SOCIAL CYBER INSTITUTE

Research Paper 2/25

CYBER CIVIL PREPAREDNESS AND RESILIENCE: TWIN STRATEGIC IMPERATIVES

Gary Waters
Greg Austin

JULY 2025

Acknowledgments

The authors would like to acknowledge the contribution of the Integrated Institute for Economic Research – Australia (IIER-A) in stimulating and informing this paper. We also thank Zara Yap for her support in publication.

About the authors

Dr Gary Waters is a Distinguished Fellow with the Social Cyber Institute. Gary served for just over 33 years in the Royal Australian Air Force (retiring early as an Air Commodore); served as a senior public servant in Defence for a further four years; and worked in the private sector as Head of Strategy for Jacobs Australia for seven years. He retired in 2013 and now works on a casual basis as an independent strategy consultant. He has written over twenty books or papers on diverse topics, including aerospace; logistics; intelligence, surveillance and reconnaissance; information superiority; cyber security; and cyber warfare. Gary continues to pursue his interests in strategy and high-level policy, and in emergent and disruptive technologies, including those associated with digital transformation and cyber security. He is a Fellow of the Royal Melbourne Institute of Technology (graduating with majors in accounting and economics); a graduate of the United Kingdom's Royal Air Force Staff College; a graduate of the University of New South Wales, with an MA (Hons) in history; a graduate of the Australian Institute of Company Directors; and a graduate of the Australian National University with a PhD in political science and international relations. He is currently a founding director (since 2018) of the Integrated Institute for Economic Research – Australia. He is also the strategic advisor (since 2022) to the CEO and Chairman of the Board of the Critical Infrastructure Information Sharing and Analysis Centre – Australia.

Professor Greg Austin has diverse international experience in cyber policy research and international security policy: Senior Fellow and head of the Program on Cyber Power and Future Conflict with the International Institute for Strategic Studies (IISS) and Professor of Cyber Security, Strategy and Diplomacy with the University of New South Wales Canberra. His academic career, including a Senior Visiting Fellowship in the Department of War Studies at Kings College London, has included twelve books on international security, as author or editor, and leadership of several international research projects. He is currently an adjunct professor in the Australia China Relations Institute at the University of Technology Sydney. His service as a research leader for prominent global NGOs, such as the International Crisis Group and the EastWest Institute, has seen him work from Brussels and London with leading governments at Ministerial level (Russia, China, UK, India, United States, Turkey, Australia), major international organisations at leadership level (United Nations, International Atomic Energy Agency, R20 for Climate Action), and leading corporations (AT&T, BT, Perot Systems). He has consulted for the UK Cabinet Office, the UK Ministry of Defence, the Foreign and Commonwealth Office, the European Commission, and the Australian Department of Foreign Affairs and Trade. He began his career in Australian public service roles, including posts in Canberra and Hong Kong, parliamentary committees, and ministerial staff. Austin has a Ph D in international relations and a Master of International Law, both from the Australian National University.

Social Cyber Institute

Discussion Paper 2/25

CYBER CIVIL PREPAREDNESS AND RESILIENCE: TWIN STRATEGIC IMPERATIVES

Gary Waters

Greg Austin

July 2025

Executive Summary

On June 1, 2025, the Australian Government released a national cyber response plan emphasising more than previously the importance of preparedness. The new focus on preparedness in this cyber plan marks a significant step forward. The plan introduces a four-tier classification of cyber incidents, with "nationally catastrophic" being the most severe. The idea is that the country needs to be ready to address country-wide cascading non-cyber effects arising from such an incident. While Australia is well-placed to deal with a range of cyber emergencies, it is not as prepared as it needs to be for one reaching the level of a national catastrophe.

The agency responsible for leading the response to a cyber catastrophe, according to the plan, is the National Emergency Management Agency (NEMA), set up in 2022. It would be supported by the National Office of Cyber Security (NOCS), set up in 2023. NOCS takes the lead in cyber incidents of lower severity. Yet, the NEMA and NOCS websites have no significant public discussion of how to prepare for the catastrophic cyber incident. We would expect the government to produce further analysis in the near future of what these preparedness plans might look like. They would need to include not only roadmaps for technical responses inside cyber systems to the catastrophic incident but also action plans for consequence management in key economic sectors, the delivery of essential services and mobilisation of the citizenry behind inevitably unpopular government decisions. Preparedness also touches on emergency law enforcement authorities, regulatory response for business, crisis communications, and geopolitical attribution -- all of which lie well outside the current scope of the Department of Home Affairs and/or the Department of Defence.

Also in June 2025, Admiral Johnston, Chief of Australia's Defence Force, emphasised the need for a change in national resilience and preparedness across military and civil sectors due to emerging threats. Preparedness involves getting ready for crises, while resilience is the capability to mitigate and recover from crises. Both are essential and mutually reinforcing, with community participation being crucial. The prominence of cyber-attacks in recent global conflicts underscores the urgency of improving Australia's cyber preparedness for extreme crisis.

This paper outlines considerations to support Australian stakeholders in developing this new paradigm both for cyber response and for the mitigation of non-cyber impacts in the circumstances of a national cyber catastrophe. We argue for placing cyber civil preparedness and resilience alongside military defence and diplomacy at the top of national security policy and making consequential changes in the machinery of government. This would include a national cyber resilience strategy to manage the consequences of catastrophic cyber emergencies.

Recommendations

The paper makes five recommendations: conducting a national assessment of cyber civil preparedness and resilience, establishing a dedicated office of cyber threat intelligence focused on the economy and society, submitting triennial national assessments to the Parliament, building a national cyber catastrophe readiness framework, and developing a new doctrine and legal authorities for programs in national civil preparedness national cyber resilience.

Contents

1. Introduction

On 1 June 2025, the Australian Government released a national cyber response plan which acknowledges for the first time the centrality of a concept of nationwide preparedness, especially in the economy and society.[1] The pamphlet is however quite brief, and the attention paid to detail is limited. The document discusses activities to build continuously on pre-existing foundations "to prepare the Australian Government and the nation to respond to cyber security incidents" (p.20). The plan acknowledges that the country needed to be able to respond to a "catastrophic cyber incident", a new formulation appearing in a major Australian cyber policy document for the first time in 2025.[2] This document represents a consolidation of the government's commitment to whole-of-society cyber preparedness, but its focus on preparedness in the plan also breaks important new ground by committing the government more explicitly to address front-and-centre, cascading non-cyber effects arising from cyber incidents.

In June 2025, the Chief of Australia's Defence Force, Admiral Johnston, called for a change by Australia on "how we think of national resilience and preparedness" because of the emerging need to consider wartime military operations mounted from Australian territory.[3] The continuing prominence of cyber-attacks and cyber defence in the Russia/Ukraine conflict,[4] a total blackout on the Iberian peninsula in April 2025 for around half a day, and the near total outage of Iran's internet at the time of the US bombing in June 2025[5] further underscore the urgency of improving Australia's cyber preparedness.

A new posture has to be rooted in thorough and regular analysis of dependencies within complex systems where catastrophic failure might undermine national resilience. The growing cyber dependencies of today's environment makes an extreme national cyber crisis almost inevitable. Threats are escalating, systems are becoming more complex, and Australia is not making the corresponding expansive adjustments in cyber preparedness and resilience policies and associated competencies at the required pace.

The dramatic turn in the AUSCYBERPLAN of 2025 to a relatively new category of severity for a cyber incident – a "nationally catastrophic cyber incident" – has major implications for policy. It is part of a four-tier classification of cyber crisis, as summarised in Table 1. This applies to cyber emergencies the classification of all national emergencies that came into use in 2024 as part of broader national reforms.[6]

Table 1: Australia's four-tier response classification of cyber incidents

Localised	Low to moderate impact, managed within a single agency or jurisdiction.
Significant	High impact, may affect multiple agencies or critical infrastructure, requires broader coordination.
Nationally Significant	Very high impact, cross-jurisdictional, may threaten national interests, requires whole-of-government coordination.
Nationally Catastrophic	Extreme to catastrophic impact and complexity, likely to overwhelm national systems and resources, requires Prime Ministerial leadership and National Emergency Management Agency (NEMA) coordination. This tier anticipates incidents with wide-ranging, severe consequences across multiple jurisdictions and critical infrastructure, involving most or all government portfolios.

[1] Australian Government. National Office of Cyber Security, "Australian Cyber Response Plan (AUSCYBERPLAN)", 1 June 2025, https://www.homeaffairs.gov.au/cyber-security-subsite/files/australian-cyber-response-plan.pdf.

[2] The concept of nationally significant catastrophic incident appears in the 2024 National Crisis Management Framework. Its first application in a cyber policy document appears to be in the "Communications Sector Playbook", p. 2, issued by the NOCS in March 2025. https://www.homeaffairs.gov.au/cyber-security-subsite/files/communications-sector-playbook.pdf.

[3] Olivia Caisley and Stephen Dziedzic, "ADF chief warns Australia must be ready to launch combat operations from home", *ABC News*, 4 June 2025. See https://www.abc.net.au/news/2025-06-04/defence-chief-warns-australia-must-be-ready-for-combat/105374804

[4] Mart Noorma, Serhii Demetrius and George Dubynskyi, "A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) & National Security and Defence Council of Ukraine, February 2024, https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf..

[5] Matt Burgess, "Iran's Internet Blackout Adds New Dangers for Civilians amid Israeli Bombings", *Wired*, 18 June 2025, https://www.wired.com/story/iran-internet-shutdown-israel/.

[6] "Australian Cyber Response Plan", pp. 8-9.

This paper reviews the implications of shifts in Australia's cyber crisis policy contained in the AUSCYBERPLAN 2025. It looks first at the concept of preparedness and what it implies for policy, before looking at resilience policy and the specific challenges of critical infrastructure. The paper has a brief conclusion with several recommendations.

2. Civil preparedness for a cyber catastrophe

There is strong and growing support in the scholarly research community for a much sharper distinction between cyber civil preparedness and other policy responses to national emergencies in cyberspace, especially resilience building.[7] Policy analysis of national cyber catastrophes by scholars and most governments remains underdeveloped. By contrast, analysis of pandemic preparedness is, for understandable reasons, highly developed and provides essential signposts for the case of cyber catastrophe where similar policy work is only at a very elementary level of development in Australia.

2.1 Pandemic preparedness in Australia

Australia's pandemic preparedness strategy now features strengthened health planning and readiness, economic scenario planning, and social resilience—underpinned by sovereign vaccine production, a new Australian Centre for Disease Control (CDC) , inclusive support for vulnerable groups, and holistic, coordinated governance. We can divide these heightened readiness plans into two distinct if interconnected domains: the country as a whole and the health system. Most of these types of activity do not yet exist in Australia for response to a nationally catastrophic cyber-induced crisis.

The Covid-19 inquiry noted the positive developments in the national emergency management framework post-Covid that were announced in 2024, but in doing so also noted that there had been gaps.[8] These included a need for "enhancing scalability, including for the management of severe to catastrophic crises" and clarification of governance arrangements, "such as the important whole-of-government coordination roles of the National Emergency Management Agency and the Department of the Prime Minister and Cabinet". The final report of the Covid-19 inquiry had a heavy emphasis on preparedness.[9]

2.1.1 Country-wide preparedness

Economic Toolkit and Scenario Planning: The 2024 COVID-19 Response Inquiry recommended the regular updating of an "economic toolkit," comprising scenario-based planning to deal robustly with a variety of pandemic-driven shocks.[10] This approach seeks to ensure continuity of essential services and effective fiscal interventions (e.g., cost-of-living relief, business support) when a pandemic disrupts normal activity. The report noted a consistent view among submissions that "emphasis on measures to control the virus often failed to account for broader economic impacts".[11]

Cross-Government Coordination: Preparedness is enhanced by integrating economic impact assessment directly into national crisis response structures, leveraging the capacity of departments beyond health to respond quickly and maintain economic stability.[12]
Equity and Inclusiveness: Official statements and inquiry findings have underscored the disproportionate pandemic impact on Aboriginal and Torres Strait

---

[7] Civil-Military Cooperation Centre of Excellence NATO, "Resilience through Civil Preparedness", 2018, https://www.cimic-coe.org/wp-content/uploads/2025/01/factsheet-resilience-through-civil-preparedness.pdf; Parawai, Yusuf Ali, Rudy A,G. Gultom, Luhut Simbolon, Anak Agung Ngurah Gunawan, "A Novel Socio-Technical Framework for Enhancing Cyber Crisis Management Capabilities" *International Journal of Safety and Security Engineering*, volume 14, issue 4, 2024, https://ssrn.com/abstract=4943118 or http://dx.doi.org/10.18280/ijsse.140415; Selena Mahmood, Mehmood Chadhar, and Selena Firmin, "Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective", *Applied Sciences*, 14(24), Article 11610, December 2024, https://www.mdpi.com/2076-3417/14/24/11610; Grethe Østby, Lars Berg, Mazaher Kianpour, Basel Katt, and Stewart Kowalski, "On the cyber-emergency preparedness in a resilient organization", Proceedings of the ESREL 2023 Conference, published 2024, https://biopen.bi.no/bi-xmlui/bitstream/handle/11250/3103216/ESREL2023_ESREL2023_Paper_only_17.pdf; M. Bristow and Irving Lachow, 'Past is Prologue: Creating a Civil Defense Mindset to Address Modern Cyber Threats', The MITRE Corporation, May 2025, https://www.mitre.org/sites/default/files/2025-05/PR-25-00303-01-Creating-Civil-Defense-Mindset-Address-Modern-Cyber-Threats.pdf;; European Parliamentary Research Service (2025) 'EU Preparedness: From Concept to Strategy?', 2025, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)772898.

[8] Commonwealth of Australia, "Final Report of the COVID-19 Response Inquiry: Lessons for Future Pandemic Preparedness, Canberra, 2024, p. 303, https://www.pmc.gov.au/sites/default/files/resource/download/covid-19-response-inquiry-report.pdf.

[9] Ibid. pp. 7-13.

[10] Ibid. p. 8. The report has 34 references to an economic toolkit.

[11] Ibid. p. 513.

[12] Ibid. p. 76.

Islander communities, culturally and linguistically diverse populations, people with disabilities, and others facing social disadvantage.[13] Pandemic plans should require targeted measures to support these groups, including modular strategies for education and high-risk settings formed in partnership with affected stakeholders.[14]

Building Trust and Social Capital: Ministers and inquiry reports stress the pivotal importance of restoring trust, social cohesion, and resilience in the wake of COVID-19.[15] This involves transparent communication, integrated human rights and mental health considerations, and strategies for long-term recovery.

Holistic Playbook: Inspired by the Covid-19 inquiry recommendations, Australia is moving towards a "high-level playbook" that integrates health, economic, and social strategies, with scenario testing and stress-testing of plans as standard practice.[16] National Cabinet is now aware of the value of its receiving cross-cutting expert advice to ensure all-of-society impacts are addressed in real time.[17]

2.1.2 Health System Preparedness

The proposals and policies from the health sector outlined below are presented as cognates of policy for the cyber system.

Local Vaccine Manufacturing and Sovereignty: A central pillar of Australia's preparedness is ensuring sovereign capability in vaccine manufacturing. The December 2024 opening of the Moderna Technology Centre in Melbourne was heralded by Health Minister Mark Butler as giving Australia "the capacity to produce up to 100 million doses of locally made vaccine in a pandemic response scenario," thus reducing reliance on global supply chains and providing rapid access when needed . This facility also supports research partnerships to bolster innovation and workforce capability.[18]

Australian Centre for Disease Control (CDC): A new CDC, announced with $251 million in funding, will serve as a national hub for pandemic planning, response, and real-time surveillance.[19] Its role includes leading disease tracking systems (including wastewater surveillance) and delivering independent, transparent advice to government and the public to reinforce trust.

National Health Strategies and Coordination: Ministerial remarks at the 2025 Immunisation Conference emphasised a "whole-of-system approach" involving all levels of government, supported by a national immunisation strategy that targets timely vaccinations, improved access for disadvantaged groups, and preparation for new vaccine technologies.[20] Coordination with research and engagement with states, territories, and international partners are integral.

2.2 Cyber catastrophe preparedness in Australia

The Covid-19 pandemic was a national catastrophe for Australia,[21] even though it fared better than many countries. The levels of preparedness for a pandemic before Covid-19 struck and those developed since look far more sophisticated than those fragments of policy the country has for a nationally catastrophic cyber crisis.

The new policy announced on 1 June 2025 introduces a strange institutional divergence between the Cyber Coordinator and the National Emergency Management Agency (NEMA).

---

[13] "Final Report of the COVID-19 Response Inquiry".
[14] C.R. Brown, J.M. Blakely and M.C. Klebe, **"**Preparing Australia for future pandemics: Strengthening trust, social capital and resilience", *Medical Journal of Australia, 222*(10), 2025, 471-478.
[15] "Final Report of the COVID-19 Response Inquiry.
[16] Ibid. p. 3.
[17] Ibid. p. 17.
[18] M. Butler, "Speech: Opening of the Moderna Technology Centre – Building Sovereign Vaccine Capability", [Speech transcript]. Department of Health and Aged Care., 4 December 2024, https://www.health.gov.au/ministers/the-hon-mark-butler-mp/media/minister-for-health-and-aged-care-speech-4-december-2024-0.
[19] Australian Government. Department of Health and Aged Care. (2025),"Establishing the Australian Centre for Disease Control", Canberra, 2025, https://www.cdc.gov.au/sites/default/files/2025-01/establishing-the-australian-centre-for-disease-control.pdf.
[20] M. Butler, "Keynote address: Communicable Diseases and Immunisation Conference – Launch of the National Immunisation Strategy for Australia", Department of Health and Aged Care, 12 June 2025, pp. 2-3, https://www.health.gov.au/ministers/the-hon-mark-butler-mp/media/keynote-communicable-diseases-immunisation-conference-2025.
[21] "Final Report of the COVID-19 Response Inquiry" p. 10: "Australia recorded the biggest drop in employment on record".

The new Cyber Response Plan sits within the Australian Government Crisis Management Framework (AGCMF). Under the AGCMF the Cyber Coordinator, as the Lead Coordinating Senior Official, leads the Australian Government's coordination response to manage consequences to three categories of cyber incidents. The Cyber Coordinator is supported by the National Office of Cyber Security (NOCS), as the Australian Government Coordinating Agency, and also leads whole-of-government cyber security incident preparedness efforts.

In a catastrophic cyber crisis (the most serious of four levels), the lead for coordination passes to the National Emergency Management Agency (NEMA), under the leadership of the Prime Minister.[22] In this case, the Cyber Coordinator is not the lead. There is little public evidence of NEMA planning to take on this role in an extreme cyber crisis. Of note, the NEMA website contains only four mentions of "cyber", one of which relates to indigenous art and the other three being generic references.[23] If NEMA is doing anything to prepare for its role in a nationally catastrophic cyber-attack, it is not immediately apparent.

The response activities that would need to be coordinated across governments and stakeholders include mitigation of the cyber breaches or incidents, consequence management activities focused on impacts of the cyber incident outside cyberspace, law enforcement activities, regulatory response activities, crisis communications (public and cross-government), and attribution.

This latest Australian evolution in planning for national cyber emergencies comes nine years after the United States set a good example[24] and at least seven years after Australian scholars made a concerted effort to put this more firmly on the government's agenda.[25] The US policy is seated in a broad framework of civil preparedness[26] that references national emergency (and cyber crisis) not just cyber incidents. Moreover, the US has declared a national emergency in cyberspace each year beginning in 2015 referencing sustained campaigns of cyber-attack, not response to a single incident.[27] In the Australian case in 2025, and taking a lead from the Defence Force Chief as mentioned earlier, the authors of this paper see the existing threat environment and therefore the necessary policy response as aligning much more around the concept of civil preparedness of the country as a whole to contain and defeat cyber campaigns in addition to building resilience against individual incidents.

The US case is premised on a web of interdependent policies and legislative authorities, ultimately dependent on the President's declaration of a national emergency in cyberspace, with the executive responses and national coordination laid out in the associated declaration.

Australia has a National Emergency Declaration Act which came into force in 2020.[28] Its reach is quite limited in practice compared with the US regime, but it does allow the Prime Minister to compel Commonwealth entities to provide relevant assessments. It addresses emergency preparedness directly, alongside risk reduction, emergency response, and emergency recovery. It is couched in terms of national harm which "has a significant national impact because of its scale or consequences" for people, animals or plants, the environment, critical infrastructure, and the continuity of essential services. The Act does not limit itself by reference to any particular sector, such as cyberspace. This Act incorporates existing legislative authorities in at least 30 other acts or administrative orders, emergency provisions or guidelines.

One could also compare the approaches of Japan and Australia for example, with the former having a more sophisticated machinery of government (a dedicated Ministerial Council) for national emergency

---

[22] "Australian Cyber Response Plan (AUSCYBERPLAN)", p. 9.
[23] Keyword search on "cyber": https://www.nema.gov.au/search?keyword=cyber.
[24] United States Government. Department of Homeland Security, "National Cyber Incident Response Plan", December 2016, https://www.cisa.gov/sites/default/files/2023-01/national_cyber_incident_response_plan.pdf.
[25] See Adam Henry and Greg Austin. "New guidelines for responding to cyber attacks don't go far enough", The Conversation, 18 December 2018, https://theconversation.com/new-guidelines-for-responding-to-cyber-attacks-dont-go-far-enough-108908. Austin and Henry organised an international conference on the subject with US, UK and NATO representatives at the University of New South Wales Canberra in November 2018. The papers from that conference were published in Greg Austin (ed), *National Emergencies in Cyberspace: the Return of Civil Defence*, Routledge 2020.
[26] United States, "National Preparedness System", Department of Homeland Security, 31 July 2020, https://www.fema.gov/emergency-managers/national-preparedness/system.
[27] See United States Government. Federal Register, Executive Order 13694 of April 1, 2015, https://www.federalregister.gov/executive-order/13694.
[28] AUSTLII, "National Emergency Declaration Act 2020 (No. 128, 2020)", https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/num_act/neda2020276/.

management and holding regular Cabinet-level audits (inspections) of likely impacts once or twice per year since 2018.[29] In 2025, Japan created new legal authorities in cyber emergencies to attack and disable foreign cyber attacks among a raft of crisis response measures.[30]

There is a major disconnect in the preference of many governments, including Australia, to frame policy in terms of a "cyber incident" (implying a containable crisis event) when in fact most countries have been subject to sustained and highly damaging cyber campaigns (multi-vector, multi-wave attacks) by state actors beginning in the early 2000s.[31] Major powers (China, the US and Russia) are planning such attacks in full scale war or in anticipation of it. As the Russian war against Ukraine has demonstrated, effects of cyber operations on civil sector interests can be substantial.

The impacts of Russian cyber operations against Ukraine have been disruptive but not catastrophic.[32] This has led some to conclude that "a combination of private sector innovation, state coordination, and emerging doctrine have made the cyber domain defence dominant".[33]

On the other hand, there is a case to be made that these analyses are "sometimes overly focused on their physical or financial impact, overlooking the individual, societal, and environmental effects, including implications for psychological and social well-being".[34] The impacts of the war (not just cyber) beginning in February 2022 , caused 64% of small and medium enterprises to suspend or close business activities.[35] By October 2023, only 9.6% of the companies that suspended their trading were at risk of closure.

So what therefore can Australian stakeholders understand by the new orientation of the Australian government to prepare for a "nationally catastrophic" cyber emergency? This topic was addressed in 2018 by a small international conference over two days at the University of New South Wales under the rubric of "cyber storm", with one of the current authors proposing the concept of "cyber blitzkrieg".[36] The conference revealed that most specialists and government officials regard a "catastrophic cyber emergency" as unlikely, "they cannot agree what priority to accord it in national strategies".[37]

---

[29] See Prime Minister's Office Japan, "National Resilience Promotion Headquarters", 6 June 2025, https://japan.kantei.go.jp/103/actions/202506/06kokudo.html . See also Cabinet Office, Government of Japan, *White Paper on Disaster Management in Japan 2024*. (Japanese edition published March 2025; English edition pending release as of July 2025). For English-language reference, the most recent publicly available edition is *White Paper on Disaster Management in Japan 2023*, https://www.bousai.go.jp/en/documentation/white_paper/pdf/2023/R5_hakusho_english.pdf. Available at: https://www.bousai.go.jp/en/documentation/white_paper/index.html. See also Ishiwatari, M. (2020) 'Engaging National and Local Governments in Japan: Coordinating Mechanisms of Disaster Management', *Natural Hazards Review*, 22(1), 04020059. https://ascelibrary.org/doi/10.1061/(ASCE)NH.1527-6996.0000423.

[30] See Tora Dvorin, "Japan's Active Cyber Defense Law: AEV & Resilience". SafeBreach, 12 June 2025, https://www.safebreach.com/blog/japan-active-cyber-defense-law/.

[31] See the reports of the US National Counter Intelligence Executive for these years, "ONCIX Reports to Congress: Foreign Economic and Industrial Espionage", https://web.archive.org/web/20130218134602/http://www.ncix.gov/publications/reports/fecie_all/index.php.

[32] See Government of Canada. Canadian Centre for Cyber Security, "Cyber Threat Activity Related to the Russian Invasion of Ukraine", 2022, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine; Center for Strategic and International Studies, "Cyber Operations during the Russo-Ukrainian War", Washington DC, 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war;
European Parliament Research Service. "The Role of Cyber in the Russian War Against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict". Brussels, European Parliament, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf;
Trustwave SpiderLabs, "The Russia-Ukraine Cyber War Part 3: Attacks on Telecom and Critical Infrastructure", 2025, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-russia-ukraine-cyber-war-part-3-attacks-on-telecom-and-critical-infrastructure/.

[33] "Cyber Operations during the Russo-Ukrainian War".

[34] Allison Pytlak, "False Alarms: Reflecting on the Role of Cyber Operations in the Russia-Ukraine War", Stimson Center, 2024, https://www.stimson.org/2024/false-alarms-role-of-cyber-operations-in-the-russia-ukraine-war/.

[35] UNDP, "Assessment of the Impact of War on Micro, Small, and Medium Enterprises in Ukraine", 2024, https://www.undp.org/sites/g/files/zskgke326/files/2024-02/UNDP-UA-assessment-war-impact-enterprises-ukraine-summary.pdf.

[36] Greg Austin, "Civil Defence Gaps under Cyber Blitzkrieg", UNSW Canberra Cyber, 2019, https://www.socialcyber.co/_files/ugd/15144d_70b23e97258f490cabbedb99326024db.pdf.

[37] See Greg Austin and Munish Sharma, "From Cyber Resilience to Civil Defence: Contested Concepts: Elusive Goals ", in Greg Austin (ed), *National Cyber Emergencies: The Return to Civil Defence*, Routledge, 2020, 10-30, p. 21.

We can only encourage the Australian Government to address its vision of a "nationally catastrophic" cyber incident in the civil sector. Most observers would see such a contingency as more serious than the effects on the civil sector of cyber operations in the Russian war against Ukraine. There are only two countries likely to have the capabilities and intent to deliver such an outcome on any other within the next decade: China or the United States. In the case of China, its offensive cyber capabilities are maturing rapidly.
Australia needs a new paradigm of cyber response that can help the country to pivot from cyber incident response to preparedness for a national cyber catastrophe. That would mean placing cyber civil preparedness alongside military defence and diplomacy at the top of Australia's national security policy, with appropriate legislated authorities for the operational command of the response. A central component of cyber civil preparedness would be a national cyber resilience strategy to prepare for national cyber emergencies. For the purposes of this paper, we distinguish between cyber civil preparedness and cyber military preparedness as set out in Table 2.

The essence of preparedness is planning and the plans need to be written down and developed through wide consultation. Neither NEMA nor NOCS is structured or funded for the challenge of coordination (as in the pandemic example) for a nationally catastrophic cyber crisis.

Table 2: Relationship between civil and military preparedness

Military preparedness	Civil-military preparedness	Civil preparedness
Led by defence minister, guided by national security committee of Cabinet	Coordinated by defence minister and national security committee of Cabinet	Led by a single minister guided by national security committee of Cabinet
Defence Act 1903	Defence Act 1903	National Emergency Declaration Act 2020
Military activities - War fighting, strategic and tactical intelligence, defence diplomacy	Combined civil and military activities - Defence industry, related R&D, procurement, alliance and partner defence supply, logistics, related intelligence work, related diplomacy	Exclusively civilian activities - Pre-crisis planning, national emergency response, food supply, telecommunications, other essential services, public health, law and order related diplomacy
Executed/led by CDF and service chiefs	Executed by military and civil organisations working together	Led exclusively by civilian actors

2.3 Cyber civil preparedness and resilience

Cyber preparedness and resilience in the civil sector have many goals in common and are intrinsically linked; however, they are different things.[38] Preparedness is about getting ready for a crisis, while resilience is the capability to mitigate a crisis and recover. Preparedness involves taking steps before the event to foresee, plan for, and organise a possible responses to hypothetical emergencies, disasters, or crises. It means being equipped with the right resources, knowledge, and skills in advance of a crisis to lessen the effects of potential threats. In contrast, resilience is how these pre-existing tools can be applied to the ability to recover and adapt after facing hardship or disruption in an actual crisis. Rather than preventing difficulties, resilience is about maintaining strength and flexibility during a crisis or emergency, enabling individuals or organisations to endure and grow despite challenges.

Preparedness helps build confidence, reduce fear, and increase self-sufficiency, all of which are critical components of resilience. Preparedness lays the groundwork for resilience, and resilience encourages proactive, flexible preparedness planning. Both are most effective when communities are actively involved. Community participation ensures that local

[38] "What is the relationship between preparedness and resilience", Survival Times, 26 February 2024, https://survivaltimes.net/what-is-the-relationship-between-preparedness-and-resilience/.

needs and strengths are reflected in planning, making efforts more sustainable and fostering a sense of ownership and strong social bonds—key ingredients for national resilience.

Cyber preparedness is mostly scenario-driven and aims at increasing readiness to cope with hypothetical crisis situations by defining response procedures, acquiring equipment, and defining training programs, among other activities. Resilience follows a more analytic approach to evaluate and improve the capacity to recover during and after an actual crisis. Resilience is not about avoiding or preventing difficulties but rather, exploiting strengths and remaining flexible amid crisis.

The AUSCYBERPLAN of 2025 appears to take a narrow view that that seems to situate cyber security at the centre of the concept and the government at the centre of preparedness. It mentions six sets of activities of which none pay any significant attention to non-cyber impacts of a catastrophic cyber emergency.[39] They are:

1. "ensuring the NOCS is well-equipped with an appropriate workforce and capabilities to support impacted entities by coordinating whole-of-government incident response efforts, including maintaining a crisis communications capability.
2. uplifting the national cyber security posture across critical infrastructure sectors and government.
3. developing and maintaining operational processes and playbooks for incident response across critical infrastructure and other key Australian sectors.
4. developing public communications to improve the cyber security awareness of the Australian public and provide guidance of what individuals or impacted entities should do to respond to cyber incidents and how the Australian Government may support them.
5. leading a National Cyber Exercise Program to exercise cyber crisis arrangements to ensure they are understood, integrated and rehearsed across government and industry
6. coordinating the delivery of the commitments and initiatives under the 2023-2030 Australian Cyber Security Strategy."

There is a strong contrast between the rather limited vision of preparedness in AUSCYBERPLAN and the concept of national preparedness laid out by the US Federal Emergency Management Administration:

> "Preparedness is the shared responsibility of our entire nation. The whole community contributes, beginning with individuals and communities, the private and nonprofit sectors, faith-based organisations, and all governments (local, regional/metropolitan, state, tribal, territorial, insular area, and Federal)".[40]

Japan too has more deeply entrenched approaches to community consultation on a national emergency than Australia has so far elaborated.

Drawing on Australia's experience of the Covid-19 pandemic, an effective national cyber preparedness plan would likely be organised around topics such as the following, where the cyber dimension is less important than a broad national sweep:

- multi-agency and multi-sector collaboration
- centralised contingency planning
- transparent public communication
- flexibility in mobilising resources
- combating misinformation
- reducing public anxiety and maintaining trust
- ensuring actionable guidance is widely disseminated.[41]

2.4 Distinguishing cyber security and resilience

There is a key difference between cyber security and cyber resilience, while noting that both are most effective when drive policy simultaneously. Cyber security applies technology, processes, and measures

[39] "Australian Cyber Response Plan (AUSCYBERPLAN)", p. 20.
[40] Department of Homeland Security, "National Preparedness Goal", 2015, p. 1, https://www.fema.gov/sites/default/files/documents/fema_gpd_national-preparedness-goal-2nd-edition_051525.pdf.
[41] See G. Mott, J.R.C. Nurse, and C. Baker-Beall, "Preparing for future Cyber Crises: Lessons from governance of the coronavirus pandemic", *Policy Design and Practice*, 6(2), 2023, 160-181, https://www.tandfonline.com/doi/abs/10.1080/25741292.2023.2205764; and A.M. Reinhold, R,J. Gore,B. Ezell, B., C.I. Izurieta, E.A. Shanahan, **"**From Cyclones to Cybersecurity: A Call for Convergence in Risk and Crisis Communications Research", *Journal of Homeland Security and Emergency Management*, 22(2), 2025, 119–138, https://pmc.ncbi.nlm.nih.gov/articles/PMC12124907/4567.

designed to protect systems such as servers, endpoints, networks and data from cyber-attacks. Cyber resilience focuses on controls to detect and respond to issues and events in the digital ecosystem, which helps to assess gaps and strengthen overall security posture. These controls enhance the various cyber security measures when leveraged together. Cyber security is a small component of cyber resilience but the two are far from the same set of activities.[42]

There is a key difference between a cyber incident and a national cyber catastrophe. In the latter, the initial cause (often a single cyber incident) becomes far less significant for policy because of the cascading effects it can cause and that rise to the level of extreme national emergency. Civil preparedness and resilience are mutually reinforcing policy goals that must dominate planning for, or responses in, a national cyber emergency but are not identical.
The Australian Government has a very basic definition of cyber resilience, which is centred on the digital systems of enterprises rather than the potential for cascading non-cyber impacts on the society as a whole or the economy:

> The ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage, and recover from, cyber security incidents.[43]

This definition is also included in guidance from the Australian Cyber Security Centre (2025).[44]

In contrast, we take the view that the upper end of response plans must be framed not in terms of a cyber incident but based on a more wide-ranging concept: national civil preparedness for an extreme or catastrophic cyber emergency.

A cyber preparedness posture will drive the pre-attack phase of policy (using risk management through the "detect, identify and protect" functions) and the post-attack phase (using consequence management through the "respond" and "recover" functions). We might add functions of "refinement" (improving through individual incidents or campaigns) and "transformation" (learning after the incident or campaign by doing things quite differently).

The need for new approaches to cyber civil preparedness, including resilience planning, comes from the realisation that the traditional focus on cyber security measures at the enterprise level are no longer enough to protect a country or its individual systems, data, and networks, from compromise.

2.4.1 Relation to the 2023 Cyber Security Strategy

In November 2023, the Australian Government released the *2023-2030 Australian Cyber Security Strategy*, which moved the frame of reference from a predominantly technical and enterprise-based one to a whole-of-nation one.[45] Through its six cyber shields, the Strategy placed the focus firmly on cyber resilience. The six cyber shields are: strong businesses and citizens; safe technology; world-class threat sharing and blocking; protected critical infrastructure; sovereign capabilities; and resilient region and global leadership.

Earlier in 2023, at the opening round of public consultations on the new strategy, the government announced the creation of the National Office of Cyber Security (NOCS).[46] The latest public information on its size and capabilities, dating from 2023, revealed a staff of five, with the ability to draw on an additional 50 staff from the Department of Home Affairs.

According to AUSCYBERPLAN 2025, the whole-of-society responses are led by the NOCS created in 2023, which supports the Cyber Security Coordinator in addressing cyber incidents of national significance. NOCS is the "central touchpoint" for organisations affected by such incidents.[47] The office has

---

[42] Alexander Kott, George (Yegor) Dubinsky, Andrii Paziuk, Stephanie E, Galaitsi, Benjamin D. Trump, Igor Linkov, "Russian Cyber Onslaught was Blunted by Ukrainian Cyber Resilience, not Merely Security", https://arxiv.org/abs/2408.14667. Roles of these authors are notable in terms fo credibility of their analysis: Alexander Kott, (Independent Consultant); George (Yegor) Dubynskyi, (Ministry of Digital Transformation of Ukraine and G.E. Pukhov Institute for Modelling in Energy Engineering); and Stephanie E. Galaitsi, Benjamin D. Trump, and Igor Linkov (U.S. Army Corps of Engineers).
[43] Australian Signals Directorate, 'Cyber resilience', undated, https://www.cyber.gov.au/glossary/cyber-resilience.
[44] Australian Signals Directorate and the Australian Cyber Security Centre, "Information Security Manual, Guidelines for Cyber Security Incidents, 2025, p. 1, https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cybersecurity-incidents.
[45] "2023-2030 Australian Cyber Security Strategy".
[46] Denham Sadler, "Govt to appoint cyber leader to run new office", Information Age, 28 February 2023, https://ia.acs.org.au/article/2023/govt-to-appoint-cyber-leader-to-run-new-office.html.
[47] Australian Government. Department of Home Affairs, "National Office of Cyber Security", 19 December 2024,

responsibilities for consequence management for "the second and subsequent order effects from cyber security incidents". It supports collaborative efforts by government and industry to "identify and mitigate the secondary harms that may result from a cyber security incident". It says that in the most severe instances, "this could include 'real world' impacts".

Policy focus areas for the NOCS outlined in the National Response Plan include its own workforce development and capabilities to support "whole-of-government incident response efforts, including maintaining a crisis communications capability". Most notably, the NOCS takes on "developing public communications to improve the cyber security awareness of the Australian public" and provision of guidance on "what individuals or impacted entities should do to respond to cyber incidents". It also has responsibility for a National Cyber Exercise Program to lay the groundwork for cyber crisis response. This activity is intended to ensure stakeholder familiarity with crisis response plans and their integration across government and industry through regular rehearsals.

The Home Affairs Annual Report 2023-24 reported that the National Cyber Security Coordinator and the NOCS, together with the department, "supported whole-of-society responses to a number of major cyber incidents".[48] It claimed that the department "has hardened Australia's cyber security environment, reduced impacts on businesses, community and industries and is well on its way to making Australia one of the most cyber secure nations by 2030." On the other hand, the annual report noted that it had not met 15 of the 40 benchmarks for implementation of the new cyber security strategy.[49]

National cyber resilience must start with the government and its agencies. The Australian Signals Directorate released its regular annual report to the Parliament in November 2024, titled 'The Commonwealth Cyber Security Posture in 2024', which found that just 15 per cent of entities met a minimum level of overall maturity; more than two-thirds failed on individual protections like multifactor authentication and privileged access; and 71 per cent indicated the use of legacy technologies had impacted their ability to implement the Essential Eight protections mandated by the Australian Signals Directorate.[50]

Through 2023, the Australian National Audit Office undertook a review of the national emergency management framework in the Department of Prime Minister and Cabinet and the National Emergency Management Agency.[51] The audit report, completed in 2024, identified key gaps, especially lack of in-depth planning and adequate community consultation. It recommended more reliance on documented, consistent processes for annual updates; stronger guidance for updating and managing crisis plans, clear criteria for plan publication, and improved documentation for annual exercise program priorities and reviews.[52] NEMA should probably focus on some these critiques in planning for an extreme cyber emergency.

At the same time, the government and its agencies can continue to invest in key strategies for strengthening cyber security and resilience, including:

- adopt zero-trust architecture
- implement multi-factor authentication
- develop incident response plans
- prioritise effective data management
- reduce sensitive data storage
- invest in threat intelligence
- provide cybersecurity training
- establish a security baseline
- enhance continuous monitoring.

As mentioned earlier, cyber resilience at a whole-of-society level hinges on the cyber resilience of key organisations. The digital landscape has fundamentally changed how governments and organisations operate, bringing new risks and challenges that call for a proactive and strategic approach to protecting the value delivered by digital assets, which include data, intellectual property, customer and stakeholder information, and technological capabilities.

---

https://www.directory.gov.au/portfolios/home-affairs/national-office-cyber-security.

[48] Australian Government. Department of Home Affairs, "Annual Report 2023-24", p. 14, https://www.homeaffairs.gov.au/reports-and-pubs/Annualreports/home-affairs-annual-report-2023-24.pdf.

[49] Ibid. p. 83.

[50] Australian Signals Directorate, "The Commonwealth Cyber Security Posture in 2024", 5 December 2024, https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/commonwealth-cyber-security-posture-2024.

[51] Australian National Audit Office "Australian Government Crisis Management Framework", 2024, https://www.anao.gov.au/sites/default/files/2024-10/Auditor-General_Report_2024-25_5.pdf.

[52] Ibid. p. 11.

Protecting the value delivered by digital assets is a strategic imperative, whose key focus must be cyber resilience, which demands cross-sectoral and cross-functional collaboration; stakeholder-specific cyber-resilience contexts; and the ability to operate through and recover from a major disruption. Cyber resilience must be integrated into an organisation's continuity planning and be aligned with that organisation's objectives.

A pro-active approach to cyber security in combatting the rising threat landscape, and to cyber resilience in dealing with the inevitable disruptions is needed, which means not only responding to immediate threats and vulnerabilities but also adopting a long-term strategy that prioritises resilience, continuous monitoring, and adaptability.

2.5 Cyber risk management and resilience

There is also an important difference between cyber risk management and resilience. The former is a process for identifying and assessing the most significant threats, developing defensive strategies, and allocating resources accordingly. Cyber resilience is about trying to minimise the impact from any incident or campaign, whether foreseen or not.[53] Traditional operational resilience is largely about disaster recovery and business continuity planning, whereas cyber risk management focuses most on establishing security infrastructure in place, ensuring the most important assets are protected against the most common threats.

A broad view of what constitutes cyber risk is fundamental to effective cyber resilience. Thus, it is important to see cyber risk as any risk that arises from the use of information services and digital technology or from their use by others in the supply chain or within the wider business environment. In this context, the authors offer these examples of risk:[54]

- Impacts that might arise from cyber events in an organisation's wider supply chain (such as disruption to a critical service on which the organisation depends – this need not be a digital service).
- Impacts other than operational business interruptions; for example, legal and financial liabilities arising from data breach or loss of integrity in data for which the organisation is accountable.
- Risks related to the manipulation of the cyber domain; for example, promotion of disinformation about an organisation or misuse of an organisation's online platforms to commit financial fraud or incite crime.
- Strategic and reputational risks associated with a failure to demonstrate a duty of care to customers, employees or other stakeholders.
- Risks relating to operational technology (OT) as well as to information technology (IT).
- Risks relating to human life (safety- and security-critical systems).

Cyber threat intelligence needs to be as focussed on the provision of information that is relevant to remediation and resilience as it is on potential sources of attack. Remediation-based, orchestrated, automated and customised threat intelligence must be the goal. Raw data is not intelligence.

A missing link in Australian policy planning is the operational chasm between cyber resilience at the enterprise level and country-wide resilience in the face of a national cyber emergency. This gap is also evident in the cyber civil preparedness posture of the country. Evidence for the existence of these gaps can be found in the 2024 Auditor General's report mentioned above

Cyber risk is a systemic risk, and needs to be treated as such, which means that effectively addressing cyber resilience starts at the system-of-systems level, not the corporation or agency level. On the other hand, in order to address cyber resilience and cyber preparedness at a whole-of-society level, the government needs to know how this might be affected by choices in risk management at the enterprise level. In that sense, just as government agencies needs to shore up their own cyber preparedness and resilience posture, so must the government work with all non-government enterprises to document and understand their risk management choices.

2.6 Governance principles for national cyber civil preparedness and resilience

Implementation of a civil preparedness strategy and its twin, a resilience strategy, must start with leadership

[53] See Olivia Powell, "What is the difference between cyber risk management and cyber resilience?", *Cyber Security Hub*, 7 February 2023, https://www.cshub.com/threat-defense/interviews/what-is-the-difference-between-cyber-risk-management-and-cyber-resilience.

[54] Ibid.

and culture (in other words, governance). The Australian Institute of Company Directors (AICD) and the Cyber Security Cooperative Research Centre (CSCRC) released their Cyber Security Governance Principles Version 2 in late November 2024, which sets out five principles, which are aimed at an "organisational cyber crisis" which could be adopted at a whole-of-society level in a preparedness strategy:[55]

- set clear roles and responsibilities
- develop, implement and evolve a comprehensive cyber strategy
- embed cyber security in existing risk management practices
- promote a culture of cyber resilience
- plan for a significant cyber security incident.

With respect to the fourth principle - cyber resilience - the following is offered, which if adopted by Government and its agencies would improve cyber resilience:

- Cyber resilience starts with culture, which begins at the top and must flow through the organisation.
- Regular, engaging and relevant training is a key tool to promote a cyber resilient culture.
- Strong cyber security practices must be incentivised and promoted.

This means that all personnel must undertake cyber security education; cyber security and resilience must be reflected in role statements and key performance indicators; the importance of cyber resilience must be communicated continuously; and there cannot be any exceptions or workarounds for anyone with respect to cyber hygiene and resilience.

2.7 Budget allocations for preparedness and resilience

The federal budget documents for 2024-25 include several statements referencing preparedness and resilience. According to the 2024-25 document, the Minister for Emergency Management and the head of the National Emergency Management Agency (NEMA) are to "develop, lead and coordinate the Commonwealth's approach to emergency management, including the support of activities relating to preparedness, response, relief, recovery, reconstruction, risk reduction and resilience for all-hazard emergencies and disasters".[56]

The same document commits the department to "Enhancing preparedness for, and responding to, cascading events that are likely to have direct impacts on national security and resilience".[57] There are several references to resilience commitments: "help businesses and citizens bounce back quickly following a cyber attack"; "Strengthening national and democratic resilience, including through national strategies and broad-ranging stakeholder engagement*";* and "building Australia's national resilience allowing Australia to anticipate, prepare, absorb, adapt and evolve from both human-induced and natural crises". There are however few details of specific resilience programs and the generic references including resilience show modest investment. We cannot verify three media claims about the 2025–26 budget: an allocation of more than $586 million "to uplift national cyber resilience"; [58] an allocation of $14.5 million to develop a legislated cyber incident reporting framework, likely landing in 2026"; or a new $120 million allocation to "strengthen Australia's cyber response capabilities and address emerging threats. This investment supports national cyber incident coordination, public-private collaboration, and critical infrastructure resilience."

2.8 A Question of Trust

In a consultation paper released in November 2024 titled *Guiding Principles to Embed a Zero Trust Culture*, the Department of Home Affairs laid out guiding principles for the uplift of current policies.[59] These guiding principles are:

[55] Australian Institute of Company Directors, "Cyber Security Governance Principles", Version 2, 25 November 2024, https://www.aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html.
[56] "Department of Home Affairs Portfolio Budget Statements 2024–25", p. 4, https://www.homeaffairs.gov.au/reports-and-pubs/Budgets/2024-25-home-affairs-pbs-full-version.pdf.
[57] Australian Government. "Department of Home Affairs Portfolio Budget Statements 2024–25", 14 May 2024, pp. 11-12, https://www.homeaffairs.gov.au/reports-and-pubs/Budgets/2024-25-home-affairs-pbs-full-version.pdf.
[58] Catherine Chipeta, "2025–26 Federal Budget: What Australia's Finance Leaders Need to Know", 2 June 2025, eftsure Blog, https://www.eftsure.com/en-au/blog/industry-news/2025-26-federal-budget-what-australias-finance-leaders-need-to-know/.
[59] Australian Government. Department of Home Affairs, "Guiding Principles to Embed Zero Trust Culture: Consultation Paper", November 2024, https://www.homeaffairs.gov.au/cyber-security-subsite/files/consultation-paper-guiding-principles-to-embed-zero-trust-culture.pdf.

- identify and manage cyber security risk at an enterprise level
- understand accountabilities and responsibilities at all levels
- know and understand your most critical and sensitive technology assets
- maintain resiliency through a comprehensive cyber strategy and uplift plans
- go beyond incident planning.

In discussing the fourth principle, the guidance identifies cyber resilience as 'The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment'.

Furthermore, the guidance discusses the cyber resilience continuum in terms of understanding that cyber security resilience is a continuous cycle that organisations are required to consider as a part of their broader business operations. It emphasises a proactive, adaptive approach, spanning readiness (an element of preparedness) and response efforts to ensure systems can continue operating in an evolving cyber risk landscape.

The guidance also identifies cyber fluency as the next step beyond cyber awareness – the ability to understand and apply knowledge of cyber-security concepts, risks, and best practices across digital environments. It recognises that traditional cyber awareness is not enough to provide protection against the sophisticated threats of the modern age. Achieving cyber fluency requires an organisation's workforce to be sufficiently trained in cyber security practices to the extent that cyber security is automatically applied in their everyday work context. Cyber fluent individuals apply their knowledge to safeguard systems and data, propagating a culture of cyber security within organisations and communities.

3. Complementary Research and Analysis

The Institute for Integrated Economic Research – Australia (IIER-A) conducted two workshops in 2020 on data access and emerging technologies to further support Australia's progress towards a national resilient posture and as part of a broader national resilience study. The major observations from the resulting study by IIER-A are published for the first time below.

- While Australia has addressed the pressing need to uplift its cyber security through a number of Government initiatives at federal and state levels, the economic impacts and unintended consequences of the raft of government initiatives, which are interdependent, are not well understood, and more sophisticated modelling is required.

- The advancement of digital technologies continues to outpace the corresponding policy, legislative and regulatory changes, notwithstanding considerable effort within Government, the Department of Home Affairs and other agencies. More focussed effort is needed to ensure well-coordinated resilience planning by governments, companies, communities and individuals as additional disruption is created through such rapid technological advancement.

- It is important for Australia to ensure that the jewel in its technology crown – data – can be accessed and protected. Data is a strategic asset and must be treated as a sovereign responsibility. To date, the need for cyber resilience has tended to focus on information systems, but it must also encompass data.

- Emerging technologies may be able to facilitate a greater degree of national information resilience if they are properly identified, procured and deployed. Australia needs to determine just what degree of sovereign capability it needs in these emerging technologies; and it needs to monitor its related supply chains to ensure adequate transparency and to have the ability to verify these supply chains where and when needed.

The authors of this paper, working with a group of international and Australian specialists, contributed a set of ideas toward that goal in a study published in 2020, examining a set of ideas around cyber civil defence and enhanced resilience policy, both for Australia and internationally.[60] In spite of significant

[60] See Gary Waters, "National Cyber Emergency Policy in Australia: Critical Infrastructure", in Greg Austin (ed), *National Cyber Emergencies: The Return to Civil Defence*, Routledge, 2020, 93-107; and Greg Austin, "US Policy: From Cyber Incidents to National Emergencies", in Austin (ed) *National Cyber Emergencies*, 31-59.

advances in policy and preparedness for national cyber emergencies, the progressions since 2020 have been gradual.

A good example is the health sector, where the Australian government decided to fund a fundamental component of cyber resilience (an Information Sharing and Assessment Centre – ISAC) in 2024 that launched in 2025, compared with the United States where the private sector set up its health ISAC in 2010.[61] The US began setting up such sector-based ISACs in 1998. The need for these organisations was demonstrated in July 2024 when the Health ISAC in the US observed that 'Three third-party supply chain attacks [had] significantly impacted healthcare delivery' in the previous three months in the USA.[62]

Australia's national cyber ecosystem encompasses inter alia: energy, other critical infrastructure, economy and commerce, industry, health, education, agriculture, defence, climate change mitigation, public sector, community preparedness, and national research. The national system is in fact deeply integrated with global cyber ecosystems. Australia must, therefore, plan to be cyber resilient in the face of major disruptions at both the national and global level.

In 2024, the case for Australia to adapt and transform its approach to national resilience in general in the face of emergencies in any sector (such as natural disasters or pandemics) on the basis of international comparisons was well made by Marc Ablong, a former senior official of the Department of Home Affairs.[63] He points out that national resilience "provides a means to deliver a more systemic approach to preparing for and managing a future in which we face more frequent, severe, complex, cascading and compounding crises. It is the ability to plan for, adapt to, prepare for, resist, respond to and recover from change and crisis, whether natural or man-made, singly or concurrently. A national resilience approach to crises helps to frame an understanding of the interconnected and interdependent nature of the systems that a country relies upon to function and provides a structure for making decisions during times of concurrent and cascading crises".

Among his recommendations, Ablong argues the need to institutionalise national resilience through a national resilience strategy, a national risk assessment, a national preparedness audit, and a national preparedness plan.

Thus, this paper's analysis of upgrading Australian cyber resilience is set against a policy background where the country as a whole is falling short in its ability to understand national risk and subsequently be more resilient to future challenges. The lack of a coherent risk assessment and resilience strategy in Australia, notwithstanding various efforts across the various jurisdictional layers, cries out for a national integrated approach. Research and activity by the Institute for Integrated Economic Research – Australia (IIER-A) supports this general proposition, and it is conducting a national risk and resilience study to help establish the national settings across all sectors. It aims to determine an approach for a National Risk Assessment with an emphasis on futures thinking addressing uncertainty; and to determine potential pathways for delivery and implementation of a National Resilience Strategy.

4. National cyber civil preparedness and resilience strategies

Cyber civil preparedness is a national security issue of first order importance alongside preparation of a country's armed forces. It deserves equal standing in the machinery of government that in the Australian case is far from evident. While a national cyber resilience strategy is needed urgently, and the discussion in this section outlines what that could look like, it is also vital for Australia to address the cyber civil preparedness side.

Tom Guarente argues that cyber security threat response is as much an emergency response and

[61] Note that a not-for-profit Critical Infrastructure (CI) ISAC was set up as a private sector initiative in February 2023, which operates across all critical infrastructure sectors. The Australian Health ISAC is managed by the CI-ISAC under a federal grant.

[62] American Hospital Association and Health ISAC, "Hospital Association and Health-ISAC Joint Threat Bulletin - TLP White", 1 August 2024, https://www.aha.org/advisory/2024-08-01-american-hospital-association-and-health-isac-joint-threat-bulletin-tlp-white.

[63] ASPI, 'National Resilience: Lessons for Australian Policy from International Experience', 2024, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2024-02/National%20resilience.pdf?VersionId=i7v1J.m1quta2TKhuQMpzyTKqmMz9eMW.

preparedness mission in a similar vein to natural disasters and physical attacks – not merely an IT resilience discussion. The technology element can certainly address how to recover from an incident, how to identify and mitigate attacks, how to prevent exfiltration, and so on. However, the kinetic effects of some cyber-attacks can result in the same dangers as any natural disaster, where people's lives are at a minimum disrupted but also potentially at risk. An attack on the electrical grid, for example, could leave thousands or even millions of citizens without power and normal essential services (food, health, water). During a heat wave or freeze, vulnerable people could be in real physical danger, and civil unrest could potentially follow.[64]

4.1 Managing Catastrophic Cyber Incidents

Australia needs to be better prepared for catastrophic cyber incidents. While cyber resilience in enterprises is important , it addresses post-incident actions, focussed on recovery. That is not sufficient; pre-incident preparation in the economy and society must also be addressed, which is where preparedness has a role to play.

Preparedness involves readiness (the ability to respond in timely and effective fashion) and sustainability (the ability to maintain that timely and effective response for as long as needed). The recent challenges on the Iberian peninsula brought into focus the need to be better prepared, not simply resilient, for disruptions in national critical infrastructure which are inevitably underpinned by cyber technologies.

Furthermore, while civil sector resilience might be sufficient in peacetime, it may not suffice in wartime. Preparedness is needed. As mentioned earlier, the Chief of the Defence Force mentioned recently that Australia needs to plan to operate warlike operations from home soil. This not only underscores the need to re-focus military preparedness, but cyber civil preparedness as well, and relate this to national resilience.

A November 2024 White Paper by the University of Oxford and the World Economic Forum, argues that "proactive collaboration and continuous learning will play a vital role in delivering cyber resilience". They define cyber resilience in terms of the ability to minimise the impact of significant cyber incidents on primary goals and objectives. Cyber resilience allows an organisation to maintain critical services, safeguard stakeholder confidence and protect strategic value, which goes beyond restoring business-as-usual operations to encompass everything that is required to sustain the organisation. This means that prioritising cyber resilience is a core strategic issue, not just as an IT issue.[65] While the WEF study focussed on organisations, the observations apply at a whole-of-nation level, indicating that more needs to be done by the government to ensure that preparedness and cyber resilience are built into the nation and the culture of its organisations.

This means:

- Anticipating and planning for cyber and sustained campaigns, based on an understanding of the threats and the potential non-cyber harms that could arise.
- Designing processes and establishing contingent capabilities to absorb and recover from incidents and extreme emergencies.
- Adopting information governance practices that can limit the impact arising from confidentiality breaches, data integrity compromises, and more devastating cyber-attacks.
- Learning from incidents and adapting to strengthen the resilience posture.

In short, cyber resilience demands the right mindset centred around supporting primary goals and objectives, with decision-making on cyber resilience embedded within the established governance structures, cyber-resilience built into business processes and information governance practices upfront, established plans for dealing with incidents – all grounded in strong cyber-security practices. However, responding to a cyber threat is as much an emergency response and preparedness mission as responding to natural disasters and physical attacks. This means that cyber security and cyber resilience must be viewed as a whole-of-society issue – fundamental to national preparedness.

Australia needs to adapt to an evolving global, regional, and domestic environment, to respond to short-term

[64] Tom Guarente, "Cybersecurity response: Not just an IT issue but an emergency preparedness priority", *Nextgov/FCW*, 26 December 2024, https://www.nextgov.com/ideas/2024/12/cybersecurity-response-not-just-it-issue-emergency-preparedness-priority/401572/.

[65] World Economic Forum, "Unpacking Cyber Resilience" White Paper, in collaboration with the University of Oxford, November 2024, https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf.

shocks (whether natural or man-made), and to prepare to respond to long-term challenges. The evolving environment, short-term shocks, and long-term challenges all have a cyber component. Hence, a national cyber resilience strategy that supports a national preparedness strategy is needed to:

- Support all elements of Australia's economy and society to effectively manage risks to the continuity of their operations through mature risk based and resilience approaches.
- Deliver initiatives through strong industry–government partnerships.
- Support all elements of Australia's economy and society to strengthen their security and resilience through resilience frameworks, tools and improved collaboration.

Such a National Cyber Resilience Strategy could set out a vision, along the lines of: To uplift the security and resilience of Australia's cyber realm in the face of increasing threats and vulnerabilities, and advance our national security, economy, and social prosperity. This will be achieved by strengthening Australia's cyber-resilient posture through an enhanced regulatory framework and strong collaboration across the entire cyber ecosystem.

The strategy also needs to address constant change in terms of:

- A wider range of hazards, including physical and natural (with scale, frequency and intensity all potentially increasing), supply chain, personnel, and cyber and information security.
- Technological advances and increased connectivity, which while creating economic efficiencies, also increase the likelihood and impact of disruptions.
- An increasingly volatile geopolitical environment, and susceptibility of the nation, its systems and people to attack by nation states, state-sponsored actors, issue motivated groups, or extremist groups, seeking to advance their own interests.

While a national cyber catastrophe may be unlikely, the Australian Government does not have a published plan for managing the non-cyber impacts. Its approach to cyber disaster management has been centred on government and industry, not on the broader economy and society.

One of the fundamental questions is whether Australian citizens or businesses, foreign citizens and businesses based in Australia follow the directions of the Prime Minister in emergency measures to contain and mitigate a nationally catastrophic cyber incident. The National Emergency Declaration Act 2020 gives no special authority for the Commonwealth to compel states, business or citizens to follow its directives and the threshold for declaring a national emergency are sufficiently low that they might not provide the necessary moral authority.[66]

4.2 Cyber Resilience Framework

A cyber resilience framework is also needed to accompany a National Cyber Resilience Strategy that allows a catastrophic national disruption to be managed more effectively. Such a framework should be built on the recognition that the interconnectedness and deep interdependence that has resulted from globalisation and connectivity means that predictions can no longer be made with great degrees of precision and that actions and reactions and their cascading effects happen much faster than before. Thus, prediction is not sufficient to confront threats and deal with challenges, and risk management is insufficient to deal with the disruption that is inevitable. Developing resilience and learning how to reconfigure to confront the unknown is a much more effective way to respond to a complex and uncertain environment.
The Tech Policy Design Centre released its *Australian Telecommunications Sector Resilience Profile: Keeping Australia connected in an uncertain world* in October 2024 that provides a useful way of managing the inevitable disruptions through a resilience framework and offers five maturity levels that have been broadened to address cyber resilience.[67] The key observation from this study is that risk is a component of resilience, not the other way around. Australia needs

[66] Law Council of Australia, "Review of the National Emergency Declaration Act 2020", Canberra: Law Council of Australia, 2021, https://lawcouncil.au/publicassets/865e50e8-55a2-eb11-943a-005056be13b5/3982%20-%20National%20Emergency%20Declaration%20Act.pdf; Australian Human Rights Commission, "Greater scrutiny of emergency powers needed", 22 April 2021, https://humanrights.gov.au/about/news/media-releases/greater-scrutiny-emergency-powers-needed.

[67] See Tech Policy Design Centre (TPDC), "Australian Telecommunications Sector Resilience Profile: Keeping Australia connected in an uncertain world", September 2024, https://techpolicy.au/wp-content/uploads/2024/10/ANU-ATSRP-Report_2024-Final.pdf.

to adopt a shared responsibility and shared vision to manage the complexity, uncertainty and interdependencies, bringing clarity to the cacophony. It can only do this by uplifting the nation's cyber resilience. Because disruption is inevitable, Australia needs to address the continuum from risk management through consequence management, through to lessons management. The challenge is how to operationalise this across all critical infrastructure sectors, and across the entire economy and society. Drawing on the *Telecommunications Sector Resilience* study, the authors of this paper suggest that building cyber resilience requires maturing capacities across all phases of disruption management – prepare and absorb (situational awareness of the risk landscape and risk management), adapt, respond, and recover (consequence management) and learn and transform (lessons management).[68]

The Study provides a useful set of definitions of these phases, which are broadened in Table 3 for more general cyber security and critical infrastructure purposes.

Table 3: Resilience Phases Definitions

Risk Management	***Prepare***. Resilience preparedness refers to the ability to mitigate and prepare for disruption. This involves having situational awareness of the risk horizon and then implementing mitigation and planning capabilities to ensure that critical assets and services can withstand, absorb, and recover from disruption. It includes the governance processes to adapt, respond to, learn from, and transform after disruptive events. ***Absorb***. Resilience absorption refers to the ability to cope with disruption. This involves robustness of technical infrastructure and coping strategies that enhance the ability to absorb shocks without significant service degradation or failure.
Consequence Management	***Adapt***. Resilience adaptation refers to the ability to prepare for disruption in advance and make positive adjustments that counter the impacts of disruption. This involves situational awareness of the risk horizon, flexible and responsive operational capabilities, continuous monitoring, and the ability to modify systems and processes in response to emerging threats and changes. ***Respond***. Resilience responsiveness refers to the ability to quickly and effectively respond to disruptions. This involves establishing incident response protocols, real-time communication systems, and coordinated efforts among stakeholders to manage and mitigate the impacts of disruptions. ***Recover***. Resilience recovery refers to the ability to restore services and return to normal operations following a disruption. This involves comprehensive recovery planning, resource allocation, and support systems that enable rapid restoration of critical functions. It also includes strategies to support long-term community recovery, ensuring that services contribute to affected communities' overall resilience and well-being.
Lessons Management	***Learn***. Resilience learning refers to the ability to learn from past disruptions and continuously improve resilience strategies. This involves systematically analysing disruptions, feedback mechanisms, and integrating lessons learned into planning and operations. ***Transform***. Resilience transformation refers to the ability to fundamentally change and improve its systems and processes in response to evolving threats, threat sources, and vulnerabilities. This involves innovation, forward-thinking governance, and the ability to implement strategic changes that enhance overall resilience.

The company *InConsult* offers a useful starting point in developing a cyber resilience framework as it addresses resilience as a continuum through pre-incident and post-incident phases and aligns the framework with overall governance. In this sense, resilience would address the risk management approach prior to an incident (noting that this does not address the preparedness aspects), and the consequence management approach after the incident. Governance would address leadership, accountability (including roles and responsibilities), and continual improvement. The pre-incident phase would involve risk management through the detect, identify and protect functions traditionally associated with cyber security. The post-incident phase would involve consequence management through the respond and recover functions, to which we could add, refine and transform. These are explained below:

- *Detect* involves ongoing, active and continual monitoring of networks and information systems to detect and escalate issues and potential cyber security incidents quickly.

[68] ibid.

- *Identify* involves anticipating and recognising the range of possible cyber risks, their causes and consequences, which means better understanding the environment and cyber risk posture. This involves a formal cyber risk assessment to identify, analyse, evaluate, and prioritise risk arising from the operation and use of information systems and networks.
- *Protect* involves implementing the right controls (policies, procedures, plans, activities) to either prevent or mitigate the impact of a cyber risk, ensuring confidentiality, integrity and availability.
- *Respond* involves timely action to limit the impact of the attack or disruption and to ensure a successful recovery. It also encompasses mandatory reporting of information security breaches for critical infrastructure entities.
- *Recover* involves restoring data and services after a cyber-attack or disruption to the pre-incident state. This necessitates a number of pre-existing and pre-tested recovery sub-plans that are clear and thorough to execute an effective response.
- *Refine and transform* involves ongoing, active and continual monitoring of networks and information systems to detect and escalate issues during the incident, and transforming through lessons learnt after recovery.[69]

As mentioned earlier, the *Australian Telecommunications Sector Resilience Profile* study also provides a useful resilience framework that uses risk management to prepare and absorb (situational awareness of the risk landscape and risk management); consequence management to adapt, respond, recover; and lessons management to learn and transform.

4.3 Cyber Resilience Maturity Levels

The *Australian Telecommunications Sector Resilience Profile* study also establishes five maturity levels that can be broadened to address cyber resilience as follows:

- *Initial*: Resilience practices are unstructured and reactive across the cyber ecosystem.
- *Developing*: Basic resilience measures are established, including initial coordination efforts across the cyber ecosystem.
- *Defined*: Resilience processes are well-defined and documented across the cyber ecosystem.
- *Managed*: Resilience practices are systematically integrated and applied consistently across the cyber ecosystem.
- *Optimised*: Resilience is continuously improved through proactive learning, innovation, and transformation, across the cyber ecosystem.

4.4 Cyber Resiliency Engineering Aid

Another useful contribution to developing a cyber resilience framework is work from MITRE in 2015.[70] Its Cyber Resiliency Engineering Framework (CREF) organises the cyber resiliency domain into a set of goals, objectives, and techniques. Goals are high-level statements of intended outcomes, which help scope the cyber resiliency domain; objectives are more specific statements of intended outcomes that serve as a bridge between techniques and goals; cyber resiliency techniques characterise approaches to achieving one or more cyber resiliency objectives that can be applied to the architecture or design of mission/business functions and the cyber resources that support them. The cyber resiliency techniques are interdependent – they support one another.

Australian public policy settings for cyber resilience are adequately cognisant of appropriate goals and objectives but need considerably more development in respect of techniques as elaborated in the CREF. Some of these are familiar as cyber security techniques (such as deception or restriction of privileges) but need to be elaborated in detail for what they mean when applied to the national resilience ecosystem.

Cyber security and cyber resilience must be viewed as a whole-of-country issue – fundamental to national preparedness. Cyber-security and cyber-resilience planning must look at the operational impact that lies beyond IT assets, and recognise that physical and

[69] InConsult, "Achieving Cyber Resilience: A New Framework", n.d., https://inconsult.com.au/publication/achieving-cyber-resilience/.

[70] See Deborah Bodeau, Richard Graubart, William Heinbockel and Ellen Laderman, "Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques", *MITRE*, May 2015, https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf.

virtual assets like operational technology, internet of things, building management systems and more must be protected from cyber threats in the same way as IT. For example, facilities management organisations with responsibility for internet-connected building access systems and security cameras must be included in cyber response activities. Agencies with medical missions should include in their cyber response activities those organisations responsible for internet-connected devices such as MRI machines and other clinical assets, which may also be vulnerable to cyber-attacks that could result in risks to people's lives in the event of a disruption or shutdown.

Emergency response plans must include all stakeholders, outlining roles and responsibilities for each. Scenario exercises similar to those used in cases of natural disasters must be conducted. As with emergency situations, planning and exercises must be regularly coordinated with external organisations, including the Australian Cyber Security Centre, Australian Security and Intelligence Organisation, and Department of Home Affairs in relation to cyber and emergency management.

In the November 2024 White Paper titled 'Unpacking Cyber Resilience' from the University of Oxford and the World Economic Forum referred to earlier, the authors point out that 'Proactive collaboration and continuous learning will play a vital role in delivering cyber resilience', allowing an organisation to maintain critical services, safeguard stakeholder confidence and protect strategic value, which goes beyond restoring business-as-usual operations to encompass everything that is required to sustain the organisation. This means that prioritising cyber resilience is a core strategic issue.[71]

Managing strategic, operational and business risks now involves a component of cyber risk, which necessitates building cyber resilience into the organisation's culture. This indicates the need to shift the focus from cyber security to cyber resilience and flow that down to all strategic, operational, business and cyber practices. As emerging and disruptive technologies are embraced, cyber resilience will become even more vital as a business enabler.

Cyber-resilient organisations need to be able to:

- Anticipate and plan for incidents, based on an understanding of the threats they are exposed to and the potential harms that could arise.
- Design processes and establish contingent capabilities that will place the organisation in a good position to absorb and recover from events.
- Adopt information governance practices that can limit the impact arising from confidentiality breaches and data integrity compromises.
- Learn from incidents affecting their own organisation and its peers and adapt to strengthen the resilience posture.
- Take a broad view of cyber risk and the many ways in which malign actors could exploit cyberspace to cause harm to their operations, profitability or reputation.

5. Critical Infrastructure Challenges

As mentioned earlier, the *2023-2030 Australian Cyber Security Strategy* outlined its six cyber shields, the fourth of which was Protected Critical Infrastructure.[72]

Australia's critical infrastructure is characterised by interconnectedness and deep interdependence across its ecosystem. CSIRO addressed Infrastructure Resilience in its July 2020 'Climate and Disaster Resilience Technical Report'.[73] It defined resilience as the capacity for critical infrastructure to absorb the impact of events and recover to a normal state, pointing out that resilient infrastructure is greater than an asset's capacity to simply withstand attack. When evaluated through the dimensions of impact on the physical, organisational, economic and social aspects of critical infrastructure, its resilience is only demonstrated where each dimension is resilient in its own right. Cyber is the pervading theme that runs across and throughout all these dimensions.

The National Disaster Risk Reduction Framework (NDRRF) recognises this complexity, supporting all jurisdictions and non-government stakeholders to collectively prepare for the hazard, exposure, vulnerabilities and capacity to survive.[74] Australia's Critical Infrastructure Resilience Strategy extends this framework with an aim to ensure the continued

[71] "Unpacking Cyber Resilience".
[72] "Australian Cyber Security Strategy 2023-2030".
[73] CSIRO, "Climate and Disaster Resilience", 2020.
[74] Australian Government. Department of Home Affairs. (2018). "National Disaster Risk Reduction Framework", 2018, https://www.homeaffairs.gov.au/emergency/files/national-disaster-risk-reduction-framework.pdf.

operation of critical infrastructure in the face of all hazards.[75]

The functions of critical infrastructure depend on each other. Networks which ensure supply of food, water and energy are the outcome of complex interactions btween physical assets, technology, society, environment and finance. Australian infrastructure is multi-jurisdictional, which requires an analysis of resilience to be undertaken in the context of Australia's federated system of government. Furthermore, much of Australia's critical infrastructure is privately owned or operated, including by some powerful foreign corporations, adding the needs and impact of non-government actors into the equation.

There are four separate dimensions to the resilience of critical infrastructure:

- Technical resilience focusing on the physical systems;
- Organisational resilience looking at management and decision making to either avoid or respond to crisis situations;
- Economic resilience covering the ability to face the extra costs that arise from a crisis; and
- Social resilience referring to society's capacity to lessen impact of a crisis.

More effective information sharing, particularly with regard to cross-dimensional information, is pivotal to improving the resilience of critical infrastructure. In the cyber realm, this translates to having an effective national multi-dimensional cyber threat intelligence (CTI) sharing capability and capacity.

Such CTI can drive significant value across threat detection, incident response, vulnerability management, and broader risk management. However, a solid risk management program is needed to set the priorities and requirements for intelligence collection that will allow the relevant information to be gathered that pertains to the most valuable assets. CTI is most valuable when it is used to contextualise security analytics about activity occurring within an organisation's infrastructure, in the economy, or the society at large.

The usefulness of the information and sources can be assessed around several key attributes - completeness, accuracy, relevance, timeliness, and ability to be actioned. The intelligence gathered must be used to inform processes and decisions.

Furthermore, CTI must be collected and operationalised on three major fronts: tactical, operational, and strategic.[76] All are necessary to help prioritise spending based on what's happening in the threat landscape.

5.1 Critical Infrastructure Resilience Strategy

The Critical Infrastructure Resilience Strategy, referred to above, was released in February 2023.[77] Its intent is to uplift the security and resilience of Australia's critical infrastructure in the face of all hazards and advance our national security, economy and social prosperity. This will be achieved by strengthening Australia's critical infrastructure through an enhanced regulatory framework and strong collaboration across the critical infrastructure community.

It provides a framework for how industry, state and territory governments, and the Australian Government will work together to mature the security and resilience of critical infrastructure, and to anticipate, prevent, prepare for, respond to and recover from all-hazards. Its objectives are to:

1. Support critical infrastructure owners and operators to effectively manage risks to the continuity of their operations through mature risk based and resilience approaches.
2. Deliver initiatives through strong industry–government partnerships.
3. Support critical infrastructure owners and operators to strengthen their security and resilience through regulatory frameworks, tools and improved collaboration.

The Strategy also argued that future security and resilience initiatives need to consider how the context of Australia's operating environment will be subject to

[75] Cyber and Infrastructure Security Centre, "Critical Infrastructure Resilience Strategy 2023", 2023, https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf.

[76] See Ericka Chickowski, 'Stop wasting money on ineffective threat intelligence: 5 mistakes to avoid', *CSO*, 15 January 2025, https://www.csoonline.com/article/3624136/stop-wasting-money-on-ineffective-threat-intelligence-5-mistakes-to-avoid.html.

[77] "Critical Infrastructure Resilience Strategy 2023".

constant change. The nation needs to consider the impact of:

- Susceptibility to a wider range of hazards, from physical and natural (including extreme weather events on unprecedented scale, frequency and intensity as a result of climate change), supply chain and personnel, to cyber and information security.
- Technological advances and increased connectivity. More systems and services are being connected to the internet and to each other, creating economic efficiencies but also increasing the likelihood and impact of disruptions.
- An increasingly volatile geopolitical environment, and susceptibility of critical infrastructure to attack by nation states, state-sponsored actors, issue motivated groups, or extremist groups, seeking to advance their own interests.

The Critical Infrastructure Resilience Strategy, dating from 2023, only goes so far. Its view does not reflect the 2025 view of a nationally catastrophic cyber incident.

The Strategy notes that resilience refers to the ability of the nation to adapt to an evolving global, regional, and domestic environment, to respond to short-term shocks (whether natural or man-made), and to prepare to respond to long-term challenges. The evolving environment, short-term shocks, and long-term challenges all have a cyber component.

Hence, a new and comprehensive national cyber resilience strategy is needed to:

1. support all elements of Australia's economy and society to effectively manage cyber risks to the continuity of their operations through mature risk based and resilience cyber approaches.
2. deliver initiatives through strong industry–government cyber partnerships.
3. support all elements of Australia's economy and society to strengthen their cyber security and resilience through resilience frameworks, tools and improved collaboration.

Furthermore, a national cyber resilience strategy needs to be twinned with a national cyber preparedness strategy that would address constant change in terms of:

- A synchronous approach to all hazards, including technical, social, physical and natural (with scale, frequency and intensity all potentially increasing), supply chain, personnel, and cyber and information security.
- Technological advances and increased connectivity, which while creating economic efficiencies, also increase the likelihood and impact of disruptions, especially through the cyber realm.
- An increasingly volatile geopolitical environment, and susceptibility of the country, its systems and people to attack by foreign states, state-sponsored actors, issue motivated groups, or extremist groups, seeking to advance their own interests, especially through the cyber realm.

5.2 CSIRO Critical Infrastructure Protection and Resilience Initiative

CSIRO is pursuing a number of resilience missions, including 'Building the resilience of Australia's critical infrastructure'. The Critical Infrastructure Protection and Resilience (CIPR) initiative seeks to create enhanced national capability to overcome the current fragmented response to Australia's essential services 'centre of vulnerability', which is where the nation's increasingly interdependent critical infrastructure sectors and systems converge with increasingly interconnected natural and human-induced hazards.[78]

CSIRO is working on two core national needs:

- *Critical Infrastructure Protection*: lifting protection of critical infrastructure sectors and the communities they serve, from the direct and flow-on impacts of multi-hazard events; and
- *Critical Infrastructure Resilience*: enhancing the resilience of critical infrastructure assets, systems, networks, supply chains and the community from changing threats.

CIPR focusses on five key areas:

[78] CSIRO, "Critical Infrastructure Protection and Resilience", n.d., https://www.csiro.au/en/about/challenges-missions/Critical-Infrastructure.

- Consensus building – creating a common national approach and language.
- Enabling multi-hazard understanding – understanding interconnections and intersections between climate and human-induced hazards.
- Informing multi-sector interdependencies – understanding interconnections and intersections between interdependent systems.
- Modelling multi-hazard multi-sector impact – understanding multi-hazard, multi-sector impact.
- Mitigating compounding cascading impacts – informing mitigation strategies to minimise cascading and compounding impact on systems.

The intent is for:

- Reduced disruptions to Australia's Critical Services.
- Increased critical infrastructure protection and resilience on a national scale.
- Growth of Australia's Critical Infrastructure service sector jobs and exports.

5.3 National Data Centre Strategy

The Albanese government is seeking to develop a national data centre strategy that emerged from a meeting with industry representatives in late October 2024. The strategy is intended to address the entire digital infrastructure pipeline, including the energy requirements of the sector as the immense compute needs of Artificial Intelligence (AI) workloads drive a substantial increase in demand for the facilities. Speaking at the National Tech Summit in Melbourne on 13 November 2024, Dr Andrew Charlton, then Special Envoy for Cybersecurity and Digital Resilience, stressed the importance of data centres and the networks behind them for Australia's digital future, describing them as a "fundamental building block of the future economy".[79]

There is no question that the increasing demand for data centres is significant. Mandala analysis estimates data centre deployable capacity in Australia is projected to more than double from 1,350 megawatts (MW) in 2024 to 3,100 MW by 2030 as data centres support an increasing number of internet-connected devices and digital services. Additional investment in Australia's data centre capacity is forecast to top $26 billion during this period to meet digital demand. Furthermore, the data centre workforce itself needs to grow by 8,300 to reach 17,900 by 2030.[80]

As the demand for data centres increases, it will place additional demands on energy supply. It is doubtful that renewables alone will provide sufficient additional capacity. As Belinda Dennett argues, Australia's doubling of its data centre capacity in the next five years will demand a concomitant increase in energy supply, whether that be through coal-fired power stations, nuclear (such as from small modular reactors), or renewable energy (wind, solar and pumped hydro) and battery energy storage systems; noting that renewable energy sources would also assist Australia in meeting its national carbon reduction goals.[81]

While major data centre operators have committed to powering their facilities with 100 per cent renewable energy by 2030, largely through power purchase agreements, some studies indicate that total capacity for data centres worldwide is expanding rapidly, with several markets requiring power that exceeds the current capacity of their power grids, leading to development pipelines that are set to more than double capacity levels. Microsoft, Google, and Amazon have all announced plans to use Small Modular Reactors (SMRs) to power data centres. New developments in purchase power agreements are discussed by Matt Pacheco;[82] and further insights into data centre power demand are discussed by Goldman Sachs Research.[83]

---

[79] See Justin Hendry, 'National data centre strategy talks break cover', *InnovationAus,* 14 November 2024, National data centre strategy talks break cover.

[80] Mandala Partners. "*Empowering Australia's Digital Future: Report*", October 2024, https://mandalapartners.com/uploads/Empowering-Australia's-Digital-Future---Report_October-2024.pdf.

[81] InnovationAus. "Powering the nation's data centre opportunity", 18 October 2024, https://www.innovationaus.com/powering-the-nations-data-centre-opportunity/.

[82] See Matt Pacheco, 'Understanding Data Center Capacity Planning & Best Practices', *Tier Point*, 21 May 2024, https://www.tierpoint.com/blog/data-center-capacity-planning/.

[83] Goldman Sachs, "Bullish expectations for US electricity are attracting new power traders", 18 July, 2024, https://www.goldmansachs.com/insights/articles/bullish-electricity-attracting-new-power-traders.

As Belinda Dennett argues further, given the essential nature of data centres and their need for a constant, 24/7 energy supply, policy responses must be carefully crafted otherwise they could damage both economies and societies. Australia must continue to grow its data centre infrastructure without undermining its climate goals and ensuring energy reliability. The transmission network will also need to change, including through increasing grid interconnection across the eastern states and developing grid-scale energy storage projects. Cloud and AI digital services companies and grid companies will need to engage more closely as the transmission network evolves.

The Australian government will need to collaborate at a much higher level across industry, including the data centre operators, the energy industry, and telecommunications companies. Novel solutions will be needed.

6. Recommendations for cyber civil preparedness and resilience

Australia lacks a formal National Security Strategy and subordinate strategies for addressing national preparedness and national resilience in the circumstances of a nationally catastrophic cyber crisis. This paper has articulated the pressing need for a Cyber Civil Preparedness Strategy and its twin, a National Cyber Resilience Strategy. We should differentiate more sharply between cyber security and cyber resilience. We need to take national cyber preparedness and resilience well beyond the scope of the current *Cyber Security Strategy 2023-2030*. We must plan for large-scale disruptions across the whole economy and society. We would benefit from development of frameworks for both cyber civil preparedness and cyber resilience that are much more attentive to and honest about maturity levels. We can do more to harden our critical infrastructure and strengthen our organisational resilience. Above all else, we must position cyber resilience in a whole-of-country posture for civil preparedness.

Civil preparedness is about the relationship between the society and the government in the execution of national security policy and human security policy. The paper suggests that the mechanisms of government for cyber civil preparedness could be most effective if they were part of a broader national effort in civil preparedness cutting across several areas of Australian deterrence and war-fighting capacity. Impacts of a cyber crisis on the population's welfare and lives must be a central, defining focus but these are not currently as high a priority in Australian planning for a national cyber catastrophe as they need to be.

At the strategic policy level, there are five recommendations.

The first recommendation is to produce a national assessment of cyber civil preparedness and resilience that addresses the challenges of volatility, uncertainty, complexity and ambiguity of the international and domestic cyberspace environment, both current and prospective. The assessment needs to address not only preparedness, as part of governance, that drives the pre-incident phase but also resilience during the crisis and post-incident phase. We should also look to the refine and transform functions (improving through the incident and learning after the incident). In order to achieve this, Government should appoint a well-resourced, independently-chaired, expert panel to urgently conduct the comprehensive national assessment and to report publicly within six months.

The second recommendation is to establish a dedicated office of cyber threat intelligence to provide a "full spectrum" strategic approach by building an Australian Cyber Preparedness and Resilience "early warning system" to identify and respond to current or emerging direct cyber risks to national interests. This would have to treat national vulnerabilities on the same level as external threats.

The third recommendation is for the government to submit triennial national Cyber Preparedness and Resilience Assessments to Parliament, prepared by a high-level expert group working with relevant agencies and university researchers, to provide a regular, publicly-available assessment of related trends, risks and impacts.

The fourth recommendation is to build an Australian National Cyber Catastrophe Readiness Framework, including maturity levels, and a roadmap to deal with the inevitable cascading disruptions, especially outside cyberspace. This should address the concept of chaos engineering, which can be used to explore and understand system behaviour under stress and provide assurance and continuity during disruptions.

Fifth, Australia needs a new doctrine, appropriate legal authorities and dedicated spending for implementation of a national civil preparedness program in order to mobilise standing capabilities that can begin to address escalating threats in at least two areas: national cyber emergency and sustained disinformation attacks. The mechanisms of

government for addressing these threats will differ substantially, and new threats may arise, but adoption of a civil preparedness doctrine may be the only way of mobilising engagement of key communities and the majority of citizens. The governmental agencies assigned these missions would ideally be supported by a standing task force or commission on national civil preparedness that produces extensive and fully-funded in-depth research. This research would ideally include annual national surveys of public attitudes to national resilience and preparedness for cyberspace in general and in discrete sectors of the economy and society.

The **Social Cyber Institute** (SCI) creates new social science insights to complement technology in the fight for a more secure cyberspace that supports individual, community and national interests on an equitable and rights-based foundation. SCI undertakes organises webinars, conference participation, and seminars, and publishes opinion, analysis and research reports and papers. SCI is a non-profit organisation supported by the Social Cyber Group which separately offers advisory and training services in cyber policy. https://socialcyber.co/social-cyber-institute

Director: Professor Glenn Withers (glenn.withers@socialcyber.co)

SOCIAL CYBER ACADEMY

The **Social Cyber Group** (SCG) and **Blended Learning International** (BLI) join forces to deliver exciting international learning experiences with high business and policy relevance, through the Social Cyber Academy. Our dedicated partners in similar professional education activities in recent years have included the **Korea Development Institute** and the **Global Development Learning Network** of the World Bank. The leaders of SCG and BLI rely on decades of experience in university-based and professional education in the US, the UK, Australia and Asia. Other clients of our Academy leaders in the field of education delivery in Australia have ranged from the Australian Department of Defence, Victorian Parliament, and the Australian Indigenous Leadership Council, through to Australian Securities Exchange, Commonwealth Bank, QANTAS Engineering, and the Salvation Army and Soldier On plus, overseas, from the Distance Learning Centre (Sri Lanka), National Organisation of Science Teachers and Educators (Philippines), and Tanri Abeng University (Indonesia), to Tongji University (China), the Singapore Exchange, National Economic Action Council (Malaysia), University of Mauritius, and the Vietnam Cryptographic Agency. https://socialcyber.co/academy

Director: Lisa Materano (lisa.materano@socialcyber.co)

SOCIAL CYBER GROUP ADVISORS

The senior researchers in the **Social Cyber Group** have decades of experience in advising government from inside and outside, often at high levels, and working with business leaders to address their strategic and operational needs. Their clients in previous roles have included the UK Foreign Office, the UK Ministry of Defence, the UK Cabinet Office, the European Commission, the New South Wales government, the Australian Department of Foreign Affairs and Trade, the Australian Director General of National Intelligence, and the Graduate Research Institute for Policy Studies in Tokyo. https://socialcyber.co/advisory

Director: Professor Greg Austin (greg.austin@socialcyber.co)