resource specialists, and training authorities involved in shaping the future of the RAN's hydrographic service and, by extension, its overall operational effectiveness.

Thesis Structure

This thesis proceeds in eight chapters, including the Conclusion. Chapter 1 examines the evolving context for the RAN's hydrographic capability, with Chapter 2 then examining the strategic drivers that underlie the need to modernise hydrography. Chapters 3 and 4 provide examinations of the various new technologies relevant to modern hydrography and allied experiences with such technologies. Chapter 5 provides a detailed analysis of the workforce transformation challenges, with Chapter 6 reflecting on what the supporting ecosystem needs to look like, before turning in Chapter 7 to how this workforce transformation should be supported by stronger policy, doctrine and regulatory alignments. Here, achieving productivity gains from the integration of new technologies requires significant adaptation in workforce structures, including how the RAN plans, trains, and develops its people. The Conclusion summarises the key findings of this thesis, reiterating the importance for the RAN to ensure that advances in technology are not viewed as replacements for personnel but as tools to enhance their capabilities and productivity.



Commanding Officer HMAS Benalla salutes the Australian White Ensign as it is lowered for the last time during the ships' decommissioning ceremony held at HMAS Cairns on 16 June 2023.

Images: Department of Defence

Chapter 1: The Evolving Landscape of RAN Hydrographic Capability

This chapter details the historical mandate of the Australian Hydrographic Service (AHS), and its evolution. It also examines traditional platforms and methodologies of collecting hydrographic data,¹⁸ focusing on the recently decommissioned *Leeuwin* and *Paluma* classes.¹⁹ These classes represent the last of ship or platform centric hydrographic capability. A significant portion of this chapter is dedicated to analysing the RAN's strategic decision to transition towards new capabilities, including a brief account of the role and implications of the Hydrographic Industry Partnership Program (HIPP) and the divestment from sovereign survey platforms.

Literature Review

The existing body of literature underscores the transformative potential of autonomous systems and AI in the maritime domain. Studies on AUVs and USVs highlight their increasing sophistication, endurance, and ability to gather high-resolution data in diverse and challenging environments.²⁰ The strategic impetus for adopting such technologies is well-documented, particularly in the context of great power competition and the need for persistent maritime domain awareness.²¹ The RAN's strategic documents, including the DSR, NDS, and RAS-AI Strategy, clearly articulate this imperative.

Existing scholarship also touches upon the challenges of integrating these new technologies. These include technical hurdles, data management complexities, ethical considerations (particularly for AI in decision-making), and the need for new operational concepts.²² However, a specific and in-depth focus on the workforce transformation required within a niche capability like naval hydrography is less prevalent. While some works discuss the general need for upskilling personnel for an AI-enabled future,²³ or

¹⁸ For example, Mohammad Hanif Hamden and Ami Hassan Md Din, 'A review of advancement of hydrographic surveying towards ellipsoidal referenced surveying technique', [IOP Conference Series: Earth and Environmental Science, Volume 169, 9th IGRSM International Conference and Exhibition on Geospatial & Remote Sensing \(IGRSM 2018\) 24–25 April 2018, Kuala Lumpur, Malaysia](https://iopscience.iop.org/article/10.1088/1755-1315/169/1/012019/pdf), see: <https://iopscience.iop.org/article/10.1088/1755-1315/169/1/012019/pdf>, accessed 1 April 2025.

¹⁹ HMAS *Leeuwin* (the last of the survey ships) is anticipated to be decommissioned in 2027.

²⁰ See for example, R. B. Wynn et al., 'Autonomous Underwater Vehicles (AUVs): Their past, present and future contributions to the advancement of marine geoscience,' *Marine Geology* 352 (2014): 451-468, see: <https://core.ac.uk/download/pdf/19963755.pdf> accessed 11 April 2025.

²¹ Australian Government, Department of Defence, 2020 Defence Strategic Update (Canberra: Department of Defence, 2020), which foreshadowed many themes in the DSR, see: <https://www.defence.gov.au/about/strategic-planning/2020-defence-strategic-update> accessed 8 April 2025.

²² Denis Hains. 'The emergence of AI in hydrography', *Hydro International* 25 February 2021, <https://www.hydro-international.com/content/article/the-emergence-of-ai-in-the-hydrography-sector> accessed 1 June 2025.

²³ Andrew Pfau. 'Preparing Sailors for the Age of AI.' US Naval Institute, *Proceedings* 148, no. 4 (April 2022), see: <https://www.usni.org/magazines/proceedings/2022/april/preparing-sailors-age-ai> accessed 1 June 2025.

the challenges of Human-Machine Teaming (HMT),²⁴ the granular detail of how a specific naval specialisation like hydrography must adapt its recruitment, training, career progression, and organisational structure is an area ripe for further investigation. This thesis aims to address this specific lacuna (in publicly available information), focusing on the RAN's unique context, including its reliance on the HIPP and the operational demands of the Indo-Pacific region.

History and evolution

The RAN Hydrographic Service was formally established on 1 October 1920.²⁵ Its origins, however, are intertwined with the British Admiralty Hydrographic Office, which undertook extensive surveys of Australian waters throughout the 19th century to support both colonial defence and burgeoning commercial development.²⁶ While the RAN assumed responsibility for hydrographic surveys in 1920, the formal responsibility for the publication of charts was taken on in 1942. Early survey work, even predating the official formation, was conducted by vessels such as HMAS *Una* in 1915, followed by pioneering efforts by ships like HMS *Fantome* and HMAS *Geranium*.²⁷

The Australian Hydrographic Office (AHO)²⁸ is the nation's primary hydrographic authority, shouldering the immense responsibility of charting an area that covers more than one-eighth of the world's surface.²⁹ This mandate encompasses a critical dual function: supporting civil maritime safety under international conventions such as the Safety of Life at Sea (SOLAS) and national legislation like the *Navigation Act 2012* (Cth), while simultaneously providing essential geospatial intelligence for Australian Defence Force (ADF) operations.³⁰ The AHO's mission explicitly includes enabling safe navigation, supporting Australia's defence and national infrastructure, and fulfilling international obligations for navigational safety and marine environmental protection.³¹

²⁴ Sidharth Kaushal et al., 'Leveraging Human-Machine Teaming: An Offset Strategy Primer and Policy Guide,' Special Competitive Studies Project, January 2024, see: <https://static.rusi.org/human-machine-teaming-sr-jan-2024.pdf> accessed 1 June 2025.

²⁵ Australian Government, Department of Defence, '100 years of hydrography in Defence,' (Canberra: Australian Hydrographic Office, 2020), 1, <https://www.hydro.gov.au/aboutus/AHO2020/100-years-of-hydrography-in-defence.pdf> accessed 5 June 2025; Navy History, 'A Brief History of the Australian Hydrographic Service,' Royal Australian Navy, <https://navyhistory.au/a-brief-history-of-the-australian-hydrographic-service/> accessed 5 June 2025.

²⁶ Australian Hydrographic Office, 'About Us,' Department of Defence, <https://www.hydro.gov.au/aboutus/aboutus.htm> accessed 5 June 2025.

²⁷ Department of Defence, 100 years of hydrography in Defence, 1; Navy History, 'A Brief History.'

²⁸ The AHS is the umbrella term for the AHO (and its staff, both Australian Public Servants and Navy personnel), the RAN's capability platforms (such as the hydrographic ships and deployable teams) and the RAN's hydrographic personnel more generally. Technically, the AHO forms part of the Australian Geospatial Intelligence Agency (AGO) and happens to have Navy personnel 'posted' to positions within the AHO (located in Wollongong). The AGO (primarily at Russell Offices, Canberra) also has Navy personnel posted to maritime geospatial positions located in Canberra.

²⁹ Royal Australian Navy, 'HMAS *Leeuwin* (II),' <https://www.navy.gov.au/capabilities/ships-boats-and-submarines/hmas-leeuwin> accessed 5 June 2025.

³⁰ Australian Hydrographic Office, "About Us."

³¹ Hydrographic Service RAN, Corporate Overview: Hydrographic Service RAN (Paper presented at the Hydrographic Service RAN Industry Briefing, Wollongong, NSW, 1996), pg 2, <https://apps.dtic.mil/sti/tr/pdf/ADA322159.pdf> accessed 5 June 2025.

The strategic importance of this capability was starkly demonstrated during the Second World War. The RAN Hydrographic Branch underwent a significant expansion, playing a vital role in supporting Allied operations in the South West Pacific Area by producing over 1.5 million chart impressions and conducting surveys, often under hazardous conditions.³² This historical precedent underscores hydrography's long-standing criticality to national defence. The enduring dual-purpose nature of Australian hydrography—serving both national civilian requirements for trade, resource management, and safety, and critical military operational needs—highlights its foundational importance.

For decades, the RAN's hydrographic capability was delivered through traditional methodologies, primarily reliant on crewed survey vessels undertaking meticulous, often protracted (many months), data collection and manual processing campaigns. These methods, while foundational, are inherently resource-intensive in terms of personnel, time, and operational costs, and could expose naval personnel to risks, particularly in contested or hazardous maritime environments.

The backbone of the RAN's inshore survey capability for over three decades was the *Paluma*-class Survey Motor Launch. Four of these 36.6-metre catamarans—HMAS *Paluma* (A01), *Mermaid* (A02), *Shepparton* (A03), and *Benalla* (A04)—were commissioned between 1989 and 1990.³³ Designed specifically for hydrographic operations in the shallow waters of northern Australia, including the Great Barrier Reef, their twin hulls offered stability, high manoeuvrability, and a shallow draught of approximately 2.2 to 2.65 metres, which allowed access to reef-strewn and coastal areas. They were equipped with sensors such as the ELAC LAZ 72 side-scan sonar and a Skipper 113 hull-mounted scanning sonar. Beyond routine surveys, these vessels conducted wreck searches, supported the installation and maintenance of shore-based tracking stations, participated in United Nations operations in East Timor, and provided aid to civil communities.³⁴ The progressive decommissioning of the *Paluma* class (HMAS *Paluma* and *Mermaid* in September 2021, followed by HMAS *Shepparton* and *Benalla* in June 2023) marked a significant step in the transition towards new systems, which was (until cancelled) explicitly linked to the introduction of modularized deployable capabilities able to be deployed on future vessels (such as the Offshore Patrol Vessel) under Project SEA 1905-1.³⁵ Due to the cancellation of Project SEA 1905 and the acquisition of advanced autonomous capabilities that project promised, the RAN (and Defence) has effectively delayed its hydrographic (and mine-counter-measures) technological transition to autonomy.

For deeper and more extensive offshore survey tasks, the RAN operated two *Leeuwin*-class Survey Ships (AGS): HMAS *Leeuwin* (A245) and HMAS *Melville* (A246), both commissioned in May 2000.³⁶ These 71.2-metre monohulls were significantly more capable, equipped with multi-beam echo sounders (Atlas Fansweep), single-beam echo sounders (Atlas Hydrographic Deso), a C-Tech CMAS forward-looking sonar, and could

³² Department of Defence, '100 years of hydrography in Defence.'

³³ 'HMAS *Paluma* (IV),' Royal Australian Navy, <https://seapower.navy.gov.au/history/units/hmas-paluma-iv> accessed 6 June 2025.

³⁴ 'HMAS *Paluma* (IV).'

³⁵ Naval Historical Society of Australia, 'HMA Ships *Paluma* and *Mermaid* decommissioned,' Call The Hands: NHSA Newsletter, no. 58 (November 2021): 4, https://nhsa-cth.s3.ap-southeast-2.amazonaws.com/Call+The+Hands_NHSA+Newsletter_Issue+58_Nov+21.docx.pdf accessed 7 June 2025.

³⁶ 'HMAS *Melville* to be decommissioned', Australian Defence Magazine, 22 July 2024, <https://www.australiandefence.com.au/news/news/hmas-melville-to-be-decommissioned>, accessed 7 June 2025.

embark and support an AS350B Squirrel helicopter and three 9-metre survey motor boats.³⁷ Designed to survey a combined 10,000 square nautical miles per annum, their roles extended beyond hydrography to include support for Mine Countermeasures (MCM) operations, maritime surveillance, disaster relief, Search and Rescue (SAR), and emergency medical assistance.³⁸ The strategic pivot towards new capabilities led to the decommissioning of HMAS *Melville* on 8 August 2024, leaving HMAS *Leeuwin* as the RAN's sole remaining dedicated hydrographic survey ship.³⁹ This reduction in organic, crewed survey platforms underscores the commitment to a new operational model.

The divestment from these legacy platforms was driven in part by their inherent limitations in the context of evolving strategic demands and technological possibilities. While highly effective for their era, their operational tempo, reliance on substantial crews,⁴⁰ and the risks associated with deploying crewed platforms in potentially hostile areas became increasingly misaligned with the strategic direction emphasizing speed, persistence, reduced human exposure, and cost-effectiveness (especially when the national charting obligations can be met under the Hydrographic Industry Partnership Program (HIPP) discussed below). The decision to retire these vessels is thus a clear manifestation of a fundamental capability shift, moving away from traditional, human-centric survey methods⁴¹ towards a more distributed, agile team-based capability, autonomous (in the future) and industry-supported hydrographic enterprise.

The following table offers a comparative overview of the key characteristics of these legacy platforms against the attributes of the emerging autonomous systems that are central to the RAN's (future) hydrographic modernisation:

³⁷ Royal Australian Navy, 'HMAS *Leeuwin* (II)'; Director General Maritime Development, Leeuwin Class Hydrographic Ship (AGS) HMAS *Leeuwin* & HMAS *Melville*, Capability Summary (Canberra: Royal Australian Navy, n.d.), 2-3, <https://core.ac.uk/download/268171259.pdf> accessed 7 June 2025.

³⁸ Director General Maritime Development, Leeuwin Class, 1-2.

³⁹ 'HMAS *Melville* to be decommissioned,' Australian Defence Magazine; 'OPINION | Understanding the cost of Australia's naval defence,' Baird Maritime, May 30, 2025, <https://www.bairdmaritime.com/security/naval/opinion-understanding-the-cost-of-australias-naval-defence> accessed 7 June 2025.

⁴⁰ Ship's complements of 13-16 for the Paluma Class and 47-57 for the Leeuwin Class.

⁴¹ Foundationally, in order to gather survey data so that maritime charts may be compiled, surveyors had to a. measure the depth of the water (eg. by measuring the length of a lead weighted rope which was lowered over the side of a ship/boat), b. connect that 'depth' to a position (before modern positioning systems were in use, close to shore surveys required accurate and well-practised triangulation methods to 'fix' a position), and c. take into account the 'tidal' height (which required separate tidal reading teams measuring the effects of tides in the survey area). These factors were 'linked' together using time. In practice, the sailor who was lowering the lead weighted rope over the side would call 'fix' when they felt the weight hit the seabed, another would record the position (by triangulation or some other positioning method), while another would record the exact time (so that the relevant tidal height (obtained from the tidal team who might be ashore) can be applied at the (later) processing stage. Echo sounders and Global Positioning System (GPS) (and equivalent technologies) have made the 'gathering of data' more effective and efficient over the years, however, autonomy promises to remove people further from the data gathering phase.

Table 1: Key Characteristics of Legacy vs. Emerging RAN Hydrographic Capabilities⁴²

Characteristic	Legacy Systems (e.g., <i>Leeuwin/Paluma</i> -class)	Emerging Systems (e.g., AUVs/USVs)
Primary Staffing	Crewed (significant complement)	Present: Multiple small deployable teams (i.e., DGSTs) Future: Small deployable teams operating multiple uncrewed or minimally crewed/remotely operated capabilities ⁴³
Typical Endurance/Persistence	Days to weeks (limited by crew fatigue, fuel, stores)	Teams remain limited by fatigue, stores, however, systems may autonomous systems may operate for days, weeks, or months (limited by power, system reliability) ⁴⁴
Data Acquisition Rate/Area Coverage Speed	Moderate; sequential survey lines by parent vessel or Survey Motor Boats (SMBs)	Potentially higher in the future due to multiple autonomous assets operating concurrently; persistent operations
Suitability for Contested/Denied Environments	Higher risk to personnel and capital-intensive platforms	Potentially lower risk to personnel; smaller, potentially more expendable or stealthier platforms; rapid deployment capability
Primary Data Collection Method	Hull-mounted or towed sonars on crewed vessels/boats	In the future , offboard autonomous sensors on AUVs/USVs; remote sensing
Reliance on Sovereign Platform vs. Industry	Primarily sovereign platforms for all survey tasks (i.e., both national and military 'survey' tasks)	Increased reliance on industry partnerships (HIPP) for national survey tasks; sovereign focus on military Geospatial Intelligence (GEOINT)

A significant element in the evolving landscape of Australian hydrography is the Hydrographic Industry Partnership Program (HIPP). Prior to the introduction of the

⁴² Data derived from Department of Defence, '100 years of hydrography in Defence'.

⁴³ The 'minimal staffing' assumption will be tested in this paper.

⁴⁴ It must be acknowledged that an AUV/USV still requires a 'place' or ship to deploy from. Traditional platforms brought all required support and infrastructure.

HIPP, the greatest changes to the conduct of hydrographic surveying were in tactical efficiencies flowing from technological change, such as the introduction of the Global Positioning System (GPS), which enabled the rapid and accurate positioning of hydrospatial data. The HIPP program however, represents a strategic shift in how Australia meets its national hydrographic survey obligations,⁴⁵ moving towards a model of increased collaboration with commercial industry (whatever the technologies in use). HIPP is a commercial initiative through which the Department of Defence partners with specialist hydrographic survey companies to 'undertake focused survey activities that contribute to national charting priorities.'⁴⁶ The stated vision for HIPP is to establish 'an efficient, effective and sustainable hydrographic survey, oceanographic and marine geophysical data collection program through a partnership with Industry to deliver a true nation-building effort.'⁴⁷ Compared to the divested/divesting RAN ship based surveying capability, industry partners are generally able to achieve three times the rate of effort (i.e., three times the amount surveyed). This is largely due to the high degree of specialization in task (i.e., surveying is not diluted by non-surveying military activities and taskings) and the ability of industry to utilize the most cost effective and efficient technologies available and suitable for a given tasking. A key objective is to achieve full, high-quality bathymetric coverage of Australia's Exclusive Economic Zone (EEZ) by 2050.⁴⁸ Industry is also well placed to test and evaluate commercial off the shelf autonomous systems and machine learning software and associated systems in a very agile way.

The program was initiated with a \$150 million government investment over five years from 2020, and the 2024 Integrated Investment Plan indicates a further commitment of approximately \$1 billion over the decade from 2024 for HIPP to continue collecting data for nautical charts and publications.⁴⁹

The AHO (as part of the Australian Geospatial Intelligence Organisation (AGO)) manages HIPP on behalf of the Department of Defence, with stakeholder agreement on survey priorities and areas facilitated through the Hydrographic Review Board, which includes representatives from the AHO, the Australian Maritime Safety Authority (AMSA), the Australian Antarctic Division, and Geoscience Australia.⁵⁰ The

⁴⁵ Australian Hydrographic Office, 'Roles and Responsibilities,' Department of Defence, see: <https://www.hydro.gov.au/aboutus/roles.htm#:~:text=The%20AHO%20is%20responsib,le%20for,collating%20and%20managing%20hydrographic%20data> accessed 8 June 2025; Australian Government, Federal Register of Legislation, 'Navigation Act 2012 (Cth)' section 223, 'Functions of the Australian Hydrographic Office,' see: https://www.legislation.gov.au/C2012A00128/2025-02-15/2025-02-15/text/original/epub/OEBPS/document_1/document_1.html#_Toc190871103 accessed 8 June 2025.

⁴⁶ Australian Hydrographic Office, 'HydroScheme Industry Partnership Program,' Department of Defence, <https://www.hydro.gov.au/NHP/hipp.htm> accessed 8 June 2025.

⁴⁷ Australian Hydrographic Office, 'HydroScheme Industry Partnership Program.'

⁴⁸ Australian Hydrographic Office, 'HydroScheme Industry Partnership Program.'

⁴⁹ 'HMAS *Melville* to be decommissioned,' Australian Defence Magazine; Department of Defence, 'Hydroscheme industry partnership program commences,' media release, 26 February 2020, <https://www.defence.gov.au/news-events/releases/2020-02-26/hydroscheme-industry-partnership-program-commences> accessed 8 June 2025; Australian Hydrographic Office, 'HydroScheme 2025,' ArcGIS StoryMaps, <https://storymaps.arcgis.com/stories/4eebeb4ac3a34f47a7699e63f006ca28> accessed 8 June 2025.

⁵⁰ Australian Hydrographic Office, 'Governance,' Department of Defence, <https://www.hydro.gov.au/aboutus/governance.htm> accessed 5 June 2025; Australian

implementation of HIPP, which has been in full operation for over five years, has had profound implications for the RAN's hydrographic capability and its workforce. By transitioning a significant portion of the national surveying responsibility to industry partners, the Navy's organic survey capability has been redeveloped and refocused on specialised military environmental information collection and the provision of military-specific geospatial intelligence (GEOINT).⁵¹

The shift of national charting data collection to HIPP aligns directly with the DSR recommendation and the NDS directive for a more 'focused force.' However, this shift also raises important questions concerning the long-term development and retention of sovereign military hydrographic expertise and the overall composition of the naval hydrographic workforce. While a detailed analysis of HIPP's efficacy is beyond the scope of this chapter, the findings of the Australian National Audit Office (ANAO) regarding broader challenges within Defence in maximising Australian Industry Participation and ensuring effective contract management provide a critical contextual consideration for the program's long-term impact on sovereign capability.⁵² HIPP, therefore, is not merely an outsourcing mechanism but a fundamental restructuring of Australia's hydrographic enterprise, a choice that aims to leverage commercial capacity for broad area surveying, thereby theoretically freeing scarce Defence resources for uniquely military hydrographic tasks, often involving advanced autonomous technologies. However, based on publicly available information, it is not clear that any increased efficiencies garnered by HIPP contracted solutions has resulted in increased charting. It is understood that the AHO did not ask for or receive an increased budget or workforce to process and quality assure the increase in data collected—perhaps increased use of AI in processing and assurance will alleviate this issue in time.

Project SEA 1770 (a Department of Defence acquisition program), focused on Rapid Environmental Assessment (REA), has delivered a suite of deployable systems designed to enhance the ADF's ability to rapidly collect, process, and disseminate tactical maritime environmental information.⁵³ The capability acquired for hydrography was survey equipment useable by (small) deployable survey teams. This capability is crucial for supporting amphibious operations, disaster relief, and ensuring safe access for naval forces in unfamiliar or dynamic littoral environments. Key deliverables under SEA 1770 included the 9.5-metre Survey Craft System (SCS), which was aimed at gathering high-quality survey data and was anticipated to be deployable from shore and

Hydrographic Office, National Report Australia to the 21st Meeting of the SWPHC (Wollongong, NSW: AHO, 2023), 2 (referring to the Hydrographic Review Board composition in previous reports, e.g. SWPHC21-08B).

⁵¹ Naval Historical Society of Australia, 'HMA Ships *Paluma* and *Mermaid* decommissioned,' Department of Defence, 'Hydroscheme industry partnership program commences.'

⁵² Australian National Audit Office, Maximising Australian Industry Participation Through Defence Contracting, Audit Report No. 25 2024–25 (Canberra: ANAO, 2025), see: <https://www.anao.gov.au/work/performance-audit/maximising-australian-industry-participation-through-defence-contracting> accessed 8 June 2025; Max Blenkin, 'ANAO reports on AIP,' Australian Defence Magazine, May 23, 2025, <https://www.australiandefence.com.au/news/news/anao-reports-on-aip> accessed 8 June 2025.

⁵³ Leidos Australia, 'Leidos Australia To Deliver Key Milestone For SEA1770,' PR Newswire, 8 October 2019, <https://enmobile.prnasia.com/releases/global/leidos-australia-to-deliver-key-milestone-for-sea1770-259877.shtml> accessed 8 June 2025; "Leidos Australia to Deliver Survey Craft for SEA1770," Offshore Energy, 8 October 2019, <https://www.offshore-energy.biz/leidos-australia-to-deliver-survey-craft-for-sea1770/> accessed 8 June 2025.

larger vessels, and also transported by road and air.⁵⁴ Complementing the SCS are the Fly Away Survey Kits (FASKs), designed for rapid deployment on vessels of opportunity, and Remus 100S Autonomous Underwater Vehicles (AUVs).⁵⁵ These systems collectively provide a flexible and rapidly deployable REA capability, enabling hydrographic and oceanographic data collection in a manner significantly different from traditional platform-centric approaches. The principle difference is that the operators do not need the same level of training and experience on the operation of the traditional platforms—consequently, the operators are more focused and specialised.

The evolving landscape of RAN hydrography, shaped by a rich history of service, the inherent limitations of now-retiring legacy platforms, overriding strategic imperatives as articulated in the DSR and NDS (discussed in greater detail in the next chapter), new models of industry partnership like HIPP, and the active procurement of advanced autonomous technologies through projects such as SEA 1770 and the possible future ambitions of a project similar to the cancelled project SEA 1905, exerts undeniable pressure for profound workforce transformation. This chapter has sought to establish the historical context and the primary drivers—the 'why' and 'what'—of this change. The strategic imperative for hydrographic modernization is dealt with in Chapter 2.

⁵⁴ Leidos Australia, 'Leidos Australia to Deliver Key Milestone for SEA1770'; Leidos, Rapid Environmental Assessment (Factsheet, Leidos Australia, September 2019), 1, <https://www.leidos.com/sites/leidos/files/2019-09/FS-Rapid-Environmental-Survey.pdf> accessed 8 June 2025.

⁵⁵ Leidos, Rapid Environmental Assessment, 1; 'Navy celebrates launch of next-gen survey boat capability,' Defence Connect, 9 November 2020, <https://www.defenceconnect.com.au/naval/7148-navy-celebrates-launch-of-next-gen-survey-boat-capability> accessed 8 June 2025.

Chapter 2: The Strategic Dimensions Impacting Hydrography in the Indo-Pacific

This chapter connects the drive for autonomous hydrography to Australia's strategic imperatives in the Indo-Pacific, as outlined in the DSR and NDS – and as also reflected in the country's strategy of denial. This concise discussion is necessary for better contextualization of the operational advantages (e.g., enhanced reach, persistence, reduced risk) and challenges (e.g., data security, system reliability, command and control (C2)) associated with employing autonomous systems in hydrographic surveys within the complex Indo-Pacific environment, as well as the implications for interoperability with allies under frameworks like AUKUS.

Any modernisation of the Royal Australian Navy's (RAN) hydrographic capability is not a technical exercise undertaken in isolation. Rather, it is a direct and necessary response to a fundamental reshaping of Australia's strategic environment. The 2023 Defence Strategic Review (DSR) and the subsequent 2024 National Defence Strategy (NDS) unequivocally state that Australia faces its most complex and challenging security landscape since the Second World War.⁵⁶ This assessment, driven by the erosion of the ten-year strategic warning time for major conflict and the scale of military expansion in the Indo-Pacific, has compelled a radical departure from previous defence postures.⁵⁷ The DSR judges the Australian Defence Force (ADF) as no longer 'fit for purpose' and mandates a transition from a 'balanced force', designed for a range of contingencies, to a 'focused force' optimised for deterrence in the maritime domain.⁵⁸

At the heart of this transformation is the adoption of a 'strategy of denial' as the new cornerstone of Defence planning.⁵⁹ This represents a profound philosophical shift. Where previous doctrine gave equal weight to shaping the strategic environment, deterring aggression, and responding with force, the NDS explicitly elevates deterrence to the primary strategic objective.⁶⁰ As Harshita Dey's observes, the strategy aims to deter conflict before it begins by denying a potential adversary any confidence that it could succeed in projecting force against Australia or its interests.⁶¹ In the maritime domain, this translates into an imperative to hold an adversary's assets at risk at the greatest possible distance, particularly within Australia's northern approaches and

⁵⁶ *Defence Strategic Review 2023*, pg 19; *2024 National Defence Strategy*, pg 4.

⁵⁷ *Defence Strategic Review 2023*, pg 24.

⁵⁸ International Institute for Strategic Studies, 'Australia's 2023 Defence Strategic Review,' *Strategic Comments* 29, no. 12 (2023), <https://www.iiss.org/publications/strategic-comments/2023/australias-2023-defence-strategic-review/> accessed 20 July 2025; *Defence Strategic Review 2023*, pg 53.

⁵⁹ *2024 National Defence Strategy* and *2024 Integrated Investment Program*.

⁶⁰ Greg Moriarty, 'National Defence Strategy' (speech, Air and Space Power Conference, Canberra, May 2024), <https://airpower.airforce.gov.au/sites/default/files/2024-05/Air%20and%20Space%20Power%20Conference%202024%20Transcript%20Mr%20Greg%20Moriarty%20National%20Defence%20Strategy.pdf> accessed 20 July 2025; *2024–28 Defence Corporate Plan* (Canberra: Commonwealth of Australia, 2024), pg 5, <https://previewapi.transparency.gov.au/delivery/assets/80a82ed1-3e33-027b-b7e0-6493f97f18f8/84004b0f-9f70-4bf9-a2d9-3b1e7229b630/2024-25%20Department%20of%20Defence%20Corporate%20Plan.pdf> accessed 20 July 2025.

⁶¹ Harshita Dey, 'Analysis of Australia's National Defence Strategy 2024,' National Maritime Foundation, 20 May 2024, https://maritimeindia.org/wp-content/uploads/2024/05/Harshita-Dey_Analysis-of-Australias-National-Defence-Strategy-2024-pdf.pdf accessed 20 July 2025.

across its critical sea lines of communication.⁶² The ability to achieve this effect is fundamentally dependent on superior knowledge of the operating environment. Effective anti-submarine and anti-surface warfare—the very means of enacting military denial at sea—are impossible without the detailed, timely, and accurate geospatial intelligence that military hydrography provides.

This strategic imperative is amplified by the character of modern maritime competition, which is increasingly conducted in the 'grey-zone'—the contested space between peace and war.⁶³ Grey-zone operations employ coercive statecraft, such as the use of maritime militias and coast guard vessels (by China), to assert control and achieve strategic gains through ambiguity and incrementalism, deliberately remaining below the threshold that would provoke an overt military response.⁶⁴ Deploying high-value, crewed naval platforms like frigates into such scenarios to counter harassment creates a disproportionate risk of miscalculation and unwanted escalation, however, may still be required in activities such as freedom of navigation operations as conducted by the US.⁶⁵ To gain the necessary geospatial intelligence, including hydrographic data, the operational advantages of uncrewed systems—persistence, scalability, and the removal of personnel from harm's way—therefore offer a compelling intelligence gathering solution.⁶⁶ AUVs and USVs can conduct the persistent surveillance and hydrographic data collection necessary to maintain domain awareness and (perhaps) assert presence without the same escalatory risk, shifting the burden of escalation back to the aggressor. Even in areas such as the high seas where the risks of contestation are low, the persistence and scalability of uncrewed systems are in themselves compelling.

However, the operationalisation of a denial strategy is not a unilateral endeavour; it is inherently a strategy of collective deterrence reliant on deep integration with allies. The AUKUS security partnership is the critical framework for this integration, with its Pillar 2

⁶² Andrew Dowse, 'Australia's Defense Strategy,' *Journal of Indo-Pacific Affairs*, 10 September 2024, https://media.defense.gov/2024/Sep/10/2003540653/-1/1/JIPA%20-%20SENIOR_LEADER_PERSPECTIVE_DOWSE.PDF accessed 20 July 2025.

⁶³ Anthony Robertson, 'What is grey-zone confrontation and why is it important?,' The Cove, 18 July 2022, <https://cove.army.gov.au/article/what-grey-zone-confrontation-and-why-it-important> accessed 20 July 2025; United States of America National Intelligence Council, 'Updated IC Gray Zone Lexicon: Key Terms and Definitions', July 2024, Appendix D, pg 11, <https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf> accessed 24 July 2025.

⁶⁴ Isaac B. Kardon, 'Combating the Gray Zone: Examining Chinese Threats to the Maritime Domain,' Carnegie Endowment for International Peace, 4 June 2024, <https://carnegieendowment.org/posts/2024/06/combating-the-gray-zone-examining-chinese-threats-to-the-maritime-domain?lang=en> accessed 24 July 2025.

⁶⁵ Michael Green et al., *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (Washington, DC: Center for Strategic and International Studies, 2017), as cited in Abhijit Singh, 'Deciphering Grey-Zone Operations in Maritime-Asia,' Observer Research Foundation, August 2018, <https://www.orfonline.org/public/uploads/posts/pdf/20230523093408.pdf> accessed 24 July 2025; United States of America, Indo-Pacific Command, 'Freedom of Navigation Operations (FONOPS) – Peaceful Principled Upholding of Int'l Law (Countering PRC Flawed Narratives)', J06/SJA TACAID Series, <https://www.pacom.mil/Portals/55/Documents/pdf/J06%20TACAID%20-%20FONOPS.pdf?ver=pH6FtE-cpgyhqfBJi2vEKg%3D%3D> accessed 24 July 2025.

⁶⁶ Sea Machines Robotics (BLOG), 'Guide to Autonomous Vessels for Hydrographic Survey in 2024,' 26 June 2024, <https://sea-machines.com/guide-to-autonomous-vessels-for-hydrographic-survey-in-2024/> accessed 24 July 2025.

workstream focused on accelerating the joint development of advanced capabilities in areas central to maritime denial: undersea systems, AI, and autonomy.⁶⁷ Initiatives like the AUKUS Undersea Robotics Autonomous Systems (AURAS) project and joint exercises focused on protecting critical undersea infrastructure are tangible evidence of this collaborative approach.⁶⁸ Yet this reliance introduces a new strategic vulnerability: capability dependency. The successful execution of Australia's national strategy is now contingent on overcoming long-standing legislative and bureaucratic barriers to technology sharing, most notably the United States' International Traffic in Arms Regulations (ITAR).⁶⁹ While reforms are underway, delays in delivering interoperable, AUKUS-enabled capabilities could create a dangerous capability gap, particularly as legacy platforms are divested (such as the hydrographic ships) in anticipation of their autonomous replacements.⁷⁰ For the RAN's hydrographic service, this means the transition to an autonomous future is not only a technological and workforce challenge but also a strategic gamble on the timely success of the AUKUS enterprise.

⁶⁷ House of Commons Library, *AUKUS pillar 2: Advanced capabilities*, Research Briefing CBP-9842 (London: UK Parliament, 2 September 2024), <https://commonslibrary.parliament.uk/research-briefings/cbp-9842/> accessed 24 July 2025.

⁶⁸ Department of Defence, 'Working to protect undersea infrastructure,' media release, 14 February 2025, <https://www.defence.gov.au/news-events/news/2025-02-14/working-protect-undersea-infrastructure> accessed 24 July 2025.

⁶⁹ Peter Tesch, 'AUKUS: Two pillars, three fallacies,' *The Interpreter*, Lowy Institute, 2 October 2024, <https://www.loyyinstitute.org/the-interpreter/aukus-two-pillars-three-fallacies> accessed 24 July 2025.

⁷⁰ Marc Ablong, 'OPINION | Understanding the cost of Australia's naval defence,' *Baird Maritime*, 30 May 2025, <https://www.bairdmaritime.com/security/naval/opinion-understanding-the-cost-of-australias-naval-defence> accessed 24 July 2025.

This page is intentionally blank

Chapter 3: Autonomous Technologies and AI in Modern Hydrography

This chapter provides an overview of the key technologies transforming hydrography. It also reviews the capabilities, limitations, and operational considerations of AUVs and USVs relevant to naval hydrographic tasks. In so doing, the application of AI and machine learning (ML) to hydrographic data processing, analysis, and product generation is explored, including the significance of the International Hydrographic Organisation (IHO) S-100 data standard.

AUVs and USVs are the primary platforms driving the transition from traditional, crewed survey platforms to a distributed and agile hydrographic capability. It is predicated on the maturation of two key technological streams: autonomous maritime systems for data acquisition and artificial intelligence for data processing and analysis. Their principal advantages are persistence and endurance; freed from the constraints of crew fatigue, they can operate for extended periods, from days to months, collecting vast datasets over wide areas. This makes them ideal for tasks such as seafloor mapping, environmental monitoring, and infrastructure inspection.⁷¹ Critically, they can be deployed into hazardous or contested environments—such as under polar ice or within denied littoral zones—without placing personnel at risk, a key consideration for military operations.⁷² Equipped with a suite of high-resolution sensors like multibeam echosounders and side-scan sonars, these platforms can acquire hydrographic data of a quality and density that often surpasses that of surface vessels, particularly in deep water.⁷³

However, their operational utility is constrained by significant limitations inherent to the maritime environment. Finite power endurance remains a primary challenge, with battery life dictating mission duration. Furthermore, the physics of the underwater domain severely restricts communication: radio waves do not penetrate water effectively, forcing AUVs to rely on low-bandwidth, high-latency acoustic communication or to surface to establish satellite links, complicating real-time command and control.⁷⁴ Consequently, navigation in GPS-denied underwater environments depends on dead reckoning, aided by systems like Inertial Navigation Systems (INS) and Doppler Velocity Logs (DVL), which accumulate positional errors over time.⁷⁵ Further, satellite based sensor systems, and laser airborne depth sounding systems⁷⁶ have limitations due to

⁷¹ Sea Machines Robotics (BLOG), 'Guide to Autonomous Vessels for Hydrographic Survey in 2024,' 26 June 2024; NOAA Ocean Exploration, 'Uncrewed Surface Vessels, <https://oceanexplorer.noaa.gov/technology/usv/usv.html> accessed 30 June 2025.

⁷² Wynn et al., 'Autonomous Underwater Vehicles (AUVs): Their past, present and future contributions to the advancement of marine geoscience,' *Marine Geology* 352 (2014): 451-468.

⁷³ Wynn et al., 'Autonomous Underwater Vehicles (AUVs)'.

⁷⁴ 'Challenges of Autonomous Underwater Vehicles in Military Hydrography,' DTIC, (<https://apps.dtic.mil/sti/citations/AD1004191>) accessed 30 July 2025; Spaulding, *Autonomous Underwater Vehicles*.

⁷⁵ Susan Sebastian et al, 'AUVs in Hydrography: Integrating Autonomous Underwater Vehicle Capability into Hydrographic Operations' *Hydro International*, 26 July 2016, <https://www.hydro-international.com/content/article/auvs-in-hydrography> accessed 31 July 2025.

⁷⁶ Department of Defence, Defence Science and Technology Group, 'Laser Airborne Depth Sounder (LADS), <https://www.dst.defence.gov.au/innovation/laser-airborne-depth-sounder-lads> accessed 30 July 2025.

the depth of penetration resulting from the 'hard' physics which rapidly attenuate electromagnetic waves when penetrating water.

The proliferation of autonomous survey platforms creates a secondary challenge: a data deluge. It may be relatively easy for a small team to deploy many autonomous platforms, which exponentially increases the data collected with the concurrent need for storage, analysis and quality control. A single autonomous system can generate terabytes of raw sonar data in one mission, creating a volume of information that is difficult to process and analyse efficiently through manual, human-centric methods. This is where AI and ML become critical enablers.⁷⁷ AI-powered algorithms are being developed to automate many of the most time-consuming aspects of the hydrographic workflow. This includes data cleaning—using ML models to automatically detect and remove 'noise' and anomalies from bathymetric datasets—and feature extraction, where algorithms can be trained to identify and classify specific seabed features, such as rock, sand, vegetation, or man-made objects like shipwrecks and pipelines.⁷⁸ The application of these 'GeoAI'⁷⁹ techniques promises to dramatically compress the timeline from data acquisition to the generation of actionable intelligence, a key requirement for military hydrography.⁸⁰

However, this reliance on AI introduces new vulnerabilities, most notably the risk of 'data poisoning', where an adversary could deliberately corrupt the training data used to build an ML model, causing it to misclassify features or fail at critical moments.⁸¹ This, along with broader ethical considerations,⁸² underscores the imperative of maintaining 'meaningful human control' over autonomous systems and subsequent processing of data: that is, ensuring that human judgement remains central to the decision as to where an AUV may be deployed and able to rely on the data collected. It warrants note that such considerations are different from those raised in relation to autonomous systems that can exert lethal force (e.g. a lethal autonomous weapon system (LAWS)): for such weapons systems, one might ethically expect greater human involvement in decision-

⁷⁷ For definition of ML, see: Lena Trabucco, 'AI-Enabled Autonomous Weapons and Human Control, Part 1: Human Control and Machine Learning Design and Development,' *International Law Studies*, The United States Naval War College, Vol 106, 534, 2025, 563-565, see: <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3115&context=ils> accessed 21 September 2025.

⁷⁸ Teledyne CARIS, 'The data processing challenge,' IHO, (https://iho.int/uploads/user/Inter-Regional%20Coordination/RHC/SEPRHC/SEPRHC13/CHRPSE13-2.5.2-CARIS_Onboard.pdf) accessed 31 July 2025.

⁷⁹ Geospatial AI.

⁸⁰ Editorial Team, 'New AI tool to streamline bathymetric data cleansing process,' Safety4Sea, 14 October 2021, <https://safety4sea.com/new-ai-tool-to-streamline-bathymetric-data-cleansing-process/> accessed 31 July 2025.

⁸¹ M. Woodlief, 'Unlock insights from hydrographic data with GeoAI,' *The International Hydrographic Review* 30, no. 1 (2025) <https://journals.lib.unb.ca/index.php/ihr/article/view/34742/1882530413> accessed 31 July 2025; Coda Octopus, "Seabed Classification," <https://www.codaoctopus.com/other-products/geo/seabed-classification> accessed 31 July 2025.

⁸² Although this paper is in relation to autonomy in weapon systems *per se*, the ethical considerations are relevant to the collection of certain types of GEOINT collected as that data may be used to inform 'targeting decisions'. Anna-Katharina Ferl, "Imagining Meaningful Human Control: Autonomous Weapons and the (De-) Legitimation of Future Warfare," 9 July 2023, *Global Society* 38 (1): 139–55. See: <https://www.tandfonline.com/doi/full/10.1080/13600826.2023.2233004#coi-statement>, accessed 5 October 2025.

making before and during deployment.⁸³ Further discussion of LAWS is beyond the scope of this thesis, even though it is not inconceivable that future autonomous hydrographic data collection platforms may also have lethal capabilities.

Underpinning this entire technological ecosystem is the International Hydrographic Organisation's (IHO) S-100 Universal Hydrographic Data Model.⁸⁴ S-100 is a framework designed to replace the legacy S-57 standard, which was too rigid to support the dynamic, data-rich environment of modern navigation.⁸⁵ S-100 is not a single product but a framework that allows for multiple, interoperable data layers to be used simultaneously. This enables a user to overlay a base S-101 Electronic Navigational Chart (ENC) with dynamic, near-real-time information such as S-102 high-resolution bathymetry, S-104 water levels, and S-111 surface currents, all within a single system.⁸⁶ Crucially, the S-100 framework is designed to be machine-readable and plug-and-play, making it the foundational digital architecture for the future of navigation. Its ability to standardise and integrate diverse hydrographic and oceanographic data streams is a fundamental enabler for both autonomous maritime systems and the AI-driven applications that process their data, effectively heralding a future of smarter and safer seas.⁸⁷ A warfighter with such data, and the ability to use such data will be at a tactical

⁸³ For an Australian Government position on LAWS see: Australian Government, 'Australia's Submission to the United Nations Secretary-General's Report on Lethal Autonomous Weapons Systems,' Department of Foreign Affairs and Trade, May 2024, [https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_\(2024\)/78-241-Australia-EN.pdf](https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_(2024)/78-241-Australia-EN.pdf) accessed 31 July 2025; Lena Trabucco, 'What is Meaningful Human Control? Cracking the Code on Autonomous Weapons and Human Judgment,' Modern War Institute at West Point, 21 September 2023, <https://mwi.westpoint.edu/what-is-meaningful-human-control-anyway-cracking-the-code-on-autonomous-weapons-and-human-judgment/> accessed 31 July 2025.

⁸⁴ The IHO standards dictate the acceptable levels of error and the methodologies for data collection and processing. See, International Hydrographic Organisation (IHO) Standards for Hydrographic Surveys, S-44 Edition 6-1.0, 2020, https://iho.int/uploads/user/pubs/standards/s-44/S-44_Edition_6.1.0.pdf, accessed 1 April 2025.

⁸⁵ SevenCs, 'S-100 Universal Hydrographic Data Model,' <https://www.sevencs.com/enc-production-tools/s-100-data-model/> accessed 31 July 2025; Seojeong Lee and Hyoseung Kim, 'IHO S-100 Data Model and Relevant Product Specification,' *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 18, no. 2 (June 2024): 297-301, https://www.researchgate.net/publication/377056086_IHO_S-100_Data_Model_and_Relevant_Product_Specification accessed 31 July 2025..

⁸⁶ IHO, 'Major Milestone Achieved in Transition to Smart Navigation with Operational Editions of S-100 Standards,' 13 January 2025, <https://iho.int/en/major-milestone-achieved-in-transition-to-smart-navigation-with-operational-editions-of-s-100-standards> accessed 31 July 2025; United States' Department of Commerce, National Oceanic and Atmospheric Administration (NOAA), 'The Universal Hydrographic Data Model: What is S-100?', <https://marinenavigation.noaa.gov/s100.html> accessed 31 July 2025.

⁸⁷ Martyn Wingrove, 'New IHO S-100 standards will stimulate new applications,' *Riviera Maritime Media*, 3 June 2022, <https://www.rivieramm.com/news-content-hub/news-content-hub/new-iho-s-100-standards-will-stimulate-new-applications-71303> accessed 31 July 2025; United Kingdom, Admiralty, 'How S-100 will shape the future of navigation,' <https://www.admiralty.co.uk/s-100-shaping-future-navigation> accessed 31 July 2025.

advantage compared to those without. Data that is analysed becomes 'intelligence',⁸⁸ intelligence which is relevant and can be readily used by warfighters creates a tactical, and in some cases, strategic advantage.

⁸⁸ 'The Role of Intelligence,' Office of National Intelligence, see:
<https://www.oni.gov.au/news/role-intelligence> accessed 5 October 2025.

Chapter 4: Integrating Autonomy: A Comparative Analysis of RAN and Allied Experiences

The strategic and technological imperatives set out in the preceding chapters are driving a fundamental shift in how navies conduct hydrographic (and mine countermeasures (MCM)) operations. Accordingly, this transition from crewed platforms to autonomous systems is not unique to the RAN but is now a common challenge faced by its closest allies. This chapter examines the RA's nascent efforts to integrate autonomy, focusing on its key operational units and acquisition projects (e.g., the Deployable Geospatial Support Teams (DGSTs) initiative) and relevant acquisition projects (e.g., SEA 1770)). It then provides a comparative analysis of the approaches being taken by the RN and the USN, drawing out pertinent lessons that can inform the RAN's own workforce transformation.

The RAN's practical integration of autonomous systems is spearheaded by its DGSTs. These small, agile teams are designed for rapid deployment into operational areas to conduct a 'rapid environmental assessment' (REA)⁸⁹, a capability crucial for amphibious operations and disaster relief.⁹⁰ During humanitarian assistance operations in Tonga and multinational exercises like RIMPAC, DGSTs have demonstrated their ability to use portable systems, such as inflatable boats equipped with multi-beam echo sounders, to survey beach approaches and landing zones, ensuring safe access for larger assets.⁹¹



Royal Australian Navy sailors prepare their geospatial survey equipment during Operation Tonga Assist 2022.⁹²



A Royal Australian Navy deployable geospatial survey team assess a reef during Operation Tonga Assist 2022.⁹³

Images: Department of Defence

⁸⁹ This assessment provides a risk profile of the environment in relation to probable operational needs.

⁹⁰ The author was the Officer in Charge of the DGST deployed on Operation Sumatra Assist (embarked HMAS *Kanimbla*) to conduct REA in preparation for beach landings at Banda Aceh after the devastating 2004 Tsunami.

⁹¹ Department of Defence, 'Navy team surveys Tonga below the waterline,' media release, 18 February 2022, <https://www.defence.gov.au/news-events/news/2022-02-18/navy-team-surveys-tonga-below-waterline>; Lily Lancaster, 'Royal Australian Navy Joins Its Army's Landing Force,' DVIDS, 15 July 2022, <https://www.dvidshub.net/news/425457/royal-australian-navy-joins-its-armys-landing-force>.

⁹² Department of Defence, Image Gallery, http://images.defence.gov.au/20220215adf8604025_0056.jpg accessed 4 August 2025.

⁹³ Department of Defence, Image Gallery, http://images.defence.gov.au/20220215adf8604025_0082.jpg accessed 4 August 2025.

It warrants note that this operational concept was formalised and equipped through acquisition programs like SEA 1770, which delivered a suite of REA tools including REMUS 100 Autonomous Underwater Vehicles and purpose-built Survey Craft.⁹⁴

The RN is pursuing a remarkably similar trajectory. Under its Mine Countermeasures and Hydrographic Capability (MHC) program, the RN is also divesting from traditional survey ships like HMS *Echo* and *Enterprise*.⁹⁵ In their place, the newly established Hydrographic Exploitation Group (HXG) operates as a specialised unit focused on deployable hydrography. Like the RAN's DGSTs, the HXG uses a combination of small survey boats (*Vahana*-class), AUVs, and other 'flyaway' kits to conduct rapid surveys. This transformation, driven by Project HECLA, is designed to make hydrographic support more agile and responsive.⁹⁶ The key lesson from the RN's experience is organizational: the decision to separate the hydrographic and meteorological specialisations into two distinct units (the HXG and the Metoc Information Warfare Group) suggests that developing deep expertise in autonomous systems requires a dedicated and focused organisational structure.⁹⁷ It is noteworthy that the RAN never did amalgamate in a way that required the meteorological and hydrographic categories to be cross-trained. In the RAN both categories gather and analyse different types of maritime geospatial intelligence (i.e. one hydrographic, one meteorological) requiring vastly different training, although they are led and administered together.

The US Navy, while also heavily investing in uncrewed systems, offers a different model of integration, not so much for its hydrographic systems, but its MCM capabilities. Rather than a platform-agnostic, deployable toolkit (which the RAN has for hydrographic, and will likely pursue for MCM), the USN's primary MCM capability is being integrated into a specific platform: the Littoral Combat Ship (LCS) Mine Countermeasures Mission Package (MP).⁹⁸ This package employs a suite of uncrewed systems, including the Mine Countermeasures Unmanned Surface Vehicle (MCM USV), which acts as a mothership for both the Unmanned Influence Sweep System (UISS) for detonating mines and the AN/AQS-20 sonar for minehunting.⁹⁹ At this

⁹⁴ BlueZone Group, 'SEA 1770 Rapid Environmental Assessment,' <https://bluezonegroup.com.au/sea-1770-rapid-environmental-assessment/> accessed 4 August 2025.

⁹⁵ 'Royal Navy launches new Hydrographic Exploitation Group to transform survey operations,' *Navy Lookout*, 4 June 2025, <https://www.navylookout.com/royal-navy-launches-new-hydrographic-exploitation-group-to-transform-survey-operations/> accessed 4 August 2025.

⁹⁶ Royal Navy News, 'New Hydrographic Unit harnesses tech to revolutionise surveying and data gathering,' Royal Navy, 4 June 2025, <https://www.royalnavy.mod.uk/news/2025/june/04/20250604-new-hydrographic-unit> accessed 4 August 2025.

⁹⁷ 'Royal Navy trials underwater gliders that can aid submarine hunters,' Royal Navy, 30 April 2020, <https://www.royalnavy.mod.uk/news/2020/april/30/300420-glider-trials> accessed 4 August 2025.

⁹⁸ US Navy, 'Littoral Combat Ships - Mine Countermeasures Mission Package,' Fact File, <https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167535/littoral-combat-ships-mine-countermeasures-mission-package/> accessed 4 August 2025.

⁹⁹ US Navy, 'Mine Countermeasures Unmanned Surface Vehicle (MCM USV),' Fact File, <https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167996/mine-countermeasures-unmanned-surface-vehicle-mcm-usv/> accessed 4 August 2025.

juncture, it is important to understand that the technologies in use for MCM, particularly the 'detection phase' is fundamentally the same as hydrographic surveying technologies. It is simply the case that the 'risk' they are seeking to mitigate against is of a different nature. The UISS and AN/AQS-20 sonar is complemented by the Knifefish, a heavyweight AUV designed to detect buried and high-clutter mines.¹⁰⁰ The USN's experience provides a cautionary lesson in the complexities of systems integration. While highly capable, the LCS MCM MP has faced significant delays and challenges during operational testing, highlighting the difficulty of fielding a reliable 'system of systems'.¹⁰¹ The overarching direction is managed by the Naval Meteorology and Oceanography Command (CNMOC), which sources data from a vast array of uncrewed platforms to provide environmental awareness.¹⁰²

For the RAN, the experiences of its allies validate its strategic direction while offering crucial insights. The parallel evolution of the RN's HXG confirms the operational logic of creating specialised, deployable teams. The RN's size and hydrographic capability is also more akin in size to the RAN's hydrographic capability. By contrast, the USN's size vastly outweighs both the RN and RAN. Consequently, the USN is able to continue to operate platforms that are specialized, thus introducing the complexity of 'systems in systems'¹⁰³ issues. The USN's journey with the LCS MCM package underscores the immense technical and programmatic challenges of integrating multiple complex autonomous systems, reinforcing the value of the RAN's more incremental, 'evergreening' approach outlined in its RAS-AI Campaign Plan.¹⁰⁴ Ultimately, the success for all three navies hinges on interoperability. The AUKUS Pillar 2 framework, with its focus on undersea capabilities and autonomy, provides the critical mechanism for this collaboration.¹⁰⁵ Joint exercises, such as the Maritime Big Play series, are essential for developing the common data standards and operating procedures needed to ensure that the autonomous systems of all three nations can operate as a cohesive force, turning technological potential into a collective strategic advantage.¹⁰⁶ Although beyond this thesis's scope, beneficial insights can also be gained from further research that engages in a comparative analysis of the hydrographic capabilities of India, France and Canada.¹⁰⁷

¹⁰⁰ General Dynamics Mission Systems, 'Knifefish Surface Mine Countermeasure UUV,' DASC, https://www.dacis.com/nuxt/programs_sample_record.C2y8zz-.pdf accessed 4 August 2025.

¹⁰¹ US Government Accountability Office, '*Littoral Combat Ship: Actions Needed to Address Significant Operational and Sustainment Challenges*,' GAO-22-105387 (Washington, D.C.: GAO, 2022), 24 February 2022, <https://www.gao.gov/products/gao-22-105387> accessed 4 August 2025.

¹⁰² Naval Meteorology and Oceanography Command, 'Naval Oceanography Office,' <https://www.cnmoc.usff.navy.mil/navocean/> accessed 4 August 2025.

¹⁰³ The by having such specialised platforms, there is an additional layer of complexity. Such platforms not only deal with the complexity of the autonomous systems they operate, but have an additional layer of 'assets' that require 'force protection', 'integration', and adoption into operational and tactical planning. These matters are far from insurmountable, however, given the USN's larger scale, it is arguably more tenable, noting that these were all matters the RAN had to consider before divestment of its hydrographic platforms.

¹⁰⁴ Royal Australian Navy, *RAS-AI Campaign Plan 2025*, 2.

¹⁰⁵ Royal Australian Navy, *RAS-AI Campaign Plan 2025*, 2.

¹⁰⁶ 'Royal Navy leads AUKUS trials to improve use of autonomous systems,' Royal Navy, 24 June 2025, <https://www.royalnavy.mod.uk/news/2025/june/24/20250624-aukus-data-sharing-exercise> accessed 4 August 2025.

¹⁰⁷ These countries particularly, have advanced hydrographic surveying capabilities.



Chapter 5: Workforce Transformation for an Autonomous Future: The Core Analysis

The preceding chapters established the strategic and technological imperatives driving the modernisation of the RAN's hydrographic capability. The strategic context of the Indo-Pacific, mandates a shift towards a 'strategy of denial' enabled by disruptive technologies, while the maturation of autonomous systems and AI offers the means to achieve this.¹⁰⁸ This chapter forms the core of the thesis, directly addressing the central research question by arguing that the successful integration of these technologies is contingent not on procurement alone, but on a profound and deliberate workforce transformation. It moves from the 'what' (technology) and 'why' (strategy) to the 'who' and 'how' of the human dimension, dissecting the multifaceted nature of this evolution—from individual skills and professional identity to the organisational culture required to field a truly hybrid human-machine force.

The Evolving Identity of the Hydrographic Specialist: From Mariner to Systems Operator

The fundamental identity of the naval hydrographic specialist is undergoing a paradigm shift. The traditional role, rooted in seamanship and the meticulous, hands-on survey work conducted from the decks of dedicated platforms like the now-decommissioned *Leeuwin* and *Paluma* classes, is becoming obsolete.¹⁰⁹ The future specialist is a technologist first: a multi-domain systems operator, data scientist, and AI interpreter whose value is defined by their ability to manage a distributed network of autonomous assets, rather than (necessarily) a deep proficiency in the full range of traditional mariner skills.¹¹⁰ This conceptual evolution is driven by tangible capability decisions. The divestment of platform-centric assets and the move towards deployable, containerised 'tool-kits' under projects such as SEA 1770 and the now cancelled SEA 1905 physically severs the surveyor from a specific ship, necessitating a new identity founded on the capability they wield, not the vessel they serve in.¹¹¹

This transition is not unique to the RAN. The Royal Navy's parallel shift away from traditional survey ships in favour of the deployable, autonomous-equipped Hydrographic Exploitation Group validates this conceptual model, demonstrating an allied move towards a capability-centric workforce.¹¹² The RAN itself signals this change in its recruitment material, which now highlights the 'adoption and delivery of leading

¹⁰⁸ Australian Government, Department of Defence, Defence Strategic Review pgs 19, 66; Australian Government, Department of Defence, 2024 National Defence Strategy pgs 4, 35.

¹⁰⁹ Jonathan Nally, 'Navy now has only one hydrographic survey ship,' Spatial Source, 12 August 2024; Australian Defence Magazine, 'HMAS *Melville* to be decommissioned,' 22 July 2024.

¹¹⁰ Clearly, such skills as basic navigation and small boat operation will be necessary if required to deploy independently as envisaged by the DGST model currently in use.

¹¹¹ Gordon Arthur, 'Australian defence programmes,' Asian Military Review, 5 June 2025, <https://www.asianmilitaryreview.com/2025/06/australian-defence-programmes/> accessed 8 August 2025; BlueZone Group, 'SEA 1770 Rapid Environmental Assessment.

¹¹² 'Royal Navy launches new Hydrographic Exploitation Group to transform survey operations,' Navy Lookout, 4 June 2025; Royal Navy News, 'New Hydrographic Unit harnesses tech to revolutionise surveying and data gathering,' Royal Navy, 4 June 2025.

edge Geospatial Autonomous systems' as a rewarding and central aspect of the role.¹¹³ This shift, however, fundamentally alters the social contract between the Navy and its sailors. Historically, a sailor's career progression was intrinsically linked to accumulating sea time on commissioned hydrographic ships, which are specialised warships. The new model, exemplified by the Deployable Geospatial Support Teams operating from shore or vessels of opportunity, disrupts this pathway.¹¹⁴ A hydrographic specialist may now accumulate less 'traditional' sea time, potentially disadvantaging them under legacy sea-time accrued pay allowance models. This creates a critical challenge for Navy's personnel management: it must redefine what constitutes valuable operational experience. Is it days at sea, or can it be the successful execution of a complex autonomous survey mission from a shore-based control centre? Failure to adapt these cultural and policy frameworks risks devaluing the very personnel who are essential to the future fight.

Building the New Workforce: Skillsets, Training, and Career Pathways

To generate this future workforce, the RAN must fundamentally adapt its approach to training, recruitment, and retention. The required competencies extend far beyond traditional hydrography into domains of robotics, data science, AI and machine learning, and systems engineering.¹¹⁵ Personnel must be skilled not only in operating autonomous vehicles but also in managing the vast datasets they produce, critically evaluating AI-driven analysis, and understanding the systems engineering principles of complex, software-intensive platforms.¹¹⁶ This necessitates a training and education pipeline that prioritises advanced technical acumen. The RAN must deepen its partnerships with institutions like the Australian Maritime College and establish clear pathways for its personnel to attain postgraduate qualifications.¹¹⁷

Recruiting and retaining this talent presents a formidable challenge. The ADF is already facing significant recruitment shortfalls in a competitive labour market, particularly for skilled individuals.¹¹⁸ The skills required for an autonomy-enabled hydrographic

¹¹³ 'Hydrographic Surveyor,' Australian Defence Force Careers, <https://www.adfcareers.gov.au/jobs/navy/hydrographic-surveyor> accessed 8 August 2025.

¹¹⁴ Department of Defence, 'Navy team surveys Tonga below the waterline,' media release, 18 February 2022, <https://www.defence.gov.au/news-events/news/2022-02-18/navy-team-surveys-tonga-below-waterline> accessed 8 August 2025; Lily Lancaster, 'Royal Australian Navy Joins Its Army's Landing Force,' DVIDS, 15 July 2022, <https://www.dvidshub.net/news/425457/royal-australian-navy-joins-its-armys-landing-force> accessed 8 August 2025.

¹¹⁵ 'Hydrographic surveyor: Job profile,' Prospects, <https://www.prospects.ac.uk/job-profiles/hydrographic-surveyor> accessed 8 August 2025; Mohammadreza Bachari-Lafteh and Abbas Harati-Mokhtari, 'Operator's Skills and Knowledge Requirement in Autonomous Ships Control Centre,' Journal of International Maritime Safety, Environmental Affairs, and Shipping 5, no. 2 (27 July 2021): 74-84, <https://doi.org/10.1080/25725084.2021.1949842> accessed 8 August 2021.

¹¹⁶ 'Hydrography,' University of South Florida, <https://www.usf.edu/marine-science/research/hydrography.aspx> accessed 8 August 2025; 'Hydrographic Science,' The University of Southern Mississippi, <https://www.usm.edu/graduate-programs/hydrographic-science.php> accessed 8 August 2025.

¹¹⁷ 'The AMSL Team,' AMC Search, <https://www.amcsearch.com.au/amsl-team> accessed 8 August 2025.

¹¹⁸ Bec Shrimpton, Zach Lambert, Australian Strategic Policy Institute, 'Regional Security and Pacific Partnerships: Recruiting Pacific Islanders into the Australian Defence Force', (Canberra: ASPI, 25 April 2024), <https://www.aspi.org.au/report/regional-security-and-pacific-partnerships-recruiting->

workforce are precisely those in high demand by the civilian technology sector, which can offer more lucrative compensation. While the introduction of a continuation bonus scheme is a positive step, a generic financial incentive may be insufficient to retain highly specialised personnel.¹¹⁹ The career pathway itself must be compelling, offering unique operational experiences, continuous professional development, and a clear trajectory to appropriate leadership positions that industry cannot replicate. The profound nature of this skills transformation is best illustrated through a direct comparison of the legacy and future roles, as detailed in Table 5.1.

Table 5.1: The Shifting Profile of the RAN Hydrographic Surveyor

Characteristic	Legacy Capability (Platform-Centric)	Future Capability (Autonomy-Enabled)
Primary Tasks	Manual data collection; ship navigation; direct sensor operation.	Mission planning for AUVs/USVs; remote system supervision; AI-assisted data validation.
Core Technical Skills	Seamanship; traditional survey techniques; celestial navigation.	Robotics operation; network management; data science; AI/Machine Learning (ML) interpretation; systems engineering.
Cognitive Skills	Methodical data recording; procedural compliance.	Complex problem-solving; interpretation of AI outputs; dynamic mission re-tasking.
Operating Environment	Aboard commissioned survey vessel (e.g., <i>Leeuwin</i> -class), mixed with shore based camps for 'tidal data collection'.	Deployable teams; shore-based control centres; vessels of opportunity.
Primary Human-Machine Interface	Ship's helm; single-beam or multi-beam echosounder, and sidescan sonar console.	Autonomous system control console; AI-driven data analysis software; collaborative mission planners.

[pacific-islanders-australian-defence](#) accessed 9 August 2025; Ryan Neelam, Lowy Institute, 'Defence and security,' Lowy Institute Poll 2025 Report, 16 June 2025, <https://poll.lowyinstitute.org/report/2025/defence-and-security/> accessed 9 August 2025.

¹¹⁹ 'Investing in Defence's people,' Minister for Defence, media release, 5 November 2024, <https://www.minister.defence.gov.au/media-releases/2024-11-05/investing-defences-people> accessed 9 August 2025; Melissa George, 'ADF retention bonus scheme,' Parliament of Australia, 20 June 2023, https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/FlagPost/2023/June/ADF-Retention accessed 9 August 2025.

Human-Machine Teaming in the Littoral: A New Operational Paradigm

The effective employment of these new systems operationalises the concept of Human-Machine Teaming (HMT) in the hydrographic context. HMT is more than a technological interface; it represents a new way of working that demands new tactics, techniques, and procedures (TTPs), robust models of trust, and a redefinition of the human's role as a supervisor and mission commander (and 'troubleshooter'), rather than a direct operator. As an offset strategy, HMT aims to improve sensing, analysis, and decision-making while removing personnel from harm's way (or when not in a conflict area, at least away from the elements)—a direct alignment with the DSR's strategic imperatives.¹²⁰ The RAN's *RAS-AI Campaign Plan 2025* explicitly identifies increasing the understanding of HMT as a key line of effort.¹²¹

This paradigm shift presents significant human factors challenges. Operators must build calibrated trust in the reliability of autonomous systems and the validity of their AI-generated outputs, maintain situational awareness while physically removed from the sensors, and manage the cognitive load of supervising multiple complex systems simultaneously.¹²² This requires a new 'language' of command and control. Traditional naval command is hierarchical and direct. An operator cannot manually pilot multiple AUVs simultaneously; therefore, the interaction must evolve from direct control (e.g., ordering 'steer 10 degrees to port') to mission-based command (e.g., 'survey this area, avoid these threat zones, maintain this data quality, and report anomalies').¹²³ This requires the human operator to develop a deep, intuitive understanding of the AI's decision-making logic, its capabilities, and its limitations. This is the essence of 'teaming,' and it necessitates a new training focus: teaching personnel how to team with an AI, a cognitive and psychological skill that transcends mere technical operation.

Organisational and Cultural Adaptation for a Hybrid Force

Ultimately, the full potential of an autonomy-enabled hydrographic capability cannot be realised within the RAN's existing organisational and cultural constructs. While the Navy has laudably articulated a need to foster a culture of innovation and agility, large military organisations are often inherently resistant to disruptive change.¹²⁴ The experience of allied navies shows that successful technology integration requires evolving acquisition strategies and a willingness to challenge established processes; systems that are not deemed 'fit for purpose' by the end-user will face resistance, undermining trust and

¹²⁰ Sidharth Kaushal et al., 'Leveraging Human-Machine Teaming: An Offset Strategy Primer and Policy Guide,' RUSI, Special Competitive Studies Project, January 2024, <https://static.rusi.org/human-machine-teaming-sr-jan-2024.pdf> accessed 9 August 2025; Centre for Naval Analyses, 'Addressing AI's Operational Challenges: Putting the Human in Human-Machine Teaming,' (Arlington, VA: CNA, 2021), <https://www.cna.org/reports/2021/10/Addressing-AIs-Operational-Challenges-Putting-the-Human-in-Human-Machine-Teaming.pdf> accessed 9 August 2025.

¹²¹ Royal Australian Navy, *RAS-AI Campaign Plan 2025*.

¹²² Geoffrey Ho et al, DRDC, 'Human Factors Issues in Unmanned Underwater Vehicles,' (Toronto: Defence Research and Development Canada, 2011), <https://apps.dtic.mil/sti/tr/pdf/ADA555588.pdf> accessed 9 August 2025.

¹²³ Northrop Grumman, 'Distributed Autonomy/Responsive Control – DA/RC,' <https://www.northropgrumman.com/what-we-do/mission-solutions/distributed-autonomy-responsive-control-da-rc> accessed 9 August 2025.

¹²⁴ Royal Australian Navy, 'Mission & Values,' <https://www.navy.gov.au/about-navy/mission-values> accessed 10 August 2025; Rob Hoehn, 'How the Royal Australian Navy Nurtures Innovators,' Innovation Management, 13 July 2020, <https://innovationmanagement.se/2020/07/13/how-the-royal-australian-navy-nurtures-innovators/> accessed 9 August 2025.

hindering adoption.¹²⁵ The creation of specialised units, such as the RN's HXG or the RAN's own Maritime Deployable Robotic and Autonomous Systems Experimentation Unit, is a logical step, suggesting that deep expertise may need to be nurtured in focused cells before being integrated more broadly.¹²⁶

Although not mutually exclusive, this technological shift risks creating a cultural rift between the traditional 'warrior' class, whose careers are defined by operational command at sea, and a new 'technologist' class, whose expertise is analytical and systems-based. If these new specialists are perceived merely as a 'support' function, their influence on operational planning may be limited, and the Navy will struggle to retain them. This presents a critical leadership challenge that extends beyond the hydrographic community. Senior leadership must actively champion the value of these new specialists by creating viable career pathways to senior ranks (perhaps broadening their experience beyond hydrography), integrating them fully into operational planning, and fostering a culture where data-driven insights from an AI-enabled team are valued as highly as a commander's intuition. At the higher ranks individuals will have strengths not necessarily leveraged off at the tactical level, such as strategic insight and empathy. These too should be fostered, and talent identified early, particularly for officers. Failure to bridge this cultural divide risks creating a two-tiered workforce and devaluing the very skills the Navy needs to maintain its edge in future conflicts.

The transformation of the hydrographic workforce is a complex, multi-layered challenge that extends far beyond simple retraining. It demands a fundamental rethinking of professional identity, the creation of new career models to compete for talent, the development of novel operational concepts for HMT, and a deliberate, leader-led cultural adaptation. Successfully navigating this transformation is not merely a prerequisite for a modern hydrographic capability; it is a microcosm of the challenge facing the entire RAN as it seeks to become a truly capable, AI-enabled future force.

¹²⁵ Michael Keegan, 'Navigating Technological Frontiers in the U.S. Navy,' IBM Center for The Business of Government, 12 June 202 <https://www.businessofgovernment.org/blog/navigating-technological-frontiers-us-navy> accessed 9 August 2025; A. M. C. van der Veen and M. C. van der Veen, 'On the Bridges: Insight Into the Current and Future Use of Automated Systems as Seen by Royal Navy Personnel,' Proceedings of the Human Factors and Ergonomics Society Annual Meeting 62, no. 1 (2018): 1545-1549, <https://doi.org/10.1177/1541931218621349> accessed 9 August 2025.

¹²⁶ Department of Defence, 'Nations combine on mine warfare activity,' Defence Annual Report 2023-24, <https://www.transparency.gov.au/publications/defence/department-of-defence/department-of-defence-annual-report-2023-24/chapter-2---departmental-overview/nations-combine-on-mine-warfare-activity> accessed 9 August 2025.

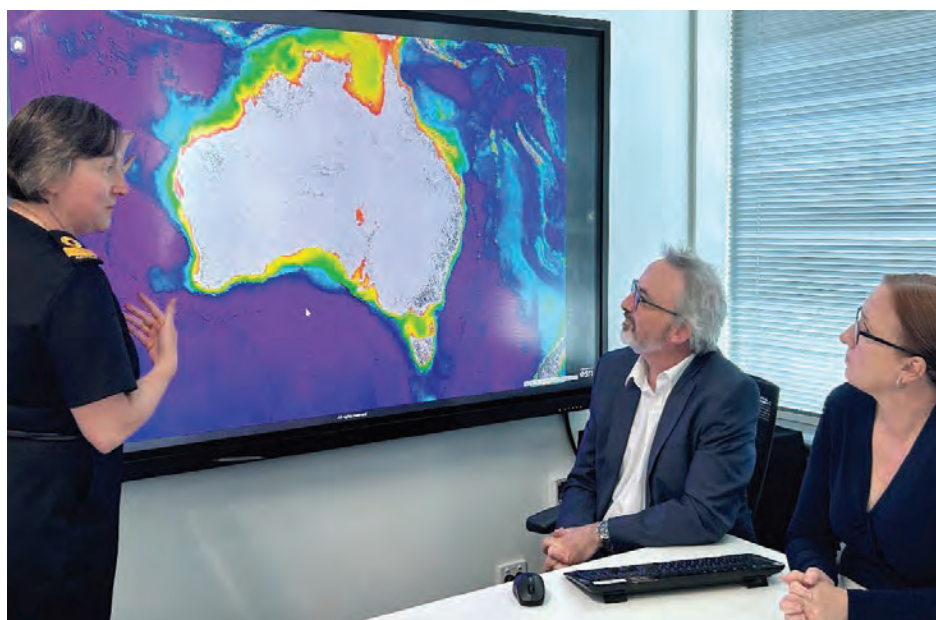


Image: Department of Defence

Chapter 6: The Supporting Ecosystem: Industry, Research, and Innovation

The profound workforce transformation detailed in the preceding chapter does not occur in a vacuum. It is both a response to and a dependency of a broader national (and international) ecosystem comprising industry partners, dedicated research and development (R&D) entities, and new innovation accelerators. The RAN's ability to generate and sustain a future hydrographic workforce is inextricably linked to the health, agility, and collaborative capacity of this ecosystem. This chapter assesses the key components of this supporting structure, evaluating the strategic role of industry partnerships, the contributions of the national research base, and the potential of new mechanisms designed to accelerate capability delivery. It argues that while Australia possesses significant strengths in this ecosystem, realising the full potential of an autonomous hydrographic capability requires a deliberate and integrated approach to harnessing these national assets.

The Strategic Shift to Industry Partnership: HIPP as a Catalyst

A central pillar of the RAN's evolving hydrographic capability model is the strategic decision to partner more closely with the commercial sector, a policy embodied by the HydroScheme Industry Partnership Program. As demonstrated in Chapter 1, HIPP outsources a significant portion of Australia's national charting responsibility to a panel of specialist hydrographic survey companies.¹²⁷ This represents a fundamental restructuring of the national hydrographic enterprise, driven by a clear strategic logic. By leveraging the capacity and innovation of the commercial sector to conduct broad-area surveying, the RAN's uniformed hydrographic workforce can be refocused on its core military function: the provision of specialised military geospatial intelligence (GEOINT) in direct support of operations.¹²⁸ This aligns closely with the *Defence Strategic Review's* recommendation for a more 'focused force'.¹²⁹

This partnership model is a significant strength, stimulating the growth of a sovereign Australian hydrographic industry and encouraging the adoption of new technologies, including the use of AUVs and USVs for nautical charting surveys.¹³⁰ However, it also introduces a critical weakness and a long-term strategic risk. An over-reliance on industry for foundational survey tasks risks the atrophy of core military hydrographic skills within the permanent naval force. This creates a potential capability dependency, where the RAN might lose the organic ability to conduct large-scale or complex survey operations without commercial support. It could be argued that even without HIPP military hydrographic skills and experience was already atrophying due to tasking hydrographic surveying platforms with other unrelated high priority taskings such as border protection. The conduct of rapid environmental assessment (REA) military

¹²⁷ Australian Hydrographic Office, 'HydroScheme Industry Partnership Program,' <https://www.hydro.gov.au/NHP/hipp.htm> accessed 11 August 2025; Department of Defence, 'Hydroscheme industry partnership program commences,' media release, 26 February 2020, <https://www.defence.gov.au/news-events/releases/2020-02-26/hydroscheme-industry-partnership-program-commences> accessed 11 August 2025.

¹²⁸ Department of Defence, 'Hydroscheme industry partnership program commences.'

¹²⁹ Australian Government, Department of Defence, *Defence Strategic Review* (Canberra: Department of Defence, 2023), pg 53.

¹³⁰ AusSeabed, February 2021 Newsletter, 'Australian's National Hydrographic Surveying has Evolved — HIPP has Arrived,' pgs 3-9, https://www.ausseabed.gov.au/_data/assets/pdf_file/0005/106934/February_2021_Newsletter22.pdf accessed 11 August 2025.

surveys is assisted when the 'operators' (i.e. the hydrographic surveyors) have a great deal of experience in surveying generally. Furthermore, the HIPP model places immense pressure on Defence's ability to act as an 'intelligent customer'—requiring a workforce skilled not just in surveying, but in complex contract management, quality assurance, and the verification of industry-provided data. The challenge for the RAN (and more directly, the Australian Geospatial Intelligence Organisation (AGO) to which the AHO is a part)¹³¹, therefore, is to strike a delicate balance: leveraging industry's strengths without sacrificing the sovereign military expertise that is indispensable in a contested environment.

The National Research and Development Engine

Underpinning the technological advancement of the hydrographic capability is a national R&D ecosystem composed of government, academic, and collaborative research entities. At its core is the Defence Science and Technology Group (DSTG), the Australian government's lead agency for applying science and technology to national security.¹³² DSTG provides impartial scientific advice and works closely with AGO, the RAN, industry, and academia to deliver capability enhancements, playing a key role in shaping and executing the *RAS-AI Campaign Plan*.¹³³ Its deep expertise in areas such as sonar technology, data processing, and systems integration provides the essential scientific foundation for acquiring and fielding complex autonomous systems.¹³⁴ Importantly it keeps abreast of international technological developments, both in industry generally and militaries.

Complementing DSTG is the Trusted Autonomous Systems Defence Cooperative Research Centre (TAS DCRC), a unique entity established to foster collaboration between industry, research organisations, and Defence.¹³⁵ TAS DCRC's focus is not just on autonomy, but on *trusted* autonomy, addressing the critical HMT challenges central to the workforce transformation.¹³⁶ Its work on developing assurance methodologies and supporting the creation of regulatory frameworks, such as the Australian Code of Practice for Autonomous and Remotely Operated Vessels, is a vital enabler for the safe and effective operationalisation of these new technologies.¹³⁷ The opportunity presented by this R&D landscape is the potential to create a virtuous cycle: Defence defines the operational problems, DSTG and TAS DCRC facilitate the collaborative research to solve them, and industry partners commercialise and deliver the solutions.

¹³¹ Australian Government, National Intelligence Community, Australian Geospatial-Intelligence Organisation, <https://www.intelligence.gov.au/agencies/ago> accessed 11 August 2025.

¹³² Defence Science and Technology Group, 'About,' <https://www.dst.defence.gov.au/> accessed 11 August 2025.

¹³³ Royal Australian Navy, *RAS-AI Campaign Plan 2025*, pg 5.

¹³⁴ Defence Science and Technology, DST Capability Portfolio (Canberra: Department of Defence, 2017), pg 11, https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST_Capability_Portfolio_051017.pdf accessed 11 August 2025.

¹³⁵ Trusted Autonomous Systems, "About," accessed August 10, 2025, <https://tas.tech/>.

¹³⁶ Rachel Horne, 'Trusted Autonomous Systems, Defence Cooperative Research Centre Submission to the Independent Review of Domestic Commercial Vessel Safety Legislation,' 30 March 2022, <https://www.infrastructure.gov.au/sites/default/files/documents/dcvir-submission-7-trusted-autonomous-systems.pdf> accessed 11 August 2025.

¹³⁷ Trusted Autonomous Systems Defence Cooperative Research Centre, Submission.

Accelerating Innovation: From Concept to Capability

A persistent weakness in Australia's defence innovation ecosystem has been the difficulty in transitioning promising technologies from the laboratory into the hands of the warfighter—a challenge often referred to as the 'valley of death'.¹³⁸ The establishment of the Advanced Strategic Capabilities Accelerator (ASCA) is a direct response to this systemic problem, created to fast-track the development and acquisition of disruptive capabilities.¹³⁹ With a mission-oriented approach and a mandate to move with speed and agility, ASCA represents a significant opportunity to overcome the institutional inertia that can stifle innovation.¹⁴⁰

ASCA's relevance to hydrographic modernisation is already evident. Its inaugural 'Mission Zero' is the Ghost Shark program,¹⁴¹ which delivers three extra-large autonomous undersea vehicles (XL-AUVs), a clear investment in the future of maritime autonomy (although from publicly available information it is not clear they can collect hydrographic data).¹⁴² Furthermore, ASCA is actively leveraging the AUKUS Pillar 2 framework through initiatives like the Maritime Innovation Challenge, which focuses on undersea communications and the control of autonomous systems.¹⁴³ This mechanism provides a powerful pathway to not only accelerate sovereign capability but also to ensure deep interoperability with key allies. The primary threat to this model is structural/cultural. The success of ASCA will depend on its ability to challenge Defence's traditional risk-averse culture and streamline cumbersome procurement processes, which have historically been barriers to rapid innovation.¹⁴⁴

¹³⁸ Jennifer Jackett, 'Defence innovation and the Australian national interest,' Black Swan Strategy Issue 9, June 2023, (Perth: Defence & Security Institute, University of Western Australia), <https://defenceuwa.com.au/wp-content/uploads/2024/10/Black-Swan-Strategy-Paper-9-Defence-Innovation-and-the-Australian-National-Interest-Jennifer-Jackett.pdf> accessed 16 August 2025.

¹³⁹ Department of Defence, 'The establishment of the Advanced Strategic Capabilities Accelerator,' media release, 1 May 2023, <https://www.dst.defence.gov.au/news/2023/05/01/establishment-advanced-strategic-capabilities-accelerator> accessed 16 August 2025.

¹⁴⁰ Pat Conroy, quoted in 'The Advanced Strategic Capabilities Accelerator is up and running to drive defence innovation,' Asia-Pacific Defence Reporter, 5 July 2023, <https://asiapacificdefencereporter.com/the-advanced-strategic-capabilities-accelerator-is-up-and-running-to-drive-defence-innovation/> accessed 16 August 2025.

¹⁴¹ Department of Defence, 'Equipping the Royal Australian Navy with next generation autonomous undersea vessels,' media release, 10 September 2025, see: <https://www.minister.defence.gov.au/media-releases/2025-09-10/equipping-royal-australian-navy-next-generation-autonomous-undersea-vehicles> accessed 21 September 2025.

¹⁴² Advanced Strategic Capabilities Accelerator, 'Ghost Shark – Mission Zero,' <https://www.asca.gov.auhttps://www.asca.gov.au/activities/missions/ghost-shark-mission-zero> accessed 16 August 2025.

¹⁴³ Advanced Strategic Capabilities Accelerator, 'AUKUS Maritime Innovation Challenge 2025: undersea communications and autonomy,' <https://www.asca.gov.au/current-activities/aukus-maritime-innovation-challenge-2025-undersea-communications-autonomy> accessed 16 August 2025.

¹⁴⁴ Sam Davis et al, 'Innovation Catalyst: ASCA, Accelerating technology development and capability delivery through superior process and reduced barrier partnerships,' Defence Industry Leadership Program Research Paper, November 2023, <https://dtc.org.au/files/documents/DILP-Research-Papers/2023/Innovation-Catalyst.pdf> accessed 16 August 2025.

In synthesis, the ecosystem supporting the RAN's hydrographic modernisation is characterised by significant strengths and opportunities. It possesses a growing and increasingly capable domestic industry, a robust government-led R&D base, and new, agile mechanisms designed to accelerate innovation. However, it is also beset by weaknesses and threats, including the risk of eroding sovereign military skills through over-reliance on industry, a historically risk-averse institutional culture, and the immense pressure of a deteriorating strategic environment that demands capability delivery at an unprecedented pace. For the transformed hydrographic workforce, this ecosystem is the professional environment in which it must operate. Its ability to effectively partner with industry, collaborate with researchers, and leverage new innovation pathways will be the ultimate determinant of whether the promise of an autonomous future can be translated into a decisive capability edge for the RAN.

Chapter 7: Policy, Doctrine, and Regulatory Alignment: Supporting the Transformation

The successful transformation of the Royal Australian Navy's hydrographic workforce, as analysed in the previous chapters, is not solely dependent on acquiring new technologies or developing new skillsets. It requires an equally profound evolution in the 'soft infrastructure' that governs naval operations: the policies, doctrine, and legal frameworks that provide the authority, guidance, and constraints for the employment of an autonomy-enabled capability. The strategic direction in the NDS and the technological potential of Robotics, Autonomous Systems, and Artificial Intelligence create a powerful momentum for change.¹⁴⁵ However, this momentum risks being stalled by legacy doctrinal concepts and a regulatory environment designed for an era of exclusively human-crewed vessels. This chapter evaluates the alignment of the RAN's existing policy and doctrine with the demands of its future hydrographic force and examines the significant challenges posed by the national and international legal landscape, arguing that without deliberate reform in these areas, the full potential of the transformed workforce and its advanced capabilities cannot be realised.

Aligning Naval Doctrine with a Transformed Capability

The RAN has demonstrated strategic foresight in its high-level policy documents, most notably the *RAS-AI Strategy 2040* and its supporting *RAS-AI Campaign Plan 2025*.¹⁴⁶ These documents articulate a clear vision for leveraging autonomous systems to enhance combat power, increase mass, and reduce risk to personnel, directly aligning with the DSR's 'Strategy of Denial'.¹⁴⁷ The *Campaign Plan* explicitly identifies the workforce as a key line of effort, acknowledging the need for new training paradigms and a deeper understanding of HMT.¹⁴⁸ This represents a crucial top-down endorsement of the workforce transformation at the heart of this thesis.

However, a gap persists between this high-level strategic vision and the development of detailed operational doctrine. The transition from a platform-centric to a capability-centric mindset, exemplified by the divestment of survey ships in favour of deployable 'tool-kits' under projects like SEA 1770 and the discontinued SEA 1905, requires a fundamental rewrite of the tactical-level doctrine that guides how hydrographic effects are delivered.¹⁴⁹ Traditional maritime doctrine is built around the ship as the primary unit of action. The new model, centred on agile, shore-based or vessel-of-opportunity-deployed teams like the DGSTs, demands new concepts of operation (CONOPS) that are not yet fully mature.¹⁵⁰ The experiences of allied navies, particularly the Royal

¹⁴⁵ *Defence Strategic Review 2023*, pgs 19 and 66; *2024 National Defence Strategy*, pgs 4 and 35.

¹⁴⁶ *Robotics, Autonomous Systems & Artificial Intelligence (RAS-AI) Strategy 2040*; *RAS-AI Campaign Plan 2025*.

¹⁴⁷ *RAS-AI Campaign Plan 2025*.

¹⁴⁸ Sidharth Kaushal et al., 'Leveraging Human-Machine Teaming: An Offset Strategy Primer and Policy Guide,' RUSI, Special Competitive Studies Project, January 2024, <https://static.rusi.org/human-machine-teaming-sr-jan-2024.pdf> accessed 18 August 2025.

¹⁴⁹ Gordan Arthur, 'Australian defence programmes,' *Asian Military Review*, 5 June 2025, <https://www.asianmilitaryreview.com/2025/06/australian-defence-programmes/> accessed 18 August 2025.

¹⁵⁰ Lily Lancaster, 'Royal Australian Navy Joins Its Army's Landing Force,' *DVIDS*, 15 July 2022, <https://www.dvidshub.net/news/425457/royal-australian-navy-joins-its-armys-landing-force> accessed 18 August 2025; Department of Defence, 'Navy team surveys Tonga below the waterline,' media release, 18 February 2022,

Navy's establishment of the HXG, provide a valuable template, but the RAN must develop its own doctrine tailored to its specific strategic geography and force structure.¹⁵¹ Without this doctrinal evolution, the transformed workforce will be equipped with revolutionary tools but constrained by evolutionary—or even archaic—rules of employment. The RAN DGSTs are equipped with conventional small boat technologies (e.g., multi-beam echo-sounders, and side-scan sonars) rather than AUV and RAS systems, with the exception of a small number of REMUS 100S AUVs that are being used to 'explore' the possibilities of such technology.

Navigating the National Regulatory Maze (other than warships/Defence vessels)

A significant handbrake on the operationalisation of autonomous maritime systems (particularly in the civilian sector)¹⁵² is the national and international legal framework, which was conceived entirely for crewed vessels. In Australia, the primary legislative instruments are the *Navigation Act 2012* and the *Marine Safety (Domestic Commercial Vessel) National Law Act 2012*.¹⁵³ A fundamental challenge arises from the core definitions within these Acts. The definition of a 'vessel' is tied to its use in 'navigation,' a term traditionally interpreted as involving planned movement directed by a human navigator.¹⁵⁴ While a remotely operated vehicle with a human 'in the loop' may meet this definition, the status of a fully autonomous vessel operating on its own artificial intelligence is legally ambiguous.¹⁵⁵

This ambiguity extends to the concepts of 'master' and 'crew.' Both Acts define the master as the person with 'command or charge of the vessel'.¹⁵⁶ It may be difficult to argue that a remote operator, potentially thousands of kilometres away, or a software programmer/operator who set the mission parameters weeks earlier, has command and charge in the traditional sense.¹⁵⁷ Similarly, the definition of a 'seafarer' implies a person

<https://www.defence.gov.au/news-events/news/2022-02-18/navy-team-surveys-tonga-below-waterline> accessed 18 August 2025.

¹⁵¹ 'New Hydrographic Unit harnesses tech to revolutionise surveying and data gathering,' Royal Navy, 4 June 2025, <https://www.royalnavy.mod.uk/news/2025/june/04/20250604-new-hydrographic-unit> accessed 18 August 2025.

¹⁵² Section 10 of the *Navigation Act 2012* (Cth) provides some exemptions from the Act, see: https://www.legislation.gov.au/C2012A00128/2025-02-15/2025-02-15/text/original/epub/OEBPS/document_1/document_1.html#_Toc190870788 accessed 21 September 2025.

¹⁵³ *Navigation Act 2012* (Cth), see: <https://www.legislation.gov.au/C2012A00128/latest/text> accessed 21 September 2025; *Marine Safety (Domestic Commercial Vessel) National Law Act 2012* (Cth), see: <https://www.legislation.gov.au/C2012A00121/latest/text> accessed 21 September 2025.

¹⁵⁴ *Navigation Act 2012* (Cth); *Marine Safety (Domestic Commercial Vessel) National Law Act 2012* (Cth).

¹⁵⁵ David Anderson, 'Autonomous Ship Laws in Australia,' MLAANZ, May 2018, https://www.mlaanz.org/uploads/1/2/1/3/121322722/autonomous_ship_laws_australia.pdf accessed 18 August 2025.

¹⁵⁶ Anderson, 'Autonomous Ship Laws in Australia.' See s14 of the *Navigation Act 2012* (Cth) for definition of 'master', see: https://www.legislation.gov.au/C2012A00128/2025-02-15/2025-02-15/text/original/epub/OEBPS/document_1/document_1.html#_Toc190870793 accessed 21 September 2025.

¹⁵⁷ Australian Maritime Safety Authority, "AMSA policy on regulatory treatment of uncrewed and/or autonomous vessels," February 20, 2020, <https://www.amsa.gov.au/vessels-operators/domestic-commercial-vessels/amsa-policy-regulatory-treatment-uncrewed-and-or>.

working 'on board a vessel'.¹⁵⁸ These definitional challenges are not merely academic; they have profound implications for assigning legal responsibility, liability, and accountability in the event of a marine incident. The Australian Maritime Safety Authority (AMSA) has adopted a pragmatic, risk-based policy to navigate these issues, using flexibility mechanisms like exemptions to allow for the operation of uncrewed systems.¹⁵⁹ However, this approach is a temporary solution to a systemic problem. Arguably, the law has not kept pace with technology, creating a 'clunky' and burdensome regulatory environment that relies on workarounds rather than providing clear, purpose-built guidance for the operators of these new systems.¹⁶⁰ I anticipate that such domestic 'workarounds' of the law, will become evidence of State practice that will ultimately 'change' the international customary law upon which such domestic law is based—but further analysis of this argument however, is beyond the scope of this thesis.

For military (particularly Navy) AUVs and RAS vessels, they could be considered to be 'warships', thus exempting them from such domestic legislation and the application of relevant international law.¹⁶¹ Again, such legal detail required to articulate the application of the *Work Health and Safety Act 2011* (Cth), is beyond this thesis's scope; however, the RAN would be required to construct a 'seaworthiness' system that meets the legislated work, health and safety requirements for eliminating or at least mitigating risk to the lowest practicable level.¹⁶² The Navy is well-versed in such 'seaworthiness' practices and application as this is what is pursued for the internal (to Navy) regulation of warships and other Defence vessels currently in operation.

The International Challenge: COLREGs and the Uncrewed Vessel

This regulatory friction is magnified at the international level by the *International Regulations for Preventing Collisions at Sea 1972* (COLREGs). These rules are the bedrock of safe navigation globally, but their application to uncrewed vessels is fraught with difficulty.¹⁶³ The most acute problem lies with Rule 5, which mandates that every

¹⁵⁸ Australian Maritime Safety Authority, 'AMSA policy on regulatory treatment of uncrewed and/or autonomous vessels,' 20 February 2020, <https://www.amsa.gov.au/vessels-operators/domestic-commercial-vessels/amsa-policy-regulatory-treatment-uncrewed-and-or> accessed 24 August 2025; See section 14 of the *Navigation Act 2012* (Cth) for definition of 'seafarer', see: https://www.legislation.gov.au/C2012A00128/2025-02-15/2025-02-15/text/original/epub/OEBPS/document_1/document_1.html#_Toc190870793 accessed 21 September 2025.

¹⁵⁹ Australian Maritime Safety Authority, 'Autonomous vessels in Australia,' 24 August 2022, <https://www.amsa.gov.au/vessels-operators/domestic-commercial-vessels/autonomous-vessels-australia> accessed 18 August 2025.

¹⁶⁰ Nick Lemon, 'Autonomous shipping from a regulatory perspective,' IALA, <https://www.iala.int/content/uploads/2018/01/12.00-Nick-Lemon-Autonomous-shipping-from-a-regulatory-perspective.pdf> accessed 24 August 2025.

¹⁶¹ Section 10 of the *Navigation Act 2012* (Cth) provides some exemptions from the Act, see: https://www.legislation.gov.au/C2012A00128/2025-02-15/2025-02-15/text/original/epub/OEBPS/document_1/document_1.html#_Toc190870788 accessed 21 September 2025.

¹⁶² See Part 2-Health and Safety Duties in the *Work Health and Safety Act 2011* (Cth), see: https://www.legislation.gov.au/C2011A00137/2024-07-01/2024-07-01/text/original/epub/OEBPS/document_1/document_1.html#_Toc170716031 accessed 21 September 2025.

¹⁶³ Paul Margat, Michael Staderman, 'The Application of COLREGs by Autonomous and Unmanned Vessels: Issues Raised by Situational Awareness, Night-Time Navigation and Good Seamanship,' Institute for the Protection of Maritime

vessel shall 'at all times maintain a proper look-out by sight and hearing as well as by all available means'.¹⁶⁴ The long-held interpretation of this rule is that it requires a human lookout. While an autonomous vessel's sensors may provide a more comprehensive field of view than the human eye, they arguably cannot replicate the human act of 'hearing,' nor can they guarantee the infallible, continuous connection required to provide a remote operator with the same level of situational awareness as a person on the bridge.¹⁶⁵

Furthermore, the COLREGs are imbued with the concept of 'good seamanship,' a standard of prudent action that is qualitative and context-dependent.¹⁶⁶ Translating this subjective standard into machine-executable algorithms is a monumental challenge.¹⁶⁷ An autonomous system can be programmed with the explicit rules for head-on, crossing, and overtaking situations, but presently struggles with the nuanced, judgement-based decisions that human mariners make in complex traffic scenarios. This legal and practical impasse creates a significant liability risk, which can be relevant to Navy AUVs, particularly during peacetime.¹⁶⁸ In a collision, an uncrewed vessel could be deemed to have violated Rule 5 by default, placing its owner and operator at a distinct disadvantage, regardless of the other vessel's actions.¹⁶⁹ This uncertainty poses a direct threat to the transformed workforce — and even more so to the Commonwealth of Australia — which could be placed in a position of legal jeopardy even if operating systems were to be in full compliance with the training and doctrine.

Ethical Considerations in Autonomy

While the primary role of the RAN's hydrographic capability is data collection, not the application of force, the platforms it may operate would be inherently dual-use. The same autonomous systems used for seabed mapping could, with different payloads, be used for undersea surveillance (and part of the 'targeting cycle') and or the application of kinetic effects.¹⁷⁰ Therefore, the broader legal and ethical debate surrounding LAWS

Infrastructures, German Aerospace Centre,
https://elib.dlr.de/209985/1/MARESEC_2024_paper_12.pdf accessed 24 August 2025.

¹⁶⁴ Brennan Suffern, 'Collision Regulations Need to be Updated for USVs,' Proceedings, US Naval Institute, Vol 150/2/1452, February 2024,
<https://www.usni.org/magazines/proceedings/2024/february/collision-regulations-need-to-be-updated-usvs> accessed 25 August 2025.

¹⁶⁵ Paul Margat, Michael Staderman, 'The Application of COLREGs by Autonomous and Unmanned Vessels: Issues Raised by Situational Awareness, Night-Time Navigation and Good Seamanship.'

¹⁶⁶ Philip Roche, 'The Collision Regulations and Autonomous Shipping,' Norton Rose Fulbright,
<https://www.nortonrosefulbright.com/en/knowledge/publications/5fedab67/the-collision-regulations-and-autonomous-shipping> accessed 14 September 2025; *Evergreen Marine (UK) Ltd. v Nautical Challenge LTD [2018] EWCA Civ 2173*,
<https://www.supremecourt.uk/cases/uksc-2018-0216> accessed 14 September 2025.

¹⁶⁷ Paul Margat, Michael Staderman, 'The Application of COLREGs by Autonomous and Unmanned Vessels: Issues Raised by Situational Awareness, Night-Time Navigation and Good Seamanship.'

¹⁶⁸ For Australian tort liability during wartime, see *Shaw Savill and Albion Co Ltd v Commonwealth* 88 CLR 163 [1953] HCA 24; Dr Anthony Marinac, 'Two Minute Case Notes, Shaw Savill & Albion (Negligence under another duty),'
<https://www.youtube.com/watch?v=7FrDR8ef5XU> accessed 14 September 2025.

¹⁶⁹ Brennan Suffern, 'Collision Regulations Need to be Updated for USVs.'

¹⁷⁰ Ken Crowe, 'Use of Unmanned Systems by the Australian Defence Force,' Northrop Grumman Australia, 2 January 2015,

provides an essential context for the workforce transformation if such activities were to be contemplated. Australia's position is that any use of autonomy in weapon systems must comply with international humanitarian law, particularly the principles of distinction, proportionality, and precautions in attack.¹⁷¹ This necessitates a robust legal review of all new weapon systems and, crucially, requires a level of human involvement sufficient to ensure accountability.¹⁷²

The concept of 'meaningful human control' is central to this debate.¹⁷³ Even if such autonomous systems were not to be dual-purpose weapons, meaningful human control would be directly relevant to any future hydrographic specialist. This would ensure accountability and the quality assurance of data gathered. The future hydrographic operators transition to roles supervising multiple autonomous systems, requires their training and doctrine to equip them to exercise control effectively. They must understand the capabilities and limitations of the AI, recognise when to trust its outputs, and know when and how to intervene. This is the essence of effective HMT.¹⁷⁴ The ethical obligation to ensure human accountability for the actions of a machine cannot be delegated to the machine itself. Therefore, the doctrinal and regulatory frameworks must be designed not only to enable the technology but to empower the human operator, ensuring they remain the responsible and accountable agent at the centre of the system.

The path to a fully realised, autonomy-enabled hydrographic capability is paved with more than just technological and workforce challenges. It requires a concerted effort to modernise the doctrinal, legal, and ethical frameworks that govern maritime operations. The RAN's strategic policies have set a clear and ambitious direction, but the detailed operational doctrine is still in development. More critically, the national and international legal systems are arguably lagging, creating ambiguity and risk for the very personnel tasked with operating these new systems. For a transformed hydrographic workforce to operate with confidence and effectiveness, they need more than just advanced skills and equipment; they need clear rules, modern laws, and a robust ethical framework that is fit for the autonomous age.

<https://www.aph.gov.au/DocumentStore.ashx?id=7f6210ae-58bd-4f53-a3c9-de159ada93cb&subId=303202> accessed 14 September 2025.

¹⁷¹ 'Australia's Submission to the United Nations Secretary-General's Report on Lethal Autonomous Weapons Systems,' Australian Government, Department of Foreign Affairs and Trade, RE: ODA -2024 -00019/LAWS May 2024, [https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_\(2024\)/78-241-Australia-EN.pdf](https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_(2024)/78-241-Australia-EN.pdf) accessed 14 September 2025.

¹⁷² Australia's Submission to the United Nations Secretary-General's Report on Lethal Autonomous Weapons Systems,' Australian Government, Department of Foreign Affairs and Trade.

¹⁷³ Parliament of Australia, 'Chapter 5 - Artificial Intelligence and Autonomous Weapons related issues,' https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/DefenceAR2022-23/Inquiry_into_the_Defence_Annual_Report_2022-23/Chapter_5_-_Artificial_Intelligence_and_Autonomous_Weapons_related_issues accessed 14 September 2025.

¹⁷⁴ Raphael Briant, 'Human Machine Teaming and the Future of Air Operations,' ifri, 23 September 2021, <https://www.ifri.org/en/studies/human-machine-teaming-and-future-air-operations> accessed 14 September 2025.

This page is intentionally blank

Chapter 8: Conclusion: Navigating the Future

The strategic landscape of the Indo-Pacific, as redefined by the DSR and the NDS, has set the Royal Australian Navy (RAN) on an irreversible course towards a future defined by disruptive technologies.¹⁷⁵ The modernisation of the RAN's hydrographic capability has emerged not as a niche technical upgrade, but should be seen as a foundational enabler for the nation's maritime strategy of denial. This thesis has confronted the pivotal challenge accompanying this technological change, addressing the core research question: *How would the integration of autonomous systems and artificial intelligence (AI) in the Royal Australian Navy's hydrographic capability impact workforce transformation?* The central argument, substantiated through the preceding analysis and discussion, is that the introduction of autonomous platforms and AI-driven analytics necessitates a profound and holistic transformation of the RAN's specialist hydrographic workforce. This transformation is not a simple matter of procurement and retraining; it is a complex, multi-layered challenge that demands a fundamental reimagining of professional identity, skills, career pathways, organisational culture, and the entire ecosystem that supports the capability.

Synthesis of Findings

This thesis began by setting out the inescapable strategic context. The DSR's recommendation for a 'focused force' optimised for deterrence in Australia's northern



Image: Department of Defence

approaches places a premium on superior environmental knowledge.¹⁷⁶ As Chapter 2 argued, the ability to enact denial at sea through effective anti-submarine and anti-surface warfare is impossible without the detailed, timely, and accurate geospatial intelligence that military hydrography provides. The character of modern maritime competition, increasingly conducted in the 'grey-zone', further amplifies the need for uncrewed systems that

can gather intelligence with persistence and scalability, without the escalatory risk of high-value, crewed platforms.¹⁷⁷ This strategic imperative is the primary driver of the modernisation effort.

The technological enablers for this new form of hydrography, as detailed in Chapter 3, are maturing rapidly. The dual streams of RAS for data acquisition and AI for data processing are fundamentally altering the nature of the work. AUVs and USVs offer the ability to operate persistently in hazardous environments, while AI and machine learning are becoming essential tools to manage the resultant 'data deluge' and accelerate the timeline from data collection to actionable intelligence.¹⁷⁸ This technological shift has

¹⁷⁵ Defence Strategic Review 2023, pgs 19, 66; 2024 National Defence Strategy pgs 4, 35.

¹⁷⁶ Defence Strategic Review 2023, pg 53.

¹⁷⁷ Anthony Robertson, 'What is grey-zone confrontation and why is it important?' The Cove, 18 July 2022, <https://cove.army.gov.au/article/what-grey-zone-confrontation-and-why-it-important> accessed 27 September 2025.

¹⁷⁸ Matthew Woodlief. 'Unlock Insights from Hydrographic Data With GeoAI'. *The*

catalysed a move away from the legacy, platform-centric model of the *Leeuwin* and *Paluma*-class survey ships, as outlined in Chapter 1. The RAN's current trajectory, validated by the comparative analysis of allied experiences in Chapter 4, is towards a capability-centric model. This model is defined by small, agile, and deployable units like the Deployable Geospatial Support Teams, equipped with a 'tool-kit' of systems (yet to be fully optimized with scalable autonomous systems), but a concept remarkably similar to the Royal Navy's Hydrographic Exploitation Group.¹⁷⁹

At the heart of this thesis, Chapter 5 argued that this new capability model is contingent upon a radical workforce transformation. The professional identity of the hydrographic specialist is evolving from that of a mariner, whose expertise was forged at sea, to that of a technologist—a multi-domain systems operator, data scientist, and AI interpreter. This shift creates profound challenges for the RAN's traditional personnel management structures, which have long equated sea time with operational experience and career progression. The new model demands a workforce with advanced competencies in robotics, data science, and systems engineering, skills that are in high demand across the economy, creating significant recruitment and retention challenges.¹⁸⁰ Furthermore, the effective employment of these new systems requires a new operational paradigm of Human-Machine Teaming, demanding new skills in mission-based command, calibrated trust in AI, and the management of cognitive load.¹⁸¹ This, in turn, risks creating a cultural rift between the traditional 'warrior' class and this new 'technologist' class, a divide that only deliberate, senior-leader-led action can bridge.

This transformation does not occur in isolation. As Chapter 6 assessed, it is dependent on a supporting national ecosystem of industry, research, and innovation. The HydroScheme Industry Partnership Program is a strategic strength, growing sovereign industrial capacity and allowing the uniformed workforce to focus on military-specific tasks.¹⁸² However, it also presents a strategic risk: the potential atrophy of core military survey skills if not carefully managed. The national research and development base, including the DSTG and the TAS DCRC, provides the essential engine for innovation, while new mechanisms like the Advanced Strategic Capabilities Accelerator offer a pathway to overcome the traditional 'valley of death' in defence procurement.¹⁸³ Finally,

International Hydrographic Review 30 (1). 30 March 2025.

<https://journals.lib.unb.ca/index.php/ihr/article/view/34742> accessed 27 September 2025.

¹⁷⁹ 'New Hydrographic Unit harnesses tech to revolutionise surveying and data gathering,' Royal Navy, 4 June 2025,

<https://www.royalnavy.mod.uk/news/2025/june/04/20250604-new-hydrographic-unit> accessed 27 September 2025.

¹⁸⁰ Bec Shrimpton, Zach Lambert, Australian Strategic Policy Institute, 'Regional Security and Pacific Partnerships: Recruiting Pacific Islanders into the Australian Defence Force', (Canberra: ASPI, 25 April 2024),

<https://www.aspi.org.au/report/regional-security-and-pacific-partnerships-recruiting-pacific-islanders-australian-defence> accessed 9 August 2025.

¹⁸¹ Sidharth Kaushal et al., 'Leveraging Human-Machine Teaming: An Offset Strategy Primer and Policy Guide,' RUSI, Special Competitive Studies Project, January 2024, <https://static.rusi.org/human-machine-teaming-sr-jan-2024.pdf> accessed 18 August 2025.

¹⁸² Australian Hydrographic Office, 'HydroScheme Industry Partnership Program,' Department of Defence, <https://www.hydro.gov.au/NHP/hipp.htm> accessed 8 June 2025.

¹⁸³ Jennifer Jackett, 'Defence innovation and the Australian national interest,' Black Swan Strategy Issue 9, June 2023, (Perth: Defence & Security Institute, University of Western Australia), <https://defenceuwa.com.au/wp-content/uploads/2024/10/Black->

Chapter 7 highlighted the most significant constraint on this entire enterprise: the 'soft infrastructure' of policy, doctrine, and regulation. While high-level strategy is aligned, operational doctrine is immature. Further, the national and international legal frameworks, conceived for a world of crewed vessels, are lagging behind the pace of technology, creating legal ambiguity and operational risk.¹⁸⁴

Answering the Research Question: A Holistic Transformation

The integration of autonomy and AI impacts the RAN's hydrographic workforce transformation across its entire structure. Due to the presently low uptake of autonomy in the service, the impacts and challenges are yet to be understood and absorbed. It is a holistic challenge that touches every aspect of the human capability, from the individual sailor to the strategic management of the specialisation. The impact is a fundamental shift from a workforce that *operated* equipment to one that *commands* systems; from a culture that valued time at sea to one that must value technical mastery; and from an organisation structured around platforms to one structured around deployable, mission-configurable capabilities. The transformation is therefore not merely technical, but cognitive, cultural, and organisational. Success is not guaranteed by the acquisition of AUVs; it will be determined by the Navy's ability to cultivate the human talent to employ them effectively.

Recommendations for Navigating the Future

Based on the analysis conducted in this thesis, five high-level, principle-based recommendations are offered to guide the RAN in navigating this complex transformation. These are not prescriptive solutions but strategic lines of effort intended to address the core challenges identified.

1. **Radically Reform Career Management for Technical Specialists.** The RAN must ensure that legacy career models are adapted if ill-suited to a technology-centric workforce. It should design and implement a dedicated career pathway for technical specialists, including hydrographic personnel. This new pathway must value and reward demonstrated technical mastery, the attainment of advanced qualifications in fields like data science and robotics, and successful command of complex autonomous missions. This may involve creating specialist pay scales, offering continuation bonuses tied to specific skills, and establishing clear trajectories to senior leadership for those who excel in the technical domain, ensuring their expertise is retained and integrated at the highest levels of operational planning.¹⁸⁵

2. **Champion a Deliberate, Leader-Led Cultural Shift.** Cultural change cannot be delegated; it must be driven from the top. The senior leadership of the RAN must actively and visibly champion the value of the 'technologist' class. This requires more than rhetoric; it demands tangible actions. Senior leaders should ensure these specialists are embedded in operational planning staffs, that their data-driven insights are demonstrably valued in decision-making processes, and that their unique operational contributions—whether from a shore-based control centre or a vessel of opportunity—are recognised and celebrated with the same vigour as traditional feats of seamanship. This will be critical to breaking down the cultural friction between the 'warrior' and

[Swan-Strategy-Paper-9 -Defence-Innovation-and-the-Australian-National-Interest_Jennifer-Jackett.pdf](#) accessed 16 August 2025.

¹⁸⁴ Brennan Suffern, 'Collision Regulations Need to be Updated for USVs.'

¹⁸⁵ Angela Clague, 'Expanding the Career Track for U.S. Department of the Air Force Officers to Include Technical Specialists,' RAND Corporation, 5 February 2025, https://www.rand.org/pubs/research_reports/RRA2997-1.html accessed 27 September 2025.

'technologist' and fostering a truly integrated force.¹⁸⁶ This is arguably already underway in the information warfare and cyber workforces, so it is not a stretch to apply this across other fields.

3. **Forge an Integrated and Advanced Training and Education Pipeline.**

Although the ad-hoc upskilling of personnel might be necessary in the short term to identify and optimize the most appropriate training and training pathways for technologists, it will be insufficient in the medium to long term. The RAN must establish a formal, integrated training and education pipeline that builds the hydrographic specialist of the future from enlistment/appointment to separation. This pipeline should blend foundational naval and mariner skills with a mandatory, career-long stream of advanced technical education. This requires deepening partnerships with academic institutions like the Australian Maritime College and creating funded pathways for personnel to attain postgraduate qualifications in critical fields. Given the civilian hydrographic sector is already grappling with autonomy and AI advances, it is anticipated that the civilian training and standards can be adopted to a large degree. Serious thinking will be required to ensure that the civilian standards remain appropriate to the militarized use of such technologies.

4. **Lead the Modernisation of Maritime Law and Doctrine.** The RAN cannot afford to be a passive observer in the evolution of maritime law. It must proactively influence, both nationally with the Australian Maritime Safety Authority and internationally through the International Hydrographic Organization and International Maritime Organization, the modernization of the regulatory frameworks governing autonomous vessels, particularly the COLREGs. Concurrently, but perhaps more importantly, it must accelerate the development of its own tactical-level doctrine and CONOPS for autonomous hydrographic operations. This requires a dedicated effort, potentially through a specialised experimentation unit, to wargame scenarios, test tactics, techniques and procedures, and rapidly codify the lessons observed into practical doctrine, such that they become lessons learned which empower the workforce to operate with legal and operational clarity.¹⁸⁷

5. **Actively Manage the Sovereign Skill Base.** The partnership with industry through HIPP is a strategic asset, but it must be managed with a clear-eyed view of its risks. The RAN must implement a formalised program to ensure its uniformed personnel retain and develop high-end, complex survey skills, particularly those required for contested military operations. The AHO needs to ensure there is a cadre of highly skilled 'intelligent customers' capable of sophisticated contract management and data quality assurance. It also requires ensuring that DGSTs and other military teams are regularly assigned complex survey tasks that maintain their proficiency, preventing the atrophy of the sovereign military expertise that remains the ultimate guarantor of the capability in a crisis.¹⁸⁸

Limitations and Areas for Future Research

This thesis has been constrained by its reliance on publicly available information, precluding access to classified Defence planning documents that could provide a more

¹⁸⁶ Australian National Audit Office, Defence's Implementation of Cultural Reform, Report No. 33 (2020-21) (Canberra: ANAO, 2021), see paragraphs 1.3-1.4 in 'Background', 20 May 2021, <https://www.anao.gov.au/work/performance-audit/defence-implementation-cultural-reform> accessed 27 September 2025.

¹⁸⁷ Royal Australian Navy, RAS-AI Campaign Plan 2025 (Canberra: Department of Defence, 2024), pg 7.

¹⁸⁸ Australian National Audit Office, Maximising the Value of Australian Industry Participation, Report No. 15 (2022-23) (Canberra: ANAO, 2022).

granular view of the workforce challenges and current workforce planning. Furthermore, as noted earlier, the analysis represents a snapshot in time in a field characterised by rapid technological and strategic change. Several areas warrant further, dedicated research. A detailed quantitative analysis of the current and projected skill gaps within the hydrographic workforce would provide invaluable data for planners. A longitudinal study of HIPP's long-term impact on the RAN's sovereign skill base would be critical to validating or adjusting the current industry partnership model. Finally, a comparative analysis of the workforce transformation strategies of other middle-power navies with advanced hydrographic capabilities, such as those of France or Canada, could yield further valuable insights and lessons for the RAN.

In conclusion, the RAN has correctly identified the strategic and technological necessity of modernising its hydrographic capability, albeit the acquisition project SEA1905 has been cancelled due to other priorities. Regardless, a bold and necessary transformation will be forced upon the hydrographic service, already having moved from the crewed platforms of the past to concentrate on purely military surveying, to leveraging off the autonomous systems of the future. However, this thesis has argued that the ultimate success of this endeavour will not be measured by the sophistication of the machines acquired, but by the Navy's commitment to transforming the most critical component of its capability: its people. Navigating the complex currents of this change requires more than a new chart; it requires a new kind of mariner—a technologist, a data scientist, and a mission commander, empowered by a supportive culture, a modernised career structure, and a clear policy and, to a lesser extent, legal framework. The future of hydrography is human-machine teaming, and it is only by investing in the human as deliberately as the machine that the RAN will secure the decisive strategic advantage it seeks.

This page is intentionally blank

Bibliography

Ablong, Marc. "OPINION | Understanding the cost of Australia's naval defence." *Baird Maritime*, 30 May 2025. <https://www.bairdmaritime.com/security/naval/opinion-understanding-the-cost-of-australias-naval-defence>.

Admiralty, Hydrographic Department. *Admiralty Manual of Hydrographic Surveying*. Vol. 1. London: Hydrographer of the Navy, 1965.

Advanced Strategic Capabilities Accelerator. "AUKUS Maritime Innovation Challenge 225: undersea communications and autonomy." <https://www.asca.gov.au/current-activities/aukus-maritime-innovation-challenge-2025-undersea-communications-autonomy>.

Advanced Strategic Capabilities Accelerator. "Ghost Shark - Mission Zero." <https://www.asca.gov.au/activities/missions/ghost-shark-mission-zero>.

AMC Search. "The AMSL Team." <https://www.amcsearch.com.au/amsl-team>.

Anderson, David. "Autonomous Ship Laws in Australia." MLAANZ, May 2018. https://www.mlaanz.org/uploads/1/2/1/3/121322722/autonomous_ship_laws_australia.pdf.

Arthur, Gordon. "Australian defence programmes." *Asian Military Review*, 5 June 2025. <https://www.asianmilitaryreview.com/2025/06/australian-defence-programmes/>.

Asia-Pacific Defence Reporter. "The Advanced Strategic Capabilities Accelerator is up and running to drive defence innovation." 5 July 2023. <https://asiapacificdefencereporter.com/the-advanced-strategic-capabilities-accelerator-is-up-and-running-to-drive-defence-innovation/>.

AusSeabed. "Australian's National Hydrographic Surveying has Evolved - HIPP has arrived." *February 2021 Newsletter*. https://www.ausseabed.gov.au/data/assets/pdf_file/0005/106934/February_2021_Newslatter22.pdf.

Australian Defence Force Careers. "Hydrographic Surveyor." <https://www.adfcareers.gov.au/jobs/navy/hydrographic-surveyor>.

Australian Defence Magazine. "HMAS Melville to be decommissioned." 22 July 2024. <https://www.australiandefence.com.au/news/news/hmas-melville-to-be-decommissioned>

Australian Government. "Australia's Submission to the United Nations Secretary-General's Report on Lethal Autonomous Weapons Systems." Department of Foreign Affairs and Trade, May 2024. [https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_\(2024\)/78-241-Australia-EN.pdf](https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_(2024)/78-241-Australia-EN.pdf).

Australian Government. *2024-28 Defence Corporate Plan*. Canberra: Commonwealth of Australia, 2024. <https://previewapi.transparency.gov.au/delivery/assets/80a82ed1-3e33-027b-b7e0-6493f97f18f8/84004b0f-9f70-4bf9-a2d9-3b1e72296630/2024-25%20Department%20of%20Defence%20Corporate%20Plan.pdf>.

Australian Government, Department of Defence. *2020 Defence Strategic Update*. Canberra: Department of Defence, 2020. <https://www.defence.gov.au/about/strategic-planning/2020-defence-strategic-update>.

Australian Government, Department of Defence. *2024 National Defence Strategy*. Canberra: Department of Defence, 2024. <https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program>.

Australian Government, Department of Defence. *Defence Strategic Review*. Canberra: Department of Defence, 2023. <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>.

Australian Government, Federal Register of Legislation. *Marine Safety (Domestic Commercial Vessel) National Law Act 2012 (Cth)*. <https://www.legislation.gov.au/C2012A00121/latest/text>.

Australian Government, Federal Register of Legislation. *Navigation Act 2012 (Cth)*. <https://www.legislation.gov.au/C2012A00128/latest/text>.

Australian Government, Federal Register of Legislation. *Work Health and Safety Act 2011 (Cth)*. <https://www.legislation.gov.au/C2011A00137/latest/text>.

Australian Government, Office of National Intelligence, 'The Role of Intelligence,' <https://www.oni.gov.au/news/role-intelligence>.

Australian Government, National Intelligence Community. "Australian Geospatial-Intelligence Organisation." <https://www.intelligence.gov.au/agencies/ago>.

Australian Hydrographic Office. "100 years of hydrography in Defence." Canberra: Australian Hydrographic Office, 2020. <https://www.hydro.gov.au/aboutus/AHO2020/100-years-of-hydrography-in-defence.pdf>.

Australian Hydrographic Office. "About Us." Department of Defence. <https://www.hydro.gov.au/aboutus/aboutus.htm>.

Australian Hydrographic Office. "Governance." Department of Defence. <https://www.hydro.gov.au/aboutus/governance.htm>.

Australian Hydrographic Office. "HydroScheme 2025." ArcGIS StoryMaps. <https://storymaps.arcgis.com/stories/4eebeb4ac3a34f47a7699e63f006ca28>.

Australian Hydrographic Office. "HydroScheme Industry Partnership Program." Department of Defence. <https://www.hydro.gov.au/NHP/hipp.htm>.

Australian Hydrographic Office. *National Report Australia to the 21st Meeting of the SWPHC*. Wollongong, NSW: AHO, 2023.

Australian Hydrographic Office. "Our Role." <https://www.hydro.gov.au/aboutus/what.htm>.

Australian Hydrographic Office. "Roles and Responsibilities." Department of Defence. <https://www.hydro.gov.au/aboutus/roles.htm>.

Australian Hydrographic Office. "What is Hydrography?" <https://www.hydro.gov.au/aboutus/what.htm>.

Australian Maritime Safety Authority. "AMSA policy on regulatory treatment of uncrewed and/or autonomous vessels." 20 February 2020. <https://www.amsa.gov.au/vessels-operators/domestic-commercial-vessels/amsa-policy-regulatory-treatment-uncrewed-and-or>.

Australian Maritime Safety Authority. "Autonomous vessels in Australia." 24 August 2022. <https://www.amsa.gov.au/vessels-operators/domestic-commercial-vessels/autonomous-vessels-australia>.

Australian National Audit Office. *Defence's Implementation of Cultural Reform*. Report No. 33 (2020-21). Canberra: ANAO, 2021. <https://www.anao.gov.au/work/performance-audit/defence-implementation-cultural-reform>.

Australian National Audit Office. *Maximising Australian Industry Participation Through Defence Contracting*. Audit Report No. 25 2024-25. Canberra: ANAO, 2025. <https://www.anao.gov.au/work/performance-audit/maximising-australian-industry-participation-through-defence-contracting>.

Australian National Audit Office. *Maximising the Value of Australian Industry Participation*. Report No. 15 (2022-23). Canberra: ANAO, 2022.

Bachari-Lafteh, Mohammadreza, and Abbas Harati-Mokhtari. "Operator's Skills and Knowledge Requirement in Autonomous Ships Control Centre." *Journal of International Maritime Safety, Environmental Affairs, and Shipping* 5, no. 2 (2021): 74-84. <https://doi.org/10.1080/25725084.2021.1949842>.

Blenkin, Max. "ANAO reports on AIP." *Australian Defence Magazine*, 23 May 2025. <https://www.australiandefence.com.au/news/news/anao-reports-on-aip>.

BlueZone Group. "SEA 1770 Rapid Environmental Assessment." <https://bluezonegroup.com.au/sea-1770-rapid-environmental-assessment/>.

Briant, Raphael. "Human Machine Teaming and the Future of Air Operations." ifri, 23 September 2021. <https://www.ifri.org/en/studies/human-machine-teaming-and-future-air-operations>.

Centre for Naval Analyses. "Addressing AI's Operational Challenges: Putting the Human in Human-Machine Teaming." Arlington, VA: CNA, 2021. <https://www.cna.org/reports/2021/10/Addressing-AIs-Operational-Challenges-Putting-the-Human-in-Human-Machine-Teaming.pdf>.

Clague, Angela. "Expanding the Career Track for U.S. Department of the Air Force Officers to Include Technical Specialists." RAND Corporation, 5 February 2025. https://www.rand.org/pubs/research_reports/RRA2997-1.html.

Coda Octopus. "Seabed Classification." <https://www.codaoctopus.com/other-products/geo/seabed-classification>.

Crowe, Ken. "Use of Unmanned Systems by the Australian Defence Force." Northrop Grumman Australia, 2 January 2015. <https://www.aph.gov.au/DocumentStore.ashx?id=7f6210ae-58bd-4f53-a3c9-de159ada93cb&subId=303202>.

Davis, Sam, et al. "Innovation Catalyst: ASCA, Accelerating technology development and capability delivery through superior process and reduced barrier partnerships."

Defence Industry Leadership Program Research Paper, November 2023.
<https://dtc.org.au/files/documents/DILP-Research-Papers/2023/Innovation-Catalyst.pdf>.

Defence Connect. "Navy celebrates launch of next-gen survey boat capability." 9 November 2020. <https://www.defenceconnect.com.au/naval/7148-navy-celebrates-launch-of-next-gen-survey-boat-capability>.

Defence Science and Technology. *DST Capability Portfolio*. Canberra: Department of Defence, 2017.
https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST%20Capability%20Portfolio_051017.pdf.

Defence Science and Technology Group. "About." <https://www.dst.defence.gov.au/>.

Department of Defence. "Equipping the Royal Australian Navy with next generation autonomous undersea vessels." Media release, 10 September 2025.

Department of Defence. "Hydroscheme industry partnership program commences." Media release, 26 February 2020. <https://www.defence.gov.au/news-events/releases/2020-02-26/hydroscheme-industry-partnership-program-commences>.

Defence Annual Report 2023-24.
<https://www.transparency.gov.au/publications/defence/department-of-defence/department-of-defence-annual-report-2023-24/chapter-2--departmental-overview/nations-combine-on-mine-warfare-activity>.

Department of Defence. "Navy team surveys Tonga below the waterline." Media release, 18 February 2022. <https://www.defence.gov.au/news-events/news/2022-02-18/navy-team-surveys-tonga-below-waterline>.

Department of Defence. "The establishment of the Advanced Strategic Capabilities Accelerator." Media release, 1 May 2023.
<https://www.dst.defence.gov.au/news/2023/05/01/establishment-advanced-strategic-capabilities-accelerator>.

Department of Defence. "Working to protect undersea infrastructure." Media release, 14 February 2025. <https://www.defence.gov.au/news-events/news/2025-02-14/working-protect-undersea-infrastructure>.

Department of Defence, Defence Science and Technology Group. "Laser Airborne Depth Sounder (LADS)." <https://www.dst.defence.gov.au/innovation/laser-airborne-depth-sounder-lads>.

Dey, Harshita. "Analysis of Australia's National Defence Strategy 2024." National Maritime Foundation, 20 May 2024. https://maritimeindia.org/wp-content/uploads/2024/05/Harshita-Dey_Analysis-of-Australias-National-Defence-Strategy-2024-pdf.pdf.

Director General Maritime Development. *Leeuwin Class Hydrographic Ship (AGS) HMAS Leeuwin & HMAS Melville, Capability Summary*. Canberra: Royal Australian Navy, n.d. <https://core.ac.uk/download/268171259.pdf>.

Dowse, Andrew. "Australia's Defence Strategy." *Journal of Indo-Pacific Affairs*, 10 September 2024. https://media.defence.gov/2024/Sep/10/2003540653/-1/-1/1/JIPA%20-%20SENIOR_LEADER_PERSPECTIVE_DOWSE.PDF.

DTIC. "Challenges of Autonomous Underwater Vehicles in Military Hydrography." <https://apps.dtic.mil/sti/citations/AD1004191>.

Editorial Team. "New AI tool to streamline bathymetric data cleansing process." *Safety4Sea*, 14 October 2021. <https://safety4sea.com/new-ai-tool-to-streamline-bathymetric-data-cleansing-process/>.

Evergreen Marine (UK) Ltd. v Nautical Challenge LTD [2018] EWCA Civ 2173. <https://www.supremecourt.uk/cases/uksc-2018-0216>.

Ferl, Anna-Katharina. 2023. "Imagining Meaningful Human Control: Autonomous Weapons and the (De-) Legitimisation of Future Warfare." *Global Society* 38 (1): 139–55. doi:10.1080/13600826.2023.2233004.

General Dynamics Mission Systems. "Knifefish Surface Mine Countermeasure UUV." DASC. https://www.dacis.com/nuxt/programs_sample_record.C2v8zz-.pdf.

George, Melissa. "ADF retention bonus scheme." Parliament of Australia, 20 June 2023. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/FlagPost/2023/June/ADF-Retention.

Hains, Denis. "The emergence of AI in hydrography." *Hydro International*, 25 February 2021. <https://www.hydro-international.com/content/article/the-emergence-of-ai-in-the-hydrography-sector>.

Hamden, Mohammad Hanif, and Ami Hassan Md Din. "A review of advancement of hydrographic surveying towards ellipsoidal referenced surveying technique." *IOP Conference Series: Earth and Environmental Science*, Volume 169, 9th IGRSM International Conference and Exhibition on Geospatial & Remote Sensing (IGRSM 2018) 24-25 April 2018, Kuala Lumpur, Malaysia. <https://iopscience.iop.org/article/10.1088/1755-1315/169/1/012019/pdf>.

Ho, Geoffrey, et al. "Human Factors Issues in Unmanned Underwater Vehicles." Toronto: Defence Research and Development Canada, 2011. <https://apps.dtic.mil/sti/tr/pdf/ADA555588.pdf>.

Hoehn, Rob. "How the Royal Australian Navy Nurtures Innovators. *Innovation Management*, 13 July 2020. <https://innovationmanagement.se/2020/07/13/how-the-royal-australian-navy-nurtures-innovators/>.

Horne, Rachel. "Trusted Autonomous Systems, Defence Cooperative Research Centre Submission to the Independent Review of Domestic Commercial Vessel Safety Legislation." 30 March 2022. <https://www.infrastructure.gov.au/sites/default/files/documents/dcvir-submission-7-trusted-autonomous-systems.pdf>.

House of Commons Library. *AUKUS pillar 2: Advanced capabilities*. Research Briefing CBP-9842. London: UK Parliament, 2 September 2024. <https://commonslibrary.parliament.uk/research-briefings/cbp-9842/>.

Hydrographic Service RAN. *Corporate Overview: Hydrographic Service RAN*. Paper presented at the Hydrographic Service RAN Industry Briefing, Wollongong, NSW, 1996. <https://apps.dtic.mil/sti/tr/pdf/ADA322159.pdf>.

International Hydrographic Organisation. "Major Milestone Achieved in Transition to Smart Navigation with Operational Editions of S-100 Standards." 13 January 2025. <https://iho.int/en/major-milestone-achieved-in-transition-to-smart-navigation-with-operational-editions-of-s-100-standards>.

International Hydrographic Organisation. *Standards for Hydrographic Surveys, S-44 Edition 6-1.0*. 2020. https://iho.int/uploads/user/pubs/standards/s-44/S-44_Edition_6.1.0.pdf.

International Institute for Strategic Studies. "Australia's 2023 Defence Strategic Review." *Strategic Comments* 29, no. 12 (2023). <https://www.iiss.org/publications/strategic-comments/2023/australias-2023-defence-strategic-review/>.

Jackett, Jennifer. "Defence innovation and the Australian national interest." *Black Swan Strategy Issue* 9, June 2023. Perth: Defence & Security Institute, University of Western Australia. <https://defenceuwa.com.au/wp-content/uploads/2024/10/Black-Swan-Strategy-Paper-9-Defence-Innovation-and-the-Australian-National-Interest-Jennifer-Jackett.pdf>.

Kardon, Isaac B. "Combating the Grey Zone: Examining Chinese Threats to the Maritime Domain." Carnegie Endowment for International Peace, 4 June 2024. <https://carnegieendowment.org/posts/2024/06/combating-the-gray-zone-examining-chinese-threats-to-the-maritime-domain?lang=en>.

Kaushal, Sidharth, et al. "Leveraging Human-Machine Teaming: An Offset Strategy Primer and Policy Guide." Special Competitive Studies Project, January 2024. <https://static.rusi.org/human-machine-teaming-sr-jan-2024.pdf>.

Keegan, Michael. "Navigating Technological Frontiers in the U.S. Navy." IBM Center for The Business of Government, 12 June 2024. <https://www.businessofgovernment.org/blog/navigating-technological-frontiers-us-navy>.

Lancaster, Lily. "Royal Australian Navy Joins Its Army's Landing Force." DVIDS, 15 July 2022. <https://www.dvidshub.net/news/425457/royal-australian-navy-joins-its-armys-landing-force>.

Lee, Seojeong, and Hyoseung Kim. "IHO S-100 Data Model and Relevant Product Specification." *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 18, no. 2 (June 2024): 297-301. https://www.researchgate.net/publication/377056086_IHO_S-100_Data_Model_and_Relevant_Product_Specification.

Leidos. *Rapid Environmental Assessment*. Factsheet, Leidos Australia, September 2019. <https://www.leidos.com/sites/leidos/files/2019-09/FS-Rapid-Environmental-Survey.pdf>.

Leidos Australia. "Leidos Australia To Deliver Key Milestone For SEA1770." PR Newswire, 8 October 2019. <https://enmobile.prnasia.com/releases/global/leidos-australia-to-deliver-key-milestone-for-sea1770-259877.shtml>.

"Leidos Australia to Deliver Survey Craft for SEA1770." *Offshore Energy*, 8 October 2019. <https://www.offshore-energy.biz/leidos-australia-to-deliver-survey-craft-for-sea1770/>.

Lemon, Nick. "Autonomous shipping from a regulatory perspective." IALA. <https://www.iala-aism.org/content/uploads/2018/01/12.00-Nick-Lemon-Autonomous-shipping-from-a-regulatory-perspective.pdf>.

Liivoja, Rain, and Valjatage, Ann. (eds.) "Autonomous Cyber Capabilities under International Law." 2021, NATO Cooperative Cyber Defence Centre of Excellence.

Marinac, Anthony. "Two Minute Case Notes, Shaw Savill & Albion (Negligence under another duty)." YouTube video, 1:59. <https://www.youtube.com/watch?v=7FrDR8ef5XU>.

Margat, Paul, and Michael Staderman. "The Application of COLREGs by Autonomous and Unmanned Vessels: Issues Raised by Situational Awareness, Night-Time Navigation and Good Seamanship." Institute for the Protection of Maritime Infrastructures, German Aerospace Centre. https://elib.dlr.de/209985/1/MARESEC%202024_paper_12.pdf.

Minister for Defence. "Investing in Defence's people." Media release, 5 November 2024. <https://www.minister.defence.gov.au/media-releases/2024-11-05/investing-defences-people>.

Moriarty, Greg. "National Defence Strategy." Speech, Air and Space Power Conference, Canberra, May 2024. <https://airpower.airforce.gov.au/sites/default/files/2024-05/Air%20and%20Space%20Power%20Conference%202024%20Transcript%20Mr%20Greg%20Moriarty%20National%20Defence%20Strategy.pdf>.

Nally, Jonathan. "Navy now has only one hydrographic survey ship." *Spatial Source*, 12 August 2024. <https://www.spatialsource.com.au/navy-now-has-only-one-hydrographic-survey-ship/>.

Naval Historical Society of Australia. "HMA Ships Paluma and Mermaid decommissioned." *Call The Hands: NHSA Newsletter*, no. 58 (November 2021): 4. https://nhsa-cth.s3.ap-southeast-2.amazonaws.com/Call+The+Hands_NHSA+Newsletter_Issue+58_Nov+21.docx.pdf.

Naval Meteorology and Oceanography Command. "Naval Oceanographic Office." <https://www.cnmoc.usff.navy.mil/navoceanol/>.

Navy History. "A Brief History of the Australian Hydrographic Service." Royal Australian Navy. <https://navyhistory.au/a-brief-history-of-the-australian-hydrographic-service/>.

Navy Lookout. "Royal Navy launches new Hydrographic Exploitation Group to transform survey operations." 4 June 2025. <https://www.navylookout.com/royal-navy-launches-new-hydrographic-exploitation-group-to-transform-survey-operations/>.

Neelam, Ryan. "Defence and security." *Lowy Institute Poll 2025 Report*, 16 June 2025. <https://poll.lowyinstitute.org/report/2025/defence-and-security/>.

NOAA Ocean Exploration. "Uncrewed Surface Vessels." <https://oceanexplorer.noaa.gov/technology/usv/usv.html>.

Northrop Grumman. "Distributed Autonomy/Responsive Control - DA/RC." <https://www.northropgrumman.com/what-we-do/mission-solutions/distributed-autonomy-responsive-control-da-rc>.

Parliament of Australia. "Chapter 5 - Artificial Intelligence and Autonomous Weapons related issues."

https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/DefenceAR2022-23/Inquiry_into_the_Defence_Annual_Report_2022-23/Chapter_5-Artificial_Intelligence_and_Autonomous_Weapons_related_issues.

Pfau, Andrew. "Preparing Sailors for the Age of AI." *US Naval Institute, Proceedings* 148, no. 4 (April 2022).

<https://www.usni.org/magazines/proceedings/2022/april/preparing-sailors-age-ai>.

Prospects. "Hydrographic surveyor: Job profile." <https://www.prospects.ac.uk/job-profiles/hydrographic-surveyor>.

Robertson, Anthony. "What is grey-zone confrontation and why is it important?" *The Cove*, 18 July 2022. <https://cove.army.gov.au/article/what-grey-zone-confrontation-and-why-it-important>.

Roche, Philip. "The Collision Regulations and Autonomous Shipping." Norton Rose Fulbright.

<https://www.nortonrosefulbright.com/en/knowledge/publications/5fedab67/the-collision-regulations-and-autonomous-shipping>.

Royal Australian Navy. "HMAS Leeuwin (II)."

<https://www.navy.gov.au/capabilities/ships-boats-and-submarines/hmas-leeuwin>.

Royal Australian Navy. "HMAS Paluma (IV)."

<https://seapower.navy.gov.au/history/units/hmas-paluma-iv>.

Royal Australian Navy. "Mission & Values." <https://www.navy.gov.au/about-navy/mission-values>.

Royal Australian Navy. *RAS-AI Campaign Plan 2025*. Canberra: Department of Defence, 2024. <https://www.navy.gov.au/sites/default/files/2024-02/RAS-AI-Campaign-Plan-2025.pdf>.

Royal Australian Navy. *Robotics, Autonomous Systems & Artificial Intelligence (RAS-AI) Strategy 2040*. Canberra: Department of Defence, 2020. <https://www.navy.gov.au/sites/default/files/2024-02/RAS-AI-Strategy-2040.pdf>.

Royal Navy. "Royal Navy leads AUKUS trials to improve use of autonomous systems." 24 June 2025. <https://www.royalnavy.mod.uk/news/2025/june/24/20250624-aukus-data-sharing-exercise>.

Royal Navy. "Royal Navy trials underwater gliders that can aid submarine hunters." 30 April 2020. <https://www.royalnavy.mod.uk/news/2020/april/30/300420-glider-trials>.

Royal Navy News. "New Hydrographic Unit harnesses tech to revolutionise surveying and data gathering." Royal Navy, 4 June 2025. <https://www.royalnavy.mod.uk/news/2025/june/04/20250604-new-hydrographic-unit>.

Sea Machines Robotics (BLOG). "Guide to Autonomous Vessels for Hydrographic Survey in 2024." 26 June 2024. <https://sea-machines.com/guide-to-autonomous-vessels-for-hydrographic-survey-in-2024/>.

Sebastian, Susan, et al. "AUVs in Hydrography: Integrating Autonomous Underwater Vehicle Capability into Hydrographic Operations." *Hydro International*, 26 July 2016. <https://www.hydro-international.com/content/article/auvs-in-hydrography>.

SevenCs. "S-100 Universal Hydrographic Data Model." <https://www.sevencs.com/enc-production-tools/s-100-data-model/>.

Shaw Savill and Albion Co Ltd v Commonwealth 88 CLR 163 [1953] HCA 24.

Shrimpton, Bec and Zach Lambert. *Regional Security and Pacific Partnerships: Recruiting Pacific Islanders into the Australian Defence Force*. Canberra: ASPI, 25 April 2024. <https://www.aspi.org.au/report/regional-security-and-pacific-partnerships-recruiting-pacific-islanders-australian-defence>.

Singh, Abhijit. "Deciphering Grey-Zone Operations in Maritime-Asia." Observer Research Foundation, August 2018. <https://www.orfonline.org/public/uploads/posts/pdf/20230523093408.pdf>.

Suffern, Brennan. "Collision Regulations Need to be Updated for USVs." *Proceedings*, US Naval Institute, Vol 150/2/1452, February 2024. <https://www.usni.org/magazines/proceedings/2024/february/collision-regulations-need-be-updated-usvs>.

Teledyne CARIS. "The data processing challenge." IHO. https://iho.int/uploads/user/Inter-Regional%20Coordination/RHC/SEPRHC/SEPRHC13/CHRPSE13-2.5.2-CARIS_Onboard.pdf.

Tesch, Peter. "AUKUS: Two pillars, three fallacies." *The Interpreter*, Lowy Institute, 2 October 2024. <https://www.lowyinstitute.org/the-interpreter/aukus-two-pillars-three-fallacies>.

Trabucco, Lena. "AI-Enabled Autonomous Weapons and Human Control, Part 1: Human Control and Machine Learning Design and Development." *International Law Studies*, The United States Naval War College, Vol 106 (2025): 534-565. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3115&context=ils>.

Trabucco, Lena. "What is Meaningful Human Control? Cracking the Code on Autonomous Weapons and Human Judgment." Modern War Institute at West Point, 21 September 2023. <https://mwi.westpoint.edu/what-is-meaningful-human-control-anyway-cracking-the-code-on-autonomous-weapons-and-human-judgment/>.

Trusted Autonomous Systems. "About." <https://tas.tech/>.

United Kingdom, Admiralty. "How S-100 will shape the future of navigation." <https://www.admiralty.co.uk/s-100-shaping-future-navigation>.

United States' Department of Commerce, National Oceanic and Atmospheric Administration (NOAA). "The Universal Hydrographic Data Model: What is S-100?" <https://marinenavigation.noaa.gov/s100.html>.

United States of America, Indo-Pacific Command. "Freedom of Navigation Operations (FONOPS) - Peaceful Principled Upholding of Int'l Law (Countering PRC Flawed Narratives)." 106/SJA TACAID Series. <https://www.pacom.mil/Portals/55/Documents/pdf/J06%20TACAID%20-%20FONOPS.pdf?ver=pH6fTE-cpgyhqfBJi2vEKg%3D%3D>.

United States of America National Intelligence Council. "Updated IC Gray Zone Lexicon: Key Terms and Definitions." July 2024. <https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf>.

US Department of Defense. "DoD Directive No. 3000.09: Autonomy in Weapons Systems." 21 November 2012. <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.

US Government Accountability Office. "Littoral Combat Ship: Actions Needed to Address Significant Operational and Sustainment Challenges." GAO-22-105387. Washington, D.C.: GAO, 24 February 2022. <https://www.gao.gov/products/gao-22-105387>.

US Navy. "Littoral Combat Ships - Mine Countermeasures Mission Package." Fact File. <https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167535/littoral-combat-ships-mine-countermeasures-mission-package/>.

US Navy. "Mine Countermeasures Unmanned Surface Vehicle (MCM USV)." Fact File. <https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167996/mine-countermeasures-unmanned-surface-vehicle-mcm-usv/>.

University of South Florida. "Hydrography." <https://www.usf.edu/marine-science/research/hydrography.aspx>.

University of Southern Mississippi. "Hydrographic Science." <https://www.usm.edu/graduate-programs/hydrographic-science.php>.

van der Veen, A. M. C., and M. C. van der Veen. "On the Bridges: Insight Into the Current and Future Use of Automated Systems as Seen by Royal Navy Personnel." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 62, no. 1 (2018): 1545-1549. <https://doi.org/10.1177/1541931218621349>.

Wingrove, Martyn. "New IHO S-100 standards will stimulate new applications." *Riviera Maritime Media*, 3 June 2022. <https://www.rivieramm.com/news-content-hub/news-content-hub/new-iho-s-100-standards-will-stimulate-new-applications-71303>.

Woodlief, Matthew. "Unlock insights from hydrographic data with GeoAI." *The International Hydrographic Review* 30, no. 1 (2025). <https://journals.lib.unb.ca/index.php/ihr/article/view/34742/1882530413>.

Wynn, R. B., et al. "Autonomous Underwater Vehicles (AUVs): Their past, present and future contributions to the advancement of marine geoscience." *Marine Geology* 352 (2014): 451-468. <https://core.ac.uk/download/pdf/19963755.pdf>



ADF
Australian Defence Force

Case Studies in Strategy

Case Study 1: *Lessons for students of strategy from economics – getting the economics of war wrong*

Colonel Phillip Baldoni, CSM

Case Study 2: *Ancient Carthage – Power and Strategy in the Punic Wars*

Colonel Gwilym Leech, CSM

Case Study 3: *Having applied relevant theory and concepts to the Byzantine Empire, what are the most important lessons for students of strategy?*

Warrant Officer David Turnbull, CSC



This section includes a range of case studies written for the Foundations of Strategy and Strategic Art unit. The unit provides course members with the foundational skills and knowledge that underpin the Defence and Strategic Studies Course (DSSC) program. It includes the concept of power with an emphasis on national power, theories of international relations, the meaning and realities of strategy, problem solving techniques and the challenge of wicked problems in the 21st century. Course member explore these concepts through in depth analysis of a historical case study.

Case Study 1: *Lessons for students of strategy from economics – getting the economics of war wrong*

Colonel Phillip Baldoni, CSM

The context of this case study is focused on the US Civil War. The study topic provides course members with an opportunity to consider the application of military power to achieve political outcomes, the role of civil-military relations, and the impact of international context and/or economic factors.

Case Study 2: *Ancient Carthage – Power and Strategy in the Punic Wars*

Colonel Gwilym Leech, CSM

This case study explores why Carthage, a wealthy, powerful and expansive hegemon, failed to meet the threat represented by Rome's rise. It examines how a state that had grown in power and stature for seven centuries could be destroyed in one. It posits that the factors that allow a state to attain power may not enable it to retain power when circumstances change.

Case Study 3: *Having applied relevant theory and concepts to the Byzantine Empire, what are the most important lessons for students of strategy?*

Warrant Officer David Turnbull, CSC

This case study topic offers the opportunity to examine an empire seeking to maintain its place in a very dangerous context. It also allows for an exploration of the use of diplomacy, espionage and economics in order to achieve security outcomes.

About the Authors



Colonel Phil Baldoni enlisted into the Army in 1998 as a Cavalry Trooper and entered the Royal Military College in 2000. He graduated into the Royal Australian Corps of Transport. He has served in a variety of regimental positions in road transport and movements control roles, and was the commanding officer of the 9th Force Support Battalion in 2019-2020. He has also worked in sustainment and logistic support to operations in Army Headquarters, Headquarters Joint Operations Command, and Joint Logistics Command. His operational experience includes deployments to Australian and multi-national headquarters in Iraq and Afghanistan. He graduated from Australian Command and Staff College in 2014, and the Defence Strategic Studies Course in 2025. He holds a Bachelor of Professional Studies with a specialisation in Peace Studies, a Masters of Military and Defence Studies, a Masters of International Relations and a Masters of Business Administration. In 2026, he posted back to Joint Logistics Command as the Commander of Joint Logistics Unit Victoria.



Colonel Gwilym Leech is an Australian Army officer with experience in strategy and policy, operations and plans, concepts and experimentation, force design and international engagement. He is a graduate of the Australian Command and Staff College and a Fellow of the Defence Strategic Studies Course.



Warrant Officer David Turnbull, CSC enlisted in the Royal Australian Air Force in January 1989 as a 15 year old Armament Trade Apprentice. He enjoyed postings to 75 Squadron, 77 Squadron and 3 Squadron, followed by numerous stints within Capability Acquisition and Sustainment Group across acquisition, sustainment and executive roles. Warrant Officer Turnbull currently serves as the Air Mobility Group Warrant Officer. He completed a Bachelor of Administrative Leadership in 2010, Master of Business in 2012, Master of Military and Defence Studies in 2020, and Master of National Security and Strategy – Defence Policy in 2025.



Image: Kurz & Allison. *Assault on Fort Sanders*. Tennessee, 1891. Chicago: Kurz & Allison, Art Publishers. Photograph. <https://www.loc.gov/item/91721203/>.

Case Study 1: Lessons for students of strategy from economics – getting the economics of war wrong

"No, you dare not make war on cotton. No power on earth dares to make war upon it. Cotton is king!"

Sen. John Hammond, South Carolina, 1858¹

Introduction

The American Civil War was fought from 1861 to 1865. It has voluminous literature, perhaps because it can be used as an example of an inflection point in the history of warfare. On the battlefield, Napoleonic era technological limits to communication required soldiers to fight in close-order ranks while facing rifled muskets and artillery that greatly increased lethality². At sea, steam powered and turreted ironclad warships faced sailing ships with muzzle-loaded cannon. Railways and steam ships allowed the movement and sustainment of large armies in multiple theatres, while generals struggled to find a coherent method of forging widely dispersed tactical engagements into a coherent strategy. At the grand strategic level, politicians on both sides developed methods to manage their civil-military relations³. The war was also a contest between the mobilisation of the modern economic systems that fuelled its scope and ferocity. This essay will concentrate on this last aspect: the economic underpinnings of the war effort.

This is not a new area of study – scholarship in the field attributing the causes of the war to Northern economic expansionism date to before the second world war⁴. There is a significant body of literature on the economic conditions and financing of both the Union and Confederate war efforts. Rather than describe lessons for economic strategy (i.e. using the economy as an instrument of national power), this essay will draw out lessons for students of strategy for the use of military power. It does not seek to make economists out of strategists, but aims to show that failure to appreciate the economic underpinning of military power can lead to defeat. This will be shown using the 'influence effect' theory of Albert Hirschman, an influential scholar of the use of economic power in international relations, to demonstrate two points of relevance to students of strategy. The first point relates to the management of important groups inside the strategist's own state, and the second relates to the management of groups within a state that the strategist intends to influence. While not proposing that these points encompass the entire reasons for the Confederacy's defeat, they played a large part and remain relevant to students of strategy today.

To demonstrate this, the reasons that these points remain relevant will be explained through a description of the economic similarities between the time of the Civil War and today. This will show that there is enough in common for a case study of the period to remain relevant. A description will then be given of the three components of Hirschman's influence effect theory and why these are relevant to students of strategy. This will illuminate the link between sub-state actors, economic factors and strategic success or

¹ Quoted by Randall Bedwell, *Brink of Destruction: A quotable History of the Civil War* (Cumberland House, 1999), 20.

² Russell F. Weigley, *A Great Civil War: A Military and Political History, 1861-1865* (Indiana University Press, 2000), XIX.

³ See, for example, Elliot A. Cohen, *Supreme Command* (Simon and Schuster, 2002), 15-51.

⁴ Jane Flaherty, "The Exhausted Condition of the Treasury on the Eve of the Civil War", *Civil War History*, v. 55, n. 2 (2009), 248-249.

failure. Two lessons will then be derived from this framework. The first relates to the Confederacy's poor integration of the economic interests of its most powerful sub-state actors with war aims, showing students of strategy that misaligned interests within a state can contribute to defeat. The second relates to the Confederacy's unsuccessful attempts at economic coercion of its trade partners; showing students of strategy that poor understanding of the sub-state actors inside a target state can be fatal to successful strategy.

Relevance – going from the specific 150 years ago, to the general today

In assessing lessons from studies of the past, students of strategy should be cautious of what lessons they draw. In examining the American Civil War, the student of strategy should question why lessons from a war conducted almost 150 years ago are relevant. In this case, the strategic lessons presented are related to the economic underpinnings of military and national strategy. The international economic conditions of the time have parallels to the present. Unlike the mercantilist international economy of the 18th century, dominated by institutions such as the East India Company, the period of 1846-1870 was an imperfect free trade system much like today⁵. Much as the United States has done in the post-civil war period, it engaged in protectionist practices such as tariffs before the Civil War⁶. While many countries adhered to the now abandoned gold standard for their currencies, neither the Union nor the Confederacy did⁷. Robert O'Brien and Marc Williams note that this international economic system after the Napoleonic wars was "based on liberal principles that are similar to the guiding principles of today's dominant powers and institutions"⁸. These similarities between the systems of then and now provide a valid basis for drawing general lessons from the specific case study.

Theoretical lenses – managing internal and external polities. How domestic interests get a strategic vote

Albert Hirschman is mostly known for his works on the political economy. In an early but influential work, *National power and the structure of foreign trade*, he described several important effects of the use of trade as an instrument of national power. One of these, which will be the focus of this essay, is the 'influence effect'. This is the *political* consequences of engaging in mutually beneficial exchange⁹. Three aspects of the influence effect will be used to provide insight into why Confederate strategy failed.

The first aspect of the influence effect examined is that in any state involved in trade, there will be groups, such as the producers of export goods, for whom the stoppage of trade would be disproportionately disadvantageous. These groups, referred to by Hirschman as 'commercial fifth columns' will exert influence on governments to maintain friendly policies towards states to trading partners¹⁰. To strengthen the link to other elements of strategy, a complementary means of examining the influence of substate actors, selectorate theory, will be introduced. This will be used to explore the effects of two sub-state actors: slave holders inside the Confederacy, and manufacturers inside Britain.

⁵ Robert O'Brien and Marc Williams, *Global Political Economy: Evolution and Dynamics* (Palgrave MacMillan, 5th edition, 2016), 67, 71.

⁶ James H. Nolt, *International Political Economy: The Business of War and Peace* (Taylor & Francis Group, 2013), 118.

⁷ O'Brien and Williams, *Global Political Economy*, 68

⁸ O'Brien and Williams, *Global Political Economy*, 68

⁹ Hirschman, *National Power and the Structure of Foreign Trade*, 16.

¹⁰ Hirschman, *National Power and the Structure of Foreign Trade*, 29.

The second aspect is that an exporting nation has an incentive to put in place policies that make it difficult for the trading partner to dispense with the imports. "A country trying to make the most out of its strategic position with respect to its own trade will try precisely to create conditions which make the interruption of trade of much graver concern to its partners than itself"¹¹. The Confederacy's attempts to leverage its cotton trade as an instrument of strategy will be examined.

The third aspect is that as this trade re-orientation occurs, the economy of the smaller state can become increasingly conditioned on that of the larger.¹² This can result in asymmetrical influence effects as even if the smaller state has made its trade as indispensable as possible, the consequences for interruption for itself are disproportionate. Combined with the second aspect, this will be explored in relation to the Confederate cotton trade with Britain.

Substate actors in the Confederacy – important selectorates and southern financing

To understand the implications of financing on the failure of Confederate strategy, it is necessary to understand some of the underlying factors. The American Civil War has advantages as a case study in strategy due to the relative similarities of the belligerents: both were, by modern standards, imperfect democracies with modern economies.¹³ The Confederacy perpetuated many of the political and economic institutions of the United States after succession. The differences in remaining variables can therefore be instructive.

There were significant differences between Union and Confederate war financing models in three principle areas: Loans, government issued notes, and taxes. The union financed 31% of their war effort with loans, 14% with notes, and 20% with tax revenues. Confederate war funding relied almost exclusively on notes (a massive 54% of total revenue), 19% on loans, and less than 4% through taxes¹⁴. Taxation accounted for less than 1% of Confederate government revenue throughout its short existence¹⁵. The Confederacy's extreme reliance on methods other than taxation had several effects that contributed to strategic failure. The first is that compensating for lack of tax revenue and specie through printing money backed "by nothing but faith" resulted in hyper-inflation that destroyed its economy¹⁶. The second was that the lack of tax revenues posed severe credibility problems in the international money market, resulting in Confederate

¹¹ Hirschman, *National Power and the Structure of Foreign Trade*, 16.

¹² Eric Helleiner, "Economic Foundations of Strategy: Beyond Smith, Hamilton and List," in *The New Makers of Modern Strategy: From the Ancient World to the Digital Age*, ed. Jonathan Kirshner and Hal Brands (Princeton University Press, 2023), 256

¹³ For the Confederacy as a modern economy, using the criteria of Nobel laureate economist Edmund Phelps, see Michael Brem Bonner, *Confederate Political Economy: Creating and Managing a Southern Corporatist Nation*, (LSU Press, 2016), 183. For the trade between imperfect democracies, see Joaquim Ramos Silva, "Trade between asymmetrical democratic countries," *Journal of Economic Studies*, v. 26 n. 4/5 (1999): 412-413.

¹⁴ Rose Razaghian, *Financial Civil War: The Confederacy's Financial Policies, 1861-1864*. Yale ICF Working Paper No. 04-45 (Yale University, Last Revised June 2005), 1.

¹⁵ Donald Stoker, *The Grand Design: Strategy and the U. S. Civil War* (Oxford University Press Incorporated, 2010), 25; and Weigley, *A Great Civil War*, 69.

¹⁶ Stoker, *The Grand Design*, 25; Mark R. Wilson, *The Business of Civil War: Military Mobilization and the State, 1861-1865* (Johns Hopkins University, 2006), 227, puts hyperinflation in the Confederacy at close to 5000% compared to the Union's at around 75% for the same period.

bonds and notes being severely discounted. Only in the final years of the war did the Confederacy enact effective taxation, which was too late¹⁷. The Confederacy's inability to develop an effective wartime finance model, compared to the relative success of the Union¹⁸, directly contributed to its defeat.¹⁹

The Confederacy had reasons to be averse to taxation. The first of these was in Confederate elites' ideological aversion to the concentration of power in federal hands rather than in those of the states²⁰. The second is more prosaic. Taxes on property were the most common form of direct taxation in the antebellum period²¹. The proportion of slaves as a percentage of total property in the Confederacy's 'deep south' states in 1860 averaged 46%, while being significantly lower elsewhere²². Records of voting decisions in the Confederate congress show that proposals for tax on property were most opposed by representatives from deep south states at the beginning of the war. Conversely, deep south states strongly supported such taxation when impending Union victory and emancipation imperiled slavery²³. By this stage of the war, such measures were too late – 'the side with the best credit won'²⁴. It is this second reason, the failure of the Confederacy to align the interests of an internal polity with national aims that is more germane to the lessons for modern students of strategy.

In order to understand the influence of this internal polity, it is useful to combine Hirschman's influence effect with selectorate theory. Selectorate theory offers a way to understand the roles and interests of sub-state actors that expands on the potential 'commercial fifth columns' Hirschman describes. Randolph Silversson and Bruce Bueno de Mesquita are key scholars of this theory. They define a selectorate as a group that leaders require support from to maintain power, and who require public and private goods to do so. Victory is only one such public good²⁵. The majority of slaves in deep south states were involved in cotton production²⁶, which in turn accounted for more than half of United States exports before the war²⁷. The deep south states, comprising seven of the 15 Confederate states, were too powerful a selectorate for the Confederacy's leaders to ignore their wealth production interests²⁸. The public goods required to keep this selectorate aligned with Confederate goals was protection of their ability to generate wealth. Paradoxically, this protection resulted in the Confederacy's diminutive tax revenue, which in turn removed all credibility from its chosen instrument for financing the war – the issue of notes. This crippled its ability to provide the war material it required. By the time that slave states interests in avoiding defeat eclipsed their need

¹⁷ Razaghian, *Financial Civil War*, 21, 28-30.

¹⁸ Razaghian, *Financial Civil War*, 17.

¹⁹ Ariel Ron and Sofia Valeonti. "Money War: Democracy, Taxes and Inflation in the U.S. Civil War," *Cambridge Journal of Economics*, v. 47 n. 2 (2023): 283; Nolt, *International Political Economy*, 131.

²⁰ Razaghian, *Financial Civil War*, 6.

²¹ Razaghian, *Financial Civil War*, 10.

²² Razaghian, *Financial Civil War*, 8-9.

²³ Razaghian, *Financial Civil War*, 28-30.

²⁴ Nolt, *International Political Economy*, 123.

²⁵ Randolph M Silversson and Bruce Bueno de Mesquita. "The Selectorate Theory and International Politics." *Oxford Research Encyclopedia of Politics*. 28 Jun. 2017; accessed 07 March 2025 at <https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-293>

²⁶ Corbett et al, *US History* (OpenStax College, 2021), 289.

²⁷ O'Brien and Williams, *Global Political Economy*, 65.

²⁸ Bruce Bueno de Mesquita et al, "Testing Novel Implications from the Selectorate Theory of War." *World Politics*, v. 56, no. 3 (April) (2004):370.

to protect wealth generation (i.e. the needs of the selectorate were aligned with the needs of leaders' strategy), it was too late to effect the outcome of the war. The lesson for students of strategy here is that *enacting effective strategy requires a state to align the aims of its selectorates*.

Substate actors in Britain – important selectorates and asymmetric trade relationships

While the previous lesson concentrated on managing domestic sub-state actors, the next lesson for students of strategy provides an example of the impacts of failing to correctly diagnose the interests of external substate actors. In this case, the example used will be the Confederacy's miscalculation of Britain's interests in the war. Here, the Confederacy badly misjudged domestic factors in Britain, which (like the financing failure described above, contributed to its eventual defeat. Hirschman's influence effect will be used to explain this outcome.

The Confederacy had good reason to believe that cotton could contribute to leverage with European powers. After succession, it controlled most of the United States' cotton producing land. Europe, and Britain in particular, were highly dependent on Southern cotton. In 1860, some 67 - 87% of raw cotton stock in Britain was from the United States, with the overwhelming majority from Confederate states²⁹. The cotton crop of 1861 was worth almost 10 times the amount of gold held by southern states, providing huge potential for securing war materiel³⁰. In addition, Britain's leaders were at best ambivalent to both the Union and the Confederacy³¹. Confederate leaders almost assumed that this reliance could be leveraged to secure recognition of the Confederacy, resulting in more substantial military aid and pressure on the Union to negotiate³². From the start of the war, these assumptions proved to be false.

The Confederacy made several misjudgments in its attempts to use the cotton trade for international leverage. In the first year of the war, an incoherent financial policy resulted in the Confederacy buying cotton to use as leverage for credit abroad, but it then failed to legislate against state-level and local unofficial embargoes. This provided an irritant in its attempts at diplomacy, exploited by the Union in claims that the Confederacy was employing this as an official policy³³. When the Union announced a blockade of Confederate ports, abnormally high stocks already held in Britain provided a buffer from the stoppage of trade³⁴. By 1863, cotton was flowing into Britain from other countries³⁵. British leaders, already unimpressed and irritated by clumsy Confederate diplomacy, were not coerced³⁶. "No Parliament could stomach the humiliation of bowing to what amounted to extortion³⁷". Opposition to slavery from Britain's labouring and middle classes dampened opposition from those most impacted by the cotton shortage, and

²⁹ David G. Surdam, "King Cotton: Monarch or Pretender? The State of the Market for Raw Cotton on the Eve of the American Civil War." *The Economic History Review* v. 51, n. 1 (1998): 122.

³⁰ 4.5 million bales, worth \$225 million in gold. Stoker, *The Grand Design*, 28.

³¹ Stoker, *The Grand Design*, 122-123; Duncan Andrew Campbell, "Letting Someone Else Have Your Way: The Palmerston Ministry's Foreign Policy and the American Civil War." *Journal of Liberal History*, no. 114 (March) (2022):11.

³² Stoker, *The Grand Design*, 27, 105

³³ Stoker, *The Grand Design*, 28

³⁴ Estimates vary on what the stocks were, and also what the Confederacy believed them to be. Stoker, *The Grand Design*, 27-28; Sundam, "King Cotton", 122.

³⁵ Stoker, *The Grand Design*, 30

³⁶ Weigley, *A Great Civil War*, 68-69

³⁷ Stoker, *The Grand Design*, 29

Britain could afford to provide relief to impacted industries³⁸. Britain was also reliant on grain imports from the Union. It therefore had little incentive to not comply with the Union blockade, and ultimately it remained neutral. Other countries were not inclined to risk war with the Union by breaking the blockade³⁹. The Confederacy suffered the triple blow of failing to coerce international support for its cause, loss of revenue for its war effort, and the undermining of its major commodity for underwriting bonds and notes.

This complex web of interactions can be explained through Hirschman's influence effect. The Confederacy misjudged the degree to which it had made the interruption of cotton trade unsustainable for Britain. It failed to anticipate that Britain would avert the risk of its manufacturing industry becoming one of Hirschman's 'commercial fifth columns' through the provision of relief. It over-estimated the degree to which it had made it difficult for Britain to, as Hirschman put it 'dispense entirely with the trade' or source supplies from other countries⁴⁰. Most importantly, it failed to appreciate the asymmetry of its trade relationship with Britain. While the confederacy may have had other markets for its cotton, the preponderance of trade with Britain meant that the impacts of ceasing trade were much less bearable for the Confederacy than they were for Britain. Rather than wielding influence effects, the Confederacy became the victim of them. The lesson for students of strategy here is that *even in economic relationships which verge on monopoly, strategists should not assume leverage, particularly where there is an asymmetric economic advantage against the near-monopoly holder.*

Conclusions

Despite the passage of 150 years, the American Civil War provides fertile ground for drawing lessons for students of strategy today. In examining the economic conditions of the period, characteristics of the modern international economic system can be seen. The Union, the Confederacy and their trading partners were modern states positioned in a free trade economy like that of today, and like today that free trade was imperfect. They had to make choices to manage scarcity, and like states today had to manage the interests of important substate actors inside their societies and those of their trading partners. Hence, the influence effect theory Albert Hirschman described in 1946 remains relevant today as well. The relevancy of the case study and relevancy of the theory allow for the two lessons described here: *enacting effective strategy requires a state to align the aims of its selectorates, and even in economic relationships which verge on monopoly, strategists should not assume leverage, particularly where there is an asymmetric economic advantage against the near-monopoly holder.* The Confederacy failed to learn these lessons at the time, and this contributed to their defeat.

Of all the lessons that could be drawn from the tactical, operational and strategic study of the Civil War, why are these the most important? The answer is that these lessons show that the economic element of national power impacts all others. Incoherent Confederate finance undermined their ability to pay for military power. Their clumsy attempts at coercion undermined their diplomatic leverage. Their protection of their economic interests undermined the diplomatic efforts. This points to the utility of economics-based lessons for students of strategy even if their focus is the military element of national power. In a world that continues to be characterised by asymmetric power relationships and unevenly distributed interests of sub-state actors, students of strategy will benefit from the lessons the Confederacy failed to learn.

³⁸ Stoker, *The Grand Design*, 30

³⁹ Stoker, *The Grand Design*, 104

⁴⁰ Hirschman, *National Power and the Structure of Foreign Trade*, 17

Bibliography

- Bedwell, Randall (ed). *Brink of Destruction: A quotable History of the Civil War*. Cumberland House, 1999
- Blainey, Geoffrey. *The Causes of War*. The MacMillan Press, 1973
- Bonner, Michael Brem. *Confederate Political Economy: Creating and Managing a Southern Corporatist Nation*. LSU Press, 2016
- Campbell, Duncan Andrew. "Letting Someone Else Have Your Way: The Palmerston Ministry's Foreign Policy and the American Civil War." *Journal of Liberal History*, no. 114 (March) (2022): 6–21
- Cohen, Elliot A. *Supreme Command*. Simon and Schuster, 2002
- Corbett, P. Scott; Volker Janssen; John M. Lund; Todd Pfannestiel; Paul Vickery; and Sylvie Waskiewicz. *US History*. OpenStax College, 2021. Located at: <http://openstaxcollege.org/textbooks/us-history>.
- de Mesquita, Bruce Bueno; James D. Morrow; Randolph M. Siverson; and Alastair Smith. "Testing Novel Implications from the Selectorate Theory of War." *World Politics*, v. 56, no. 3 (April) (2004): 363-388
- Flaherty, Jane. "The Exhausted Condition of the Treasury on the Eve of the Civil War", *Civil War History*, v. 55, n. 2 (2009): 244–277
- Helleiner, Eric. "Economic Foundations of Strategy: Beyond Smith, Hamilton and List." In *The New Makers of Modern Strategy: From the Ancient World to the Digital Age*, edited by Jonathan Kirshner and Hal Brands. Princeton University Press, 2023
- Hirschman, Albert O. *National Power and the Structure of Foreign Trade*, University of California Press, 1946, expanded edition 1980
- Lacey, James. "Alexander Hamilton and the Financial Sinews of Strategy." In *The New Makers of Modern Strategy: From the Ancient World to the Digital Age*, edited by Jonathan Kirshner and Hal Brands. Princeton University, 2023
- Nolt, James H. *International Political Economy: The Business of War and Peace*. Taylor & Francis Group, 2013
- O'Brien, Robert and Marc Williams. *Global Political Economy: Evolution and Dynamics*. Palgrave MacMillan, 5th edition, 2016
- Razaghian, Rose. *Financial Civil War: The Confederacy's Financial Policies, 1861-1864*. Yale ICF Working Paper No. 04-45, Yale University, Last Revised June 2005
- Ron, Ariel and Sofia Valeonti. "Money War: Democracy, Taxes and Inflation in the U.S. Civil War," *Cambridge Journal of Economics*, v. 47 n. 2 (2023): 263–288
- Silva, Joaquim Ramos. "Trade between asymmetrical democratic countries," *Journal of Economic Studies*, v. 26 n. 4/5 (1999): 412-426
- Siverson, Randolph M., and Bruce Bueno de Mesquita. "The Selectorate Theory and International Politics." *Oxford Research Encyclopedia of Politics*. 28 Jun. 2017;

<https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-293>.

Stoker, Donald. *The Grand Design: Strategy and the U. S. Civil War*. Oxford University Press Incorporated, 2010

Surdam, David G. "King Cotton: Monarch or Pretender? The State of the Market for Raw Cotton on the Eve of the American Civil War." *The Economic History Review* v. 51, n. 1 (1998): 113–132

Weigley, Russell F. *A Great Civil War: A Military and Political History, 1861-1865*. Indiana University Press, 2000

Wilson, Mark R. *The Business of Civil War: Military Mobilization and the State, 1861–1865*, Johns Hopkins University, 2006

Case Study 2: Ancient Carthage – Power and Strategy in the Punic Wars

The Punic Wars represented a cycle of conflict between Carthage and Rome that culminated in Carthage's complete destruction. As the Roman General Scipio looked upon the burning ruins of his enemy's capital, he reflected that '*all cities, nations, and authorities must, like men, meet their doom; that this happened to Ilium, once a prosperous city, to the empires of Assyria, Media, and Persia, the greatest of their time, and to Macedonia itself, the brilliance of which was so recent.*'¹ Thinking on the inevitable and inescapable fate of his own homeland, he quoted the Iliad: "*A day will come when sacred Troy shall perish, And Priam and his people shall be slain.*"²

This case study explores why Carthage, a wealthy, powerful and expansive regional hegemon, failed to meet the threat represented by Rome's rise. It examines how a state that had grown in power and stature for seven centuries could be destroyed in one. In doing so, it provides a broader lesson to students of strategy: the foundations of a state's power that underpin its strategic framework may also constrain its ability to effectively respond to a changing external environment. Put another way, the factors that allow a state to attain power may not enable it to retain power when circumstances change. Perhaps this may account for Scipio's keen observation. Students of strategy might reflect on how this lesson applies to other historical case studies, and to contemporary international relations. Employing a neoclassical realist analytical framework, the case study argues that Carthage developed and applied a discernible, coherent and successful grand strategy from its establishment in the ninth century BC to the outbreak of the Punic wars in the third century BC. This strategy aligned with Carthage's internal political, economic and cultural structures, underpinned its rapid growth, and supported a high degree of strategic stability in the Western Mediterranean for centuries. However, the rise of Rome represented a significant change to the external environment. This dislocated Carthaginian power, ultimately resulting in the failure of Carthaginian grand strategy during the First Punic War. Carthage attempted to evolve its strategy in the Second Punic War, but adaptation and strategic choice were constrained by the structural and ideational foundations of Carthaginian power. This contributed significantly to Carthage's defeat and ultimate destruction.

Can Ancient Carthage be said to have had a grand strategy? While the language of grand strategy dates from the nineteenth century, the concept of grand strategy provides a way to explore the relationship between enduring strategic conditions, capabilities, objectives, preferences and choices, and has served to illuminate a range of historical cases.³ Discernment of a Carthaginian strategic culture, world view or policy outlook is complicated by the paucity of sources, and the bias inherent in the Greek and

¹ Polybius, *The Histories*, trans. F.W. Walbank, Loeb Classical Library, vol. VI (Cambridge, Mass: Harvard University Press, 1927), 439.

² Polybius, VI:439.

³ See, for example, Marcus Müller, "A View To A Kill: Egypt's Grand Strategy In Her Northern Empire" (Brill, 2011); Bee Yun, "Persia and Pericles' Grand Strategy. Was the Peloponnesian War a Bipolar Hegemonic War?," *The International History Review* 44, no. 1 (January 2, 2022): 206–24; Athanassios Platias and Constantinos Koliopoulos, *Thucydides on Strategy: Grand Strategies in the Peloponnesian War and Their Relevance Today* (Oxford University Press, 2017); Edward Luttwak, *The Grand Strategy of the Roman Empire: From the First Century CE to the Third* (JHU Press, 2016).

Roman sources from which the modern understanding of Carthage derives.⁴ However, there is strong evidence that provides confidence in the broad outline of historical events of this period, supporting inductive analysis of motivations and policy.⁵ One further challenge: the concept of grand strategy is contested, and definitions abound.⁶ This case study adopts Posen's definition of grand strategy as "a state's theory about how it can best 'cause' security for itself."⁷ An effective grand strategy identifies threats to state security and devises "political, economic, military and other remedies for those threats."⁸ Schmidt echoes this, describing grand strategy as "the overall vision of a state's national security goals and a determination of the most appropriate means by which to achieve those goals."⁹

Posen and Schmidt emphasise security as the principle goal of the state, and the basis for grand strategy. This is precisely the formulation employed by neoclassical realism, which contends that states function to deliver security needs.¹⁰ While classical realism treats the state as a 'black box' that acts in its own rational self-interest, neoclassical realism recognises the internal factors that moderate strategic choice, including political, economic and social structures.¹¹ These moderate competition and conflict between states that result from external drivers including the emergence of threats and competing economic interests drive military action.¹² This analytical framework provides a start-point for understanding Carthaginian strategic interests, capabilities and choices, as well as those of its adversaries.

In its early years, Carthage was unremarkable – one of many small Phoenician colonies dotted along the shores of the Mediterranean.¹³ Within two centuries, it had become the wealthiest and most powerful polity west of Greece.¹⁴ The reasons for Carthage's

⁴ Craige B Champion, "Polybius and the Punic Wars," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 95–110; Bernard Mineo, "Principal Literary Sources for the Punic Wars," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 111–27.

⁵ For an overview of Carthage historiography see Adrian Goldsworthy, *The Fall of Carthage: The Punic Wars 265–146BC* (Hachette UK, 2012), 19–24.

⁶ Lukas Milewski, *The Evolution of Modern Grand Strategic Thought* (Oxford University Press, 2016), 143–53.

⁷ Barry Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Cornell University Press, 1984), 13.

⁸ Posen, 13.

⁹ Brian C. Schmidt, "The Primacy of National Security," in *Foreign Policy: Theories, Actors, and Cases*, 3rd ed. (Oxford: Oxford University Press, 2016), 215.

¹⁰ Gerlinde Groitl, "Strategic Choices: Neoclassical Realist Model of Order and Revisionism," in *Russia, China and the Revisionist Assault on the Western Liberal International Order*, by Gerlinde Groitl (Cham: Springer International Publishing, 2023), 91.

¹¹ Gideon Rose, "Neoclassical Realism and Theories of Foreign Policy," *World Politics* 51, no. 1 (1998): 144–72; Colin Elman and Michael Jensen, *The Realism Reader* (Routledge, 2014), 243; Charles L. Glaser, "The Necessary and Natural Evolution of Structural Realism," in *The Realism Reader*, ed. Colin Elman and Michael Jensen (London: Routledge, 2014), 82.

¹² Mark R. Brawley, *Political Economy and Grand Strategy: A Neoclassical Realist View* (Oxford: Taylor & Francis Group, 2009), 4.

¹³ Walter Ameling, "The Rise of Carthage to 264," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 40.

¹⁴ Dexter Hoyos, *Carthage: A Biography* (Oxford: Taylor & Francis Group, 2017), 11.

success lie in its character as a mercantilist sea power.¹⁵ Carthage's greatest advantage was its strategic location, which allowed it to control the narrow straits between North Africa, Sicily and Sardinia from its protected harbours. This enabled it to dominate and exploit lucrative north-south and east-west trade routes. Reflecting its Phoenician roots, operated as part of a vast maritime trading network of Phoenician colonies and trading posts stretching from Spain to Tyre. Carthage protected and expanded its mercantile maritime economy through two primary means – political control and military power. Eschewing conquest, Carthage extended its power through a federated network of allies, client states, trading posts and military fortifications across Spain, Sardinia, Malta, and western Sicily, assuring dominance of the western Mediterranean.¹⁶ Reflecting history, culture, geography and economic interests, Carthage's fleet was the mainstay of its hard power. Carthage developed cutting edge naval technology, fielding fast, light and manoeuvrable vessels that demonstrated superior performance against Greek and later Roman craft.¹⁷ The fleet maintained sea control, protected trade, disrupted piracy, and harried competitors. Notably, Carthage's maritime force was comprised of citizens, while its army relied almost exclusively on mercenary units commanded by Carthaginian officers.¹⁸ The use of mercenaries enabled Carthage to field substantial land forces despite the relatively small number of Carthaginian citizens.¹⁹

By the sixth century BC, an established Carthaginian elite exercised control of government, the military and foreign policy. This polity inherited a grand strategic framework founded on mercantilism, enabled by federated colonies and trading posts that extracted resources from across the region, and maintained through sea control based on maritime power. This then was Carthage's "theory about how it can best 'cause' security for itself."²⁰ These structural and ideational factors bounded Carthaginian strategic choice. Carthage's success or failure would depend on the efficacy of these grand strategic capabilities and assumptions in the context of a changing external environment, or on its ability to adapt to new contexts, threats and opportunities.

The first significant test for Carthage's grand strategy came through a challenge to its control of vital ports in Sicily. Like the Phoenicians, the Greeks had established colonies and trading networks across the Mediterranean from the ninth century BC, including on Sicily. Expanding Greek power represented a threat to Carthaginian hegemony, and in the fifth century BC mounting tensions spilled into open conflict.²¹ For two hundred years, Carthage and the Greek city states of Sicily fought a series of inconclusive wars.²² Although costly, these did not constitute an existential threat to Carthage, and they did not invalidate Carthaginian grand strategy. Rather, they represented a pattern of sustainable strategic competition, accommodated within Carthage's strategic assumptions.²³ Throughout the Sicilian Wars, Carthage continued to establish new colonies in northern Africa, Tunisia and Spain and to expand its reach into the Atlantic. Its political, economic and military power continued to grow. By the beginning of the third century BC, Carthage had restored strategic stability in Sicily, exercising effective control of the western and central regions of the island, enabling it to maintain its trade

¹⁵ Mihai Murariu, "Perspectives on Seapower and International Systems. The Case of Rome and Carthage," *Research and Science Today* 22, no. 2 (2021): 44.

¹⁶ Ameling, "The Rise of Carthage to 264," 48–51.

¹⁷ Hoyos, *Carthage*, 35–36.

¹⁸ Hoyos, 37.

¹⁹ Goldsworthy, *The Fall of Carthage*, 31.

²⁰ Posen, *The Sources of Military Doctrine*, 13.

²¹ Hoyos, *Carthage*, 54–56.

²² Goldsworthy, *The Fall of Carthage*, 27–28.

²³ Hoyos, *Carthage*, 63.

routes and colonies. It remained the most powerful state in the Western Mediterranean.²⁴ However, it would soon face an unprecedented threat to its security and its very survival.

The Punic Wars were an existential power struggle between established Carthage and an expanding Rome. On the eve of hostilities Carthage was undoubtedly the more powerful of the two belligerents in material terms. It had a stronger and more diversified economy, a broader network of territories and bases, a larger population, superior naval forces, and control of the western Mediterranean Sea.²⁵ Why then did its ancient citadel lie in ruins 120 years later, its people dead or in chains, its books and statues destroyed? The remainder of the case study explores this question. It demonstrates that the character of the Carthaginian state delimited its strategic choices and actions, contributing to failure against the very different type of power brought to bear by Rome. When Carthage's grand strategy became untenable, attempts to adapt to the new international environment were constrained by structural and ideational factors and were ultimately unsuccessful.

Founded in 753 BC, Rome grew more slowly than Carthage. Preferring conquest to trade, the early Roman state gradually gained control over the Italian peninsula through war and diplomacy.²⁶ Following establishment of the Republic in 509BC, Rome fought a series of land wars with Gauls and Etruscans in northern Italy, and with Greek colonies in the south. In this latter campaign, Roman and Carthaginian interests coincided. From the earliest days of the Roman Republic, its relations with Carthage were governed by a series of treaties that agreed to refrain from hostilities and defined spheres of influence and trading arrangements.²⁷ These treaties gave Rome a free hand on the Italian peninsula. They also supported Carthage's grand strategy, preserving critical trade routes, denying expansion of Roman settlements into Carthaginian territories, and enabling Carthage to focus its attention on the threat posed by Greek forces in Sicily.²⁸ An approach of mutual accommodation endured for over two hundred years. By the beginning of the third century BC, Rome has established control over all of Italy, and was rapidly growing in economic and military power.²⁹

Relations between Carthage and Rome began to change during the Pyrrhic War. In 280 BC, the Greek tyrant Pyrrhus launched an invasion of southern Italy and prepared to cross into Sicily. Recognising this mutual threat, Carthage and Rome signed a new treaty, agreeing that Carthaginian shipping might transport Roman troops into combat in either Italy or Sicily.³⁰ Pyrrhus invaded Sicily but was eventually repulsed. The treaty had little practical effect, but it provides insight into the strategic approach of both states. From a Carthaginian viewpoint, the agreement leveraged its maritime strengths and its tradition of using mercenaries or proxies to fight on land. But for the Romans, the treaty hinted at the limits of Carthaginian power, and the vulnerability of its armies on the rich agricultural lands of Sicily. At around the same time, Roman elites began debating the threat posed by Carthage through its control of the Western Mediterranean. Polybius

²⁴ Goldsworthy, *The Fall of Carthage*, 28.

²⁵ Iskander Rehman, "Great-Power Success in Protracted Warfare: Key Drivers and Core Components," *Adelphi Series* 62, no. 496–497 (2022): 33–34, <https://doi.org/10.1080/19445571.2022.2274678>.

²⁶ Goldsworthy, *The Fall of Carthage*, 36–38.

²⁷ Polybius, *The Histories of Polybius*, trans. F. Hultsch and Evelyn S. Shuckburgh, vol. 1 (London: Macmillan and Co, 1889), 185–87.

²⁸ John Serrati, "Neptune's Altars: The Treaties between Rome and Carthage (509–226 BC)," *The Classical Quarterly* 56, no. 1 (2006): 113–34.

²⁹ Hoyos, *Carthage*, 64–65.

³⁰ Polybius, *The Histories of Polybius*, 1:185–87.

records that “they were beginning ... to be exceedingly anxious lest, if the Carthaginians became masters of Sicily also, they should find them very dangerous and formidable neighbours ... occupying a position which commanded all the coasts of Italy.”³¹ Through the lens of classical neorealism, Carthaginian and Roman desires for economic and territorial security would put the two powers on a collision course.

The First Punic War between Carthage and Rome began in 264 BC when Roman forces landed in Sicily on the pretext of assisting a minor ally. The Romans achieved early tactical success, but lacking sufficient strength and supplies to achieve decision, they soon withdrew. From Carthage's viewpoint, this fitted with the well-established pattern of operations in Sicily. Carthage would – it supposed – maintain the balancing strategy it had employed successfully for over two centuries.³² Its mercenaries would fight to retain its foothold in Sicily, while its maritime forces would keep the war at a distance and maintain prosperity through trade, enabling it to fund ongoing military operations.³³ For a time, this proved successful. Rome resumed offensive operations, but the war settled into strategic stalemate, grinding on through a series of indecisive battles, sieges and naval engagements that lasted for almost a decade.³⁴

Unable to achieve decision in Sicily, Rome determined to break the familiar strategic pattern by challenging Carthage's control of the seas, raising a powerful new fleet.



Image: Roman War Galley. Encyclopedia Britannica. Available at <https://www.britannica.com/event/Punic-Wars#/media/1/940971/18350>

³¹ Polybius, *The Histories of Polybius*, 1:10.

³² Michael J. Taylor, “Generals and Judges: Command, Constitution and the Fate of Carthage,” *Libyan Studies*, no. 54 (2023): 38.

³³ Richard Miles, *Carthage Must Be Destroyed: The Rise and Fall of an Ancient Civilization* (Penguin, 2011), 179.

³⁴ Boris Rankov, “A War of Phases: Strategies and Stalemates 264 - 241 BC,” in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 151–55.

Carthaginian defeat at the naval battle of Mylae (260 BC) was a devastating blow to Punic confidence.³⁵ With Carthage's sea control now contested, Rome launched an audacious invasion of Africa. In 256 BC the Roman invasion fleet broke Carthage's maritime defences at the Battle of Cape Ecnomus before devastating Carthage's surrounds.³⁶ When Carthage finally halted the Roman campaign at the Battle of Tunis (255 BC), the action shifted back to Sicily where the war of attrition continued for another fourteen years.³⁷ Costs mounted on both sides. Eventually Rome achieved a decisive victory at sea, destroying the Carthaginian fleet at the Battle of the Aegates (241 BC).³⁸ The exhausted Carthaginians sued for peace, agreeing to surrender Sicily to Roman control and pay a substantial indemnity. Carthage's reliance on mercenaries would haunt it when its unpaid armies turned against it during the brutal Truceless War.³⁹ This enabled Rome to coerce a weakened Carthage to surrender Sardinia and Corsica also.⁴⁰ With the loss of these territories and the devastation of its fleet, the foundations of Carthage's maritime strategy suffered irreparable damage.

Carthage's grand strategic framework had proven unable to cope with the rise of Roman power. The Carthage polity sought to adapt to the new international environment through changes to its strategic approach. It shifted focus to the west, expanding its settlements in Iberia to access additional manpower and raw materials.⁴¹ Meanwhile Rome, having consolidated its control of the central Mediterranean Islands, established its own foothold in Iberia.⁴² This would become the next flashpoint as the two great powers sought to establish supremacy. Recognising the security threat posed by Roman encroachment into Iberia, and motivated by a desire to redress the ignominy of the First Punic War, Hannibal – Carthage's most famous General – laid siege to the Roman settlement of Saguntum in 219 BC, marking the beginning of the Second Punic War.⁴³

Carthage's strategy during this conflict represented a marked departure from its long-standing grand strategic framework. Having lost maritime supremacy, it embarked on a continental strategy.⁴⁴ Carthage sought to peel away Rome's allies and to inflict decisive defeat on its armies, thereby forcing Rome to renegotiate terms.⁴⁵ Hannibal marched his army from Iberia across the Alps and into Italy, building alliances with local tribes to secure his lines of communication and strengthen his numbers.⁴⁶ This was a new way of warfare for Carthage. Tactically, it was highly successful. Within two years, Hannibal inflicted crushing defeats on the Roman Legions at Ticinus, Trebia, Trasimene and

³⁵ Fik Meijer, "Carthage as a Maritime Power," in *Carthage: Fact and Myth*, ed. Roald Docter, Ridha Boussoffara, and Pieter ter Keurs (Leiden: Sidestone Press, 2015), 67.

³⁶ Rankov, "A War of Phases: Strategies and Stalemates 264 - 241 BC," 155–57.

³⁷ Rankov, 157–62.

³⁸ Rankov, 163–64.

³⁹ Dexter Hoyos, "Carthage in Africa and Spain, 241-218," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 206–10.

⁴⁰ Goldsworthy, *The Fall of Carthage*, 136.

⁴¹ Hoyos, "Carthage in Africa and Spain, 241-218," 214–16.

⁴² Hans Beck, "The Reasons for the War," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 235–37.

⁴³ Beck, 228–31.

⁴⁴ Edward Togo Salmon, "The Strategy of the Second Punic War," *Greece & Rome* 7, no. 2 (1960): 136.

⁴⁵ Michael P. Fronda, "Hannibal: Tactics, Strategy and Geostrategy," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 250; Daneta Billau and Donald Graczyk, "Hannibal: The Father of Strategy Reconsidered," *Comparative Strategy* 22, no. 4 (January 2003): 341–42.

⁴⁶ Hoyos, *Carthage*, 72.

Cannae.⁴⁷ However, tactical success could not translate to strategic victory.⁴⁸ For eleven years, Hannibal fought through the Italian countryside, but could not achieve decision against an enemy operating with strategic depth, short supply lines, and a strong recruiting base.⁴⁹ Rome continued to raise levies and to harry the invader while avoiding open battle.⁵⁰ Rome's control of Sicily denied Hannibal easy resupply, while Carthage's allies and mercenaries' loyalties were to prove fragile.⁵¹ In 205 BC, Rome leveraged its control of Sicily to launch another invasion of the Carthaginian homeland. Hannibal was forced to return to Carthage to defend the capital, marking the end of his Italian ambitions. Carthage suffered a final defeat at the Battle of Zama in 202BC, forcing it to agree to humiliating terms. Carthage was stripped of its overseas possessions, forbidden to possess war elephants, and its fleet was restricted to ten warships. It was required to pay a crushing indemnity to Rome, and its foreign policy was subordinated to Roman oversight.⁵²

The treaty ended Carthage's status as a great power.⁵³ For six hundred years, Carthage had grown in power and influence through a grand strategy predicated on mercantilism and sea control. In the First Punic War, Carthage's grand strategy failed when it lost the ability to exert unchallenged maritime power in the Western Mediterranean. The Second Punic War represented an attempt to adapt to changed strategic circumstances through application of an emergent strategy of continental warfare and alliance-building. This failed due to Rome's strategic depth and control of sea lines of communication, the limits of Carthaginian manpower and its overreliance on allies and mercenaries. Carthage's final strategy was one of accommodation. It sought to accept its degraded political and military status, focusing instead on its economic interests. Through trade, it rebuilt and maintained unsurpassed wealth. This attracted Roman attention, nor had Rome forgotten the trauma of Hannibal's invasion.⁵⁴ Shortly after Carthage had paid the indemnity, Rome, exhibiting a combination of greed and fear, embarked on the Third Punic War – a short, brutal campaign that culminated in Carthage's annihilation.⁵⁵

This case study demonstrates a key lesson for strategists: the foundations of a state's power that underpin its strategic framework may constrain its ability to effectively respond to a changing external environment. Neoclassical Realism suggests that Carthaginian grand strategy was motivated by a quest for security – territorial security of its homeland and of the ports that enabled it to control the Western Mediterranean, and economic security through the protection of its trading networks. Carthage's grand strategy – its theory about how to cause security for itself – was based on structural and ideational factors including politics, history and geography, which contributed to critical

⁴⁷ Klaus Rawlings, "The War in Italy, 218-203," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 300; Hoyos, *Carthage*, 72–73.

⁴⁸ Billau and Graczyk, "Hannibal: The Father of Strategy Reconsidered," 349.

⁴⁹ Fronda, "Hannibal: Tactics, Strategy and Geostrategy," 252–53.

⁵⁰ Klaus Zimmerman, "Roman Strategy and Aims in the Second Punic War," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 285–90.

⁵¹ Peter Edwell, "War Abroad: Spain, Sicily, Macedon, Africa," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 330; Rawlings, "The War in Italy, 218-203," 313; Kathryn Lomas, "Rome, Latins, and Italians in the Second Punic War," in *A Companion to the Punic Wars*, ed. Dexter Hoyos (Chichester: Wiley-Blackwell, 2011), 354; Rehman, "Great-Power Success in Protracted Warfare," 36.

⁵² Hoyos, *Carthage*, 76.

⁵³ Hoyos, 77.

⁵⁴ Hoyos, 84–86.

⁵⁵ Hoyos, 79–83.

capabilities including the ability to develop and apply maritime power, and to leverage trade to build economic power. It sought to expand its security through alliances, client states and colonies. These represented a virtuous circle – security begat security. When its security was threatened, Carthage was ready to go to war to protect its interests. For six hundred years, Carthage's strategic approach and capabilities suited its times, supporting its rise to pre-eminence in the western Mediterranean. The rise of Rome – surely one of the most significant changes to the international order in world history – dislocated Carthaginian grand strategy. Following a period of mutual accommodation, the two powers came into conflict. Both would come to depend on the Mediterranean Sea for both their security and prosperity, and both were willing to fight to protect and advance their interests. Carthage anticipated that this conflict would conform to established patterns of strategic competition. However Rome represented a new and unforeseen threat – an enemy that sought total domination, and that had the population, resources, technology and ideology to impose its will. Rome's destruction of the Carthaginian fleet and seizure of the Mediterranean Islands unwound Carthage's grand strategy. When Carthage responded with an emergent strategy of continental warfare, it lacked the resources and capabilities to win. Rather, it only succeeded in confirming in Roman minds that Carthage itself represented an intolerable threat to security: "*Carthago delenda est*" – Carthage must be destroyed.⁵⁶ Students of strategy should consider the key finding of this case study – that is, the foundations of power may constrain a state's ability to respond to changing circumstances. Building on this conclusion, a wider survey of historical and contemporary case studies might explore the prevalence and significance of this observation in the experience of empire, and its potential implications for the contemporary international system.

⁵⁶ The famous phrase attributed to Cato the Elder. See Charles E. Little, "The Authenticity and Form of Cato's Saying 'Carthago Delenda Est,'" *The Classical Journal* 29, no. 6 (1934): 429–35.

Bibliography

Ameling, Walter. "The Rise of Carthage to 264." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.

Beck, Hans. "The Reasons for the War." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.

Billau, Daneta, and Donald Graczyk. "Hannibal: The Father of Strategy Reconsidered." *Comparative Strategy* 22, no. 4 (January 2003): 335–53.

Brawley, Mark R. *Political Economy and Grand Strategy: A Neoclassical Realist View*. Oxford: Taylor & Francis Group, 2009.

Champion, Craig B. "Polybius and the Punic Wars." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.

Edwell, Peter. "War Abroad: Spain, Sicily, Macedon, Africa." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.

Elman, Colin, and Michael Jensen. *The Realism Reader*. Routledge, 2014.

Fronza, Michael P. "Hannibal: Tactics, Strategy and Geostrategy." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.

Glaser, Charles L. "The Necessary and Natural Evolution of Structural Realism." In *The Realism Reader*, edited by Colin Elmand and Michael Jensen. London: Routledge, 2014.

Goldsworthy, Adrian. *The Fall of Carthage: The Punic Wars 265-146BC*. Hachette UK, 2012.

Groitzl, Gerlinde. "Strategic Choices: Neoclassical Realist Model of Order and Revisionism." In *Russia, China and the Revisionist Assault on the Western Liberal International Order*, by Gerlinde Groitzl, 79–123. Cham: Springer International Publishing, 2023.

Hoyos, Dexter. *Carthage: A Biography*. Oxford: Taylor & Francis Group, 2017.

———. "Carthage in Africa and Spain, 241-218." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.

Little, Charles E. "The Authenticity and Form of Cato's Saying 'Carthago Delenda Est.'" *The Classical Journal* 29, no. 6 (1934): 429–35.

Lomas, Kathryn. "Rome, Latins, and Italians in the Second Punic War." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.

Luttwak, Edward. *The Grand Strategy of the Roman Empire: From the First Century CE to the Third*. JHU Press, 2016.

Meijer, Fik. "Carthage as a Maritime Power." In *Carthage: Fact and Myth*, edited by Roald Docter, Ridha Boussoffara, and Pieter ter Keurs. Leiden: Sidestone Press, 2015.

- Miles, Richard. *Carthage Must Be Destroyed: The Rise and Fall of an Ancient Civilization*. Penguin, 2011.
- Milevski, Lukas. *The Evolution of Modern Grand Strategic Thought*. Oxford University Press, 2016.
- Mineo, Bernard. "Principal Literary Sources for the Punic Wars." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.
- Müller, Marcus. "A View To A Kill: Egypt's Grand Strategy In Her Northern Empire." Brill, 2011.
- Murariu, Mihai. "Perspectives on Seapower and International Systems. The Case of Rome and Carthage." *Research and Science Today* 22, no. 2 (2021): 37–46.
- Platias, Athanassios, and Constantinos Koliopoulos. *Thucydides on Strategy: Grand Strategies in the Peloponnesian War and Their Relevance Today*. Oxford University Press, 2017.
- Polybius. *The Histories*. Translated by F.W. Walbank. Loeb Classical Library. Vol. VI. Cambridge, Mass: Harvard University Press, 1927.
- . *The Histories of Polybius*. Translated by F Hultsch and Evelyn S. Shuckburgh. Vol. 1. London: Macmillan and Co, 1889.
- Posen, Barry. *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*. Cornell University Press, 1984.
- Rankov, Boris. "A War of Phases: Strategies and Stalemates 264 - 241 BC." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.
- Rawlings, Klaus. "The War in Italy, 218-203." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.
- Rehman, Iskander. "Great-Power Success in Protracted Warfare: Key Drivers and Core Components." *Adelphi Series* 62, no. 496–497 (2022): 33–72. <https://doi.org/10.1080/19445571.2022.2274678>.
- Rose, Gideon. "Neoclassical Realism and Theories of Foreign Policy." *World Politics* 51, no. 1 (1998): 144–72.
- Salmon, Edward Togo. "The Strategy of the Second Punic War." *Greece & Rome* 7, no. 2 (1960): 131–42.
- Schmidt, Brian C. "The Primacy of National Security." In *Foreign Policy: Theories, Actors, and Cases*, 3rd ed., 206–21. Oxford: Oxford University Press, 2016.
- Serrati, John. "Neptune's Altars: The Treaties between Rome and Carthage (509–226 BC)." *The Classical Quarterly* 56, no. 1 (2006): 113–34.
- Taylor, Michael J. "Generals and Judges: Command, Constitution and the Fate of Carthage." *Libyan Studies*, no. 54 (2023): 37–44.

Yun, Bee. "Persia and Pericles' Grand Strategy. Was the Peloponnesian War a Bipolar Hegemonic War?" *The International History Review* 44, no. 1 (January 2, 2022): 206–24.

Zimmerman, Klaus. "Roman Strategy and Aims in the Second Punic War." In *A Companion to the Punic Wars*, edited by Dexter Hoyos. Chichester: Wiley-Blackwell, 2011.

This page is intentionally blank

Case Study 3: Having applied relevant theory and concepts to the Byzantine Empire, what are the most important lessons for students of strategy?

The rise and fall of empires reveal crucial lessons in strategic brilliance and failure, offering insights that help shape our present and future. The Byzantine Empire's enduring history offers a valuable case study for students of strategy. Centred on Constantinople, the Byzantine capital's strategic location on the Bosphorus Strait made it a crucial economic hub linking Europe, Africa, and Asia.¹ Its central location also made it a crucial centre of religion, particularly Christianity. Spanning the eastern Mediterranean, North Africa and the Middle East, the Empire's immense territory presented numerous strategic opportunities and threats, necessitating a grand strategy that was "lean, adaptive and innovative."² Throughout its history, successive Byzantine Emperors were forced to employ nuanced and dynamic approaches to meet ever-changing strategic circumstances. While intended to ensure survival, strategic missteps were made that also destabilised the Empire.

Drawing on the seminal works of Edward Luttwak³ and Peter Frankopan,⁴ this essay argues that the most important lessons from the Byzantine experience are the crucial roles of economy-building and nation-building as foundations of national power. This essay will identify the Byzantine Empire's grand strategy, assess the critical roles of economy-building and nation-building, and analyse their enduring relevance for contemporary strategic thinking. These insights into the Byzantine Empire's strategic resilience will offer profound lessons for modern students of strategy, emphasising the enduring relevance of economy-building and nation-building in navigating complex and challenging strategic environments.

Byzantine Grand Strategy

Grand strategy is a comprehensive framework that guides a state's use of its resources—its levers⁵—to achieve long-term objectives and priorities across all spheres of national power.⁶ The Byzantine Empire's grand strategy focused on the strategic levers of warfare, diplomacy, and statecraft. Notable Byzantine leaders, including Emperor Justinian I, skillfully integrated these elements to maintain the Empire's stability and safeguard its territorial integrity.⁷ In the strategic context, these levers fundamentally provided the 'ways'⁸ for the Byzantine Empire to implement foreign policy.

¹ Rowena Malpas, *The History of Empires: Rise and Fall of Great Powers* (Richards Education, n.d.), p. 80.

² Robert Joustra, "The (Not so) Grand Strategy of the Byzantine Empire," *Review of Faith and International Affairs* 8, no. 3 (January 1, 2010): 69–70, p. 69.

³ Edward Luttwak, *The Grand Strategy of the Byzantine Empire* (Cambridge, Mass: Belknap Press, 2009).

⁴ Peter Frankopan, *Silk Roads: A New History of the World*, Paperback edition. (Bloomsbury, 2016).

⁵ Levers of power are those resources available to states to achieve political or strategic outcomes. These are typically categorised as diplomatic, information, military, and economic. Keith Slack, "The Information Lever of Power," *Freeman Papers*, August 21, 2024, p. 3.

⁶ Nina Silove, "Beyond the Buzzword: The Three Meanings of 'Grand Strategy'," p. 27.

⁷ John Julius Norwich, *A Short History of Byzantium* (Penguin, 2013).

⁸ This paper defines strategy as: 'ends' (objectives toward which one strives) plus 'ways' (courses of action) plus 'means' (instruments by which some end can be achieved). COL Arthur Lykke cited by Lawrence Freedman, Hal Brands, ed., *The New*

Critically, these levers were derived from and underwritten by two distinct strategic 'means': the economy and societal cohesion. The grand strategy of the Byzantine Empire enabled it to endure for over a millennium, sustained primarily through effective economic management and religious patronage. These elements served as the bedrock of Byzantine national power, fortifying their resilience, and enabling them to survive during an era marked by volatility and dynamic social and political change. These strategic strengths; however, were also its weakness: the core economic and societal pillars would also play a key role in the Byzantine Empire's downfall.

The eventual collapse of the Byzantine Empire was a complex process influenced by numerous factors, including leadership dynamics, external threats, and internal religious friction that affected the consistency and effectiveness of its grand strategy. Bereft critical strategic outcomes, the Byzantines could not leverage their former strategic strength, with the once mighty empire sliding into decline from the 11th century. Central to the decline were the once robust pillars of economic management and religious patronage, the deterioration of which undermined the Empire's ability to sustain itself, adapt to emerging challenges, and maintain cohesion in the face of persistent threats. The grand strategy of the Byzantine Empire is a testament to how enduring national power can be maintained through effective strategic planning, and how it can be eroded by strategic miscalculations.

Grand Strategy and National Power

National power, the ability of a state to influence others, is central to grand strategy.⁹ Put simply, "the transmission of power in all its forms, in order to maintain policy, is the aim of grand strategy."¹⁰ Hans Morgenthau maintains that "international politics, like all politics, is a struggle for power,"¹¹ underscoring power's central role in state interactions. In the context of international relations, power dictates interactions between states, where the primary goal is to ensure national security and achieve dominance in an anarchic international system.¹² As a result, maximising power becomes a crucial objective in the ever-present shadow of state-on-state violence: nations ignore this at their peril.

The Byzantine experience underscores that economy-building and nation-building are crucial elements in developing and leveraging national power. Given this, the development and continuous refinement of grand strategy is essential in the pursuit and application of national power. Andrew Phillips argues that states develop and leverage national power through:

- State-building: Managing political discourse and power transitions.
- Economy-building: Leveraging economic potential.

Makers of Modern Strategy: From the Ancient World to the Digital Age (Princeton University Press, 2023). p. 33.

⁹ Nick Bosio, *On Strategic Art - A Guide to Strategic Thinking & the Australian Strategy Formulation Framework* (Canberra: Australian Department of Defence, 2024). p. 38.

¹⁰ Citing J. F. C. Fuller, David Gethin Morgan-Owen, "History and the Perils of Grand Strategy," *The Journal of Modern History* 92, no. 2 (June 1, 2020): 351–85, p. 356.

¹¹ Hans Morgenthau, *Politics Among Nations: The Struggle for Power And Peace* (New York: Alfred A. Knopf, 1949), p. 13.

¹² David A. Baldwin, "Realism," in *Power and International Relations, A Conceptual Approach* (Princeton University Press, 2016), 123–138.

- Nation-building: Inculcating societal identity and cohesion.¹³

Fundamentally, these elements are cyclic: enhancing one strengthens the others. Conversely, decline in any element weakens them all. This inter-connected nature highlights the need for balanced national power. Paul Kennedy posits that a state able to leverage an advanced economy benefits greatly over its rivals.¹⁴ Equally, Michael Mazarr argues that it is the qualities of a state's society, its ability to generate social cohesion that underpins national advantage.¹⁵ Together, economic and societal factors are the foundations from which all other elements of national power, such as military strength, are dependent on. By balancing economic resources and political environments, a state can navigate power dynamics and better position itself globally.

The rise and fall of the Byzantine Empire

The Byzantine Empire's history underscores how critical economic management is to national success and stability, illustrating the intricate link between economic health and state resilience. Likewise, the rise and fall of the Byzantine Empire was intrinsically linked to social cohesion: "To foster the people's willing spirit is often as important as to possess the more concrete forms of power."¹⁶ The Byzantine Empire's strong societal environment contributed to its early successes, but internal power struggles and religious friction played a role in its decline. Examining these factors reveals valuable lessons on how economic and societal stability can enhance a state's capacity to wield power effectively.

Economic Management and National Stability

The 4th century saw Constantinople emerge as the crucible between the East and West—a vital economic hub controlling key trade routes.¹⁷ At its peak, the Byzantine Empire benefited from vast commercial networks, productive lands, and taxpaying societies. However, it was these same networks, lands, and taxpayers that, at its lowest point, were lost and with them their economic contributions, all of which fuelled internal unrest. Economic wealth is a fundamental element of a state's ability to generate and sustain strategic courses of action such as warfare, diplomacy, and statecraft; therefore, it is of utmost importance that economic stability is a focal point for both internal and external policies.

Military conflict endured as a constant thread throughout Byzantine's history, be it through strategic choice or enemy invasion.¹⁸ Continuous cycles of conquest and defeat imposed significant economic costs on the Empire: "friction between great powers is almost always injurious to core interests."¹⁹ Regardless of involvement, war amongst states directly affects international trade, and hence the economic stability of not just protagonists, but also states linked to them through trade. By the 7th century, decades

¹³ Andrew Phillips cited by Bosio, *On Strategic Art - A Guide to Strategic Thinking & the Australian Strategy Formulation Framework*. p. 43.

¹⁴ Paul Kennedy, *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000*, Petite Bibliothèque Payot: Documents (Random House, 1987), p. xvii.

¹⁵ Michael J. Mazarr, "What Makes a Power Great: The Real Drivers of Rise and Fall," *Foreign Affairs* 101, no. 4 (July 1, 2022): 52–63. p. 52.

¹⁶ Basil Hart, *Strategy*, 2nd ed. (Faber and Faber, 1967), p. 322.

¹⁷ Peter Frankopan, *Silk Roads: A New History of the World*, Paperback edition. (Bloomsbury, 2016), p. 24.

¹⁸ John Julius Norwich, *A Short History of Byzantium* (Penguin, 2013).

¹⁹ Kevin Narizny, *The Political Economy of Grand Strategy* (Cornell University Press, 2007). p. 13, 19.

of conflict had reduced Byzantine territory to just Constantinople and its hinterland, with once-bustling international commerce in the Eastern Mediterranean effectively ceasing. As an outcome, trade within vibrant cities such as Athens ground to a halt: their economic centres all but abandoned.²⁰ In direct contrast, once-Roman lands such as Egypt—now in the hands of the emerging Islamic caliphate—were bustling, their cities “coursed with ideas, goods and money.”²¹ Throughout Byzantine history, trade and market control were crucial to the Empire's economic power and its ability to conquer or defend territory. Absent these economic lifelines, however, the Byzantine Empire struggled to sustain its military, finance diplomacy, and maintain internal cohesion.

At its peak, the key to Byzantine economic power centred on Constantinople's strategic location, which enabled the establishment and control of a vast agricultural and trade



Image: Parable of the Workers in the Vineyard. Unknown author - Byzantine gospel. Paris, National Library. Available at <https://gallica.bnf.fr/ark:/12148/btv1b105494556/f106.item>

network encompassing Europe, Africa and Asia.²² The 7th Century loss of Egypt to the Islamic Caliphate had profound economic and societal consequences for the Byzantine Empire given the critical importance of Egyptian agriculture in providing essential food supplies, tax revenues, and trade opportunities.²³ Equally as damaging, the loss of strategic control over lucrative Mediterranean trade to Italian city-states such as Venice and Genoa in the 13th century severely eroded Constantinople's economic stability.²⁴ The fall of the Byzantine Empire was directly attributable to the loss of these valuable economic resources—something the Empire could not recover from. The Byzantine Empire's history clearly demonstrates that strategic financial structures, trade networks and economic resources are indispensable for a nation's resilience, and their loss can

²⁰ Frankopan, *Silk Roads: A New History of the World*. p. 90.

²¹ Frankopan. p. 91.

²² Rowena Malpas, *The Fall of Civilizations: Lessons from History's Declines* (Richards Education, n.d.). p. 59.

²³ John L. Teall, “The Grain Supply of the Byzantine Empire, 330-1025,” *Dumbarton Oaks Papers* 13 (1959): 87–139.

²⁴ Frankopan, *Silk Roads: A New History of the World*. p. 156.

lead to downfall.

The robust economic foundation laid by the Byzantine Empire played a crucial role in their nation-building efforts. By fostering a stable economy, the Empire could invest in infrastructure, maintain the military, and support a thriving society. This economic stability allowed for effective governance and social cohesion, which were essential for the Empire's long-term stability and growth. Conversely, conflict and the cost of defending large borders disrupted trade and taxation, creating a vicious cycle of economic and societal instability. In this context, the interconnectedness of economy-building and nation-building becomes evident, as each component reinforces the other to create a resilient and prosperous state. Without a stable economic foundation, even the most sophisticated military or diplomatic efforts cannot sustain a state in the long term. This lesson remains relevant today, as modern nations address the complexities of economic security.

Social Cohesion and National Stability

The Silk Roads²⁵ of Eurasia facilitated not just trade but also the spread of religions, highlighting how faith and commerce intertwined to influence societal and political dynamics in the Byzantine Empire.²⁶ The societies of antiquity were highly receptive to divine guidance, where faith offered both explanations and solutions to every conceivable problem.²⁷ Across Eurasia, religions fought each other for audiences, wealth, and—above all—moral and political authority. For those in power, the desire to harness faith “was as simple as it was powerful: a society protected and favoured by the right god, or gods, thrived; those promising false idols and empty promises suffered.”²⁸ Emperor Constantine's adoption of Christianity in 312 CE unified Byzantine society, fostering cohesion under a common religion. However, it also introduced enduring divisions within the Church, which remained unresolved and plagued the Empire throughout its existence, despite the efforts of multiple emperors, including Constantine. By integrating Christianity into the Empire, Constantine's conversion enhanced internal stability and bolstered political authority.²⁹ Frankopan views this as “shrewd politics,”³⁰ with John Norwich also positing that Constantine's conversion was influenced by political considerations.³¹ Regardless of his motivations for conversion, Constantine's decision had a profound influence for both his empire and that of the Christian faith. In this aspect, Robert Jouston argues that Byzantine Orthodox Christianity stood as the real power behind Byzantine foreign policy.³²

Leveraging cultural links and religious beliefs were fundamental aspects driving Byzantine societal cohesion—and in tearing it apart. Throughout its history, differing Christian factions fought for hegemony both within the Byzantine Empire and across the Christian world. These religious disputes often led to significant political, economic, and social upheaval, impacting the stability of the Empire. Constantine, along with many Byzantine emperors, saw themselves as the custodians of Christianity, often portraying

²⁵ The Silk Roads of antiquity were a vast network of trade routes that connected the East and West, facilitating the exchange of goods, culture, and ideas across Eurasia. Frankopan.

²⁶ Frankopan.

²⁷ Frankopan. p. 28.

²⁸ Frankopan. p. 28.

²⁹ John Julius Norwich, *Byzantium: The Early Centuries*, 1990, p. 42.

³⁰ Frankopan, *Silk Roads: A New History of the World*. p. 41.

³¹ Norwich, *Byzantium: The Early Centuries*. p. 42.

³² Jouston, “The (Not so) Grand Strategy of the Byzantine Empire.” p. 70.

themselves as both political and religious leaders.³³ This dual role played a central part in the Empire's religious and political identity. Constantinople became a beacon of scholarship and religious devotion—second only to Jerusalem as the Empire's spiritual heart³⁴—influencing both Eastern Europe and the Middle East. For successive emperors, Christianity was not only a domestic political instrument in Byzantine society; it was also a source of influence over foreign empires and rulers. As Frankopan noted, “to strengthen the Empire was therefore to advance Christian salvation.”³⁵ This not only worked for the ruling emperors, but also the Church, whose interests were the most salient.

Byzantine emperors saw the Orthodox Church as a crucial ally in maintaining political, economic, and social stability, and they often sought to use the church's authority to legitimise their rule and enforce policies. For some, however, this lesson was lost and cost them their reign. Emperor Basiliscus acceded the throne in 475 CE, whereby he immediately drew the wrath of his subjects by imposing vicious taxation, and—critically—the wrath of the Church by “his ham-fisted attempts to impose Monophysitism throughout the Empire.”³⁶ Having angered both the people and the Church, it was only a matter of time before they moved against him, with Basiliscus forcibly deposed and exiled in 477 CE. As Basiliscus' experience demonstrates, the intertwining of religious and political power could result in the suppression and persecution of those holding differing beliefs—including emperors—thus destabilising the Empire.

The Byzantine Empire's strategic use of religion and cultural integration underscores the importance of fostering societal and cultural identity. Christopher Berg succinctly expresses this point, arguing that:

A threat from within was more dangerous than an enemy at the gates and the Byzantines understood that fact all too well. Keeping the people fed, clothed, and protected was expensive but necessary in order to prevent civil unrest.³⁷

In the context of imperial conquest and engendering control over vanquished populations, Berg's point is highlighted by the Byzantine maxim: “When a populous city is taken, it is important to leave the gates open, so that the inhabitants may escape and not be driven to utter desperation.”³⁸ Psychology, whether it be collective or individual, plays a key role in influencing societies and underpinning societal cohesion—particularly those newly conquered who need to be integrated into society, not alienated from it.³⁹ Leaders of modern nations can learn much from Byzantine history, particularly in how their approach to leadership directly affects their ability to build cohesive and stable communities within diverse, multi-cultural societies.

³³ James C. Skedros, “‘You Cannot Have a Church Without an Empire’: Political Orthodoxy in Byzantium,” in *Christianity, Democracy, and the Shadow of Constantine*, ed. George E. Demacopoulos and Aristotle Papanikolaou (Fordham University Press, 2017), 219–31, <http://www.jstor.org.ezproxy-b.deakin.edu.au/stable/j.ctt1gn6b41.14>. p. 220.

³⁴ Frankopan, *Silk Roads: A New History of the World*. p. 42.

³⁵ Edward Luttwak, *The Grand Strategy of the Byzantine Empire* (Cambridge, Mass: Belknap Press, 2009), p. 113.

³⁶ John Julius Norwich, *A Short History of Byzantium* (Penguin, 2013), p. 53.

³⁷ Christopher Berg, “Book Review: The Grand Strategy of the Byzantine Empire,” *De Re Militari*, 2011. Accessed 05 March 2025 from https://www.deremilitari.org/REVIEWS/Luttwak_GrandStrategyByzEmp.htm.

³⁸ Luttwak, *The Grand Strategy of the Byzantine Empire*. p. 286.

³⁹ Walter Russell Mead, “Thucydides, Polybius, and the Legacies of the Ancient World,” in *The New Makers of Modern Strategy*, ed. Hal Brands, *From the Ancient World to the Digital Age* (Princeton University Press, 2023), 41–66, p. 46.

Lessons for students of strategy

The Byzantine Empire's achievements and missteps in economy-building and nation-building present enduring lessons for generating and maintaining national power. In this context, a compelling comparison can be drawn between the Persian Empire and Byzantine Emperor Maurice. Fuelled by a strong economy ironically sustained by regular Byzantine subsidy payments—a legacy of foreign policy failure—and a softer, tolerance-based approach to practicing religion, Persian rulers oversaw a period of relative peace that went hand in glove with economic prosperity within the Empire.⁴⁰ Across Persia, numerous new cities sprang from this success, each resplendent with infrastructure and monuments built for the people.⁴¹ Tied to this was an increase in long-distance trade, particularly in luxury goods, with the resulting societal prosperity driving a vibrant commercial boom. The Persian experience underscores the importance of managing both economic and social factors for sustained prosperity. The link between economic growth and social cohesion is clear, as demonstrated by the Persian Empire's success in fostering a vibrant and prosperous society through economic development and religious tolerance.

In stark contrast, the Byzantine Empire under Emperor Maurice illustrates the consequences of neglecting these factors. For Maurice, his fundamental constraint was a lack of finances. His predecessors had left the Empire near-bankrupt, with ongoing subsidy payments to rivals such as Persia and conflict across his large frontiers leaving him unable to reconstitute the Byzantine treasury. The result of this Norwich describes as a “parsimoniousness which gradually became an obsession.”⁴² His reduction of military rations by a quarter led to mutiny in 588; his refusal to ransom twelve thousand Byzantine prisoners in 599 led to their deaths; and, the final straw for the military, his insistence on leaving troops in inhospitable winter conditions in 602 ignited riots in Constantinople which forced Maurice to flee. Eventually captured, Maurice was witness to the deaths of his four sons, before he was executed.

History presents Maurice as a wise Emperor: “[he] left the Empire immeasurably stronger than he found it.”⁴³ Regardless, the lesson of his reign remains clear, the direct link between the economy and prosperity is keenly felt by the people: If you make them paupers, they will make you pay. “Had [Maurice] allowed his soldiers only a little more bread, or his people just a few more circuses, he would have escaped his fate.”⁴⁴ Where periods of Byzantine affluence heralded the “large-scale building of Churches ... and the founding of institutions such as law schools”⁴⁵—all for the benefit of the Empire and its people—depressing economic prosperity led to dire consequences, with the fate of Emperor Maurice being just one example.

As a modern case study drawing on lessons from the Byzantine Empire, particularly under Emperor Maurice, contemporary Russia faces challenges that highlight the strategic interplay of economic and social dynamics. In both cases, Orthodox Christianity remains a core pillar of national identity.⁴⁶ Despite this clear societal strength, under economic strain even the most robust societies can falter. Russia's conflict in Ukraine mirrors Maurice's costly military campaigns, compounding fiscal

⁴⁰ Frankopan, *Silk Roads: A New History of the World*. p. 56.

⁴¹ Frankopan. p. 56.

⁴² Norwich, *A Short History of Byzantium*. p. 87.

⁴³ Norwich. p. 88.

⁴⁴ Norwich. p. 88.

⁴⁵ Frankopan, *Silk Roads: A New History of the World*. p. 127.

⁴⁶ Alexey D. Krindatch, “Changing Relationships between Religion, the State, and Society in Russia,” *GeoJournal* 67, no. 4 (2006): 267–82, p. 280.

burdens through sanctions, inflation, and economic stagnation.⁴⁷ Maurice's parsimoniousness alienated his people, sparking rebellion and his eventual downfall—a cautionary tale for Russia, where poverty and unemployment threaten to destabilise the traditionally resilient Russian community. These historical and modern parallels underscore a vital lesson for Russia: sustained fiscal stress undermines societal cohesion and stability. The cracks appearing in the Russian Orthodox community mirror the tensions that surfaced in the Byzantine Empire during times of fiscal and social strain, illustrating how unchecked economic hardships can undermine even the strongest societal institutions.

Throughout Byzantine history, the interdependence of economic stability and social cohesion played a pivotal role in the Empire's fortunes: harmonising these elements was crucial for maintaining national power. In the anarchic realm of international politics, the ability of leaders to leverage economic and societal strengths directly influences state success. As the lessons from the Byzantine Empire underscore—and Russia's current domestic situation indicates—integrating robust economy-building and inclusive nation-building initiatives is imperative for generating and projecting national power, offering timeless insights for contemporary students of strategy.

Conclusion

The Byzantine Empire's longevity highlights the critical importance of robust economy-building and inclusive nation-building as pillars of national power. Its economic success stemmed from financial stability, effective resource management, and adaptable trade networks. Similarly, its societal cohesion—anchored in religious integration—ensured internal stability and sustained influence abroad. However, its decline reveals that neglecting these foundations renders states vulnerable to decay.

The interplay of economic and social stability has defined the trajectory of states throughout history. Prosperity accompanies those who align these factors, while instability and conflict await those who fail: the decay of civilisations is often precipitated by overextension of resources and the accumulation of political and social tensions.⁴⁸ The Byzantine Empire does not stand alone as a case study where economic and social factors coalesce. The rise of Islam and its caliphates from the 7th century highlights the success of harmonising economic and social policies. By uniting diverse regions under a cohesive administration, currency, and language, these caliphates fostered stability and innovation.⁴⁹ Conversely, the British Empire's post-World War II decline illustrates the failure to adapt to shifting economic and societal dynamics, as decolonisation and economic strain eroded its global dominance.⁵⁰ For those willing to learn, history consistently shows that alignment—or lack thereof—between economic and social systems is a defining factor in determining the trajectory of empires and states.

This paper has clearly articulated the critical strategic roles of economy-building and nation-building. Further, it has provided stark evidence as to why these elements serve as key lessons for students of strategy. For modern strategists, understanding the interconnectedness of economic and societal factors across all aspects of governance is essential. Effective economic management akin to the Byzantine's can provide financial stability that supports strong social programs and institutions. Additionally, the Byzantine integration of religion and statecraft exemplifies how shared cultural and ideological frameworks can unify diverse populations. Drawing from such lessons,

⁴⁷ Rebecca Nelson, "The Economic Impact of Russia Sanctions," Congressional Research Service (Washington, February 20, 2025).

⁴⁸ Malpas, *The Fall of Civilizations: Lessons from History's Declines*. p. 3.

⁴⁹ Frankopan, *Silk Roads: A New History of the World*, p. 73-75.

⁵⁰ Malpas, p. 119.

contemporary planners and policymakers can develop nuanced strategies that integrate these elements to strengthen long-term stability and prosperity.

Bibliography

Baldwin, David A. "Realism." In *Power and International Relations*, 123–38. A Conceptual Approach. Princeton University Press, 2016.

Berg, Christopher. "Book Review: The Grand Strategy of the Byzantine Empire." *De Re Militari*, 2011.
https://www.deremilitari.org/REVIEWS/Luttwak_GrandStrategyByzEmp.htm.

Bosio, Nick. *On Strategic Art - A Guide to Strategic Thinking & the Australian Strategy Formulation Framework*. Canberra: Australian Department of Defence, 2024.

Frankopan, Peter. *Silk Roads: A New History of the World*. Paperback edition. Bloomsbury, 2016.

Hart, Basil. *Strategy*. 2nd ed. Faber and Faber, 1967.

Joustra, Robert. "The (Not so) Grand Strategy of the Byzantine Empire." *Review of Faith and International Affairs* 8, no. 3 (January 1, 2010): 69–70.

Kennedy, Paul. *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000*. Petite Bibliothèque Payot: Documents. Random House, 1987.

Krindatch, Alexey D. "Changing Relationships between Religion, the State, and Society in Russia." *GeoJournal* 67, no. 4 (2006): 267–82.

Luttwak, Edward. *The Grand Strategy of the Byzantine Empire*. Cambridge, Mass: Belknap Press, 2009.

Malpas, Rowena. *The Fall of Civilizations: Lessons from History's Declines*. Richards Education, n.d.

———. *The History of Empires: Rise and Fall of Great Powers*. Richards Education, n.d.

Mazarr, Michael J. "What Makes a Power Great: The Real Drivers of Rise and Fall." *Foreign Affairs* 101, no. 4 (July 1, 2022): 52–63.

Mead, Walter Russell. "Thucydides, Polybius, and the Legacies of the Ancient World." In *The New Makers of Modern Strategy*, edited by Hal Brands, 41–66. From the Ancient World to the Digital Age. Princeton University Press, 2023.

Morgenthau, Hans. *Politics Among Nations: The Struggle For Power And Peace*. New York: Alfred A. Knopf, 1949.

Narizny, Kevin. *The Political Economy of Grand Strategy*. Cornell University Press, 2007.

Nelson, Rebecca. "The Economic Impact of Russia Sanctions." Congressional Research Service. Washington, February 20, 2025.

Norwich, John Julius. *A Short History of Byzantium*. Penguin, 2013.

———. *Byzantium: The Early Centuries*, 1990.

Silove, Nina. "Beyond the Buzzword: The Three Meanings of 'Grand Strategy'." *Security Studies* 27, no. 1 (January 1, 2018): 27–57.

Skedros, James C. "'You Cannot Have a Church Without an Empire': Political Orthodoxy in Byzantium." In *Christianity, Democracy, and the Shadow of Constantine*, edited by George E. Demacopoulos and Aristotle Papanikolaou, 219–31. Fordham University Press, 2017.

Slack, Keith. "The Information Lever of Power." *Freeman Papers*, August 21, 2024.

Teall, John L. "The Grain Supply of the Byzantine Empire, 330-1025." *Dumbarton Oaks Papers* 13 (1959): 87–139.

