Australia needs a shake-up of defence arrangements for security of undersea cables and communication satellites

Gary Waters[1]

16 April 2026

This briefing note argues that two key foundations of Australia's critical infrastructure (undersea cables and satellite communications systems) are dangerously under-protected. The current framework, legislative, governance and capability settings for their security need urgent reform. This is especially so as reliance on Artificial Intelligence (AI), cloud services and Low-Earth Orbit (LEO) satellite constellations is accelerating. Even minor disruptions to these systems could cascade across national energy grids, emergency services, financial markets and national security operations.

There is an opportunity for Government to address this vital element of national Critical Infrastructure resilience as it responds to Dr Jill Slay's *Independent Review of the Security of Critical Infrastructure Act 2018*. It will certainly need to do more than that suggested in its *Consultation Paper for the Proposed Amendments to the Ministerial Directions Powers* and its *Consultation on the Exposure Draft of the Critical Infrastructure Risk Management Program Rules*.

Why Space and Seabed Infrastructure Matters

The *World Economic Forum Global Cyber Security Outlook of 2026* identified that "space and seabed infrastructure remain comparatively overlooked in cyber risk planning, despite enabling core functions of critical infrastructure" (pp. 54-55). It argues that by 2030, satellite-based positioning, navigation and timing will be even more essential for aviation, maritime activities, power-grid coordination and financial transactions, while satellite communications and undersea cables will form the backbone for emergency services, cloud infrastructure and international data exchange.

Very few critical infrastructure providers in Australia are considering space assets and undersea cables in their Critical Infrastructure Risk Management Plans.

[1] Gary Waters is a Distinguished Fellow, Social Cyber Institute. He was co-author with Des Ball and Ian Dudgeon of the ground-breaking analysis of Australia and Cyber Warfare (2008).

Vulnerabilities in LEO Satellite Systems

Another warning signal, if one is even needed, relates to issues raised in a new intelligence agencies' report from Australia, Canada, New Zealand and the United States that as more and more satellite communication systems launch into low earth orbit, the "attack surface" for malicious cyber actors will grow as well. The key services these new constellations provide include low-latency and high-bandwidth internet, mobile backhaul and direct-to-device communication. The report states:

> This growth puts critical networks that depend on these satellite services at greater risk. Securing this infrastructure is essential to ensuring the resilience of commercial communications, national security systems and emergency response capabilities. A successful cyber attack could lead to service disruptions, exposure of sensitive data, and even physical harm to individuals and assets. This reinforces the urgent need for robust cyber security measures.

The report tacitly acknowledges the cyber-physical nexus as it identifies the risk areas as the satellites themselves, the ground stations and terminals, end user devices that connect to LEO services, communication links and the supply chain.

Australia's Undersea Cable Exposure

These vulnerabilities in space infrastructure are mirrored—and in some respects are even more acute—in Australia's dependence on undersea cables which deliver most of the country's data and communications. The cables have inadequate protections in law, policy and capability to protect and repair them in the event of attack. Chief of the Royal Australian Navy, Vice Adm. Mark Hammond, told the 2025 Indo-Pacific International Maritime Exposition that Australia's connectivity to the global financial system and people across the world depends on the integrity of around 16 international submarine cables that plug in at various points along our coastline.

He said that the stakes of failing to protect or quickly repair those cables are existential: "While maritime trade routes and seabed cables are our lifelines, they are also our greatest vulnerabilities. The loss of either would be an existential threat to our island and to our people." This characterisation of cable disruption as "existential" underscores that the issue is not merely commercial or technical, but one of national survival.

Despite growing dependence on these undersea cables, the Australian Government has not established comprehensive accountability frameworks or response capabilities in the event of disruption. Current repair arrangements rely on private operators, seemingly on an ad hoc basis that can be subject to significant procedural delays. If the physical vulnerabilities are not adequately addressed and the cyber vulnerabilities are largely ignored, this combination of vulnerabilities could lead to disaster.

Furthermore, the importance of undersea cables is growing rapidly in cadence with the explosive growth of artificial intelligence networks that underpin data centres. Yet much of the international work on undersea cable security centres on protecting them from natural events,

intentional physical attacks or disruption, and deliberate sabotage through various means. It is time to address the cyber domain, prioritise backup connectivity in the event of cable outages, whether as a result of cyber or physical disruption, and implement strong cyber-security measures to protect from cyber-attacks that should include network monitoring, intrusion-detection systems and incident-response capabilities.

Adding to these concerns is that on 9 April 2026, British Defence Secretary John Healey told a press conference in London that the UK had uncovered a secret Russian attack submarine and underwater spy vessel mission in and around British waters that lasted over a month and threatened undersea cables. He said the deployment involved an *Akula*-class combat submarine (SSN) and a pair of surveillance submarines from Russia's Main Directorate for Deep Sea Research (GUGI).

Healey said that the *Akula* was "likely" used as a decoy to distract from the GUGI-led activities, as the sister vessels "spent time over critical infrastructure relevant to us and our allies in the North Atlantic." He also said there was "no evidence" that the cables or underwater pipelines had been damaged.

Healey said there would be serious consequences if any attempt was made by Moscow to destroy subsea infrastructure, though he did not reveal what options might be considered to effect those serious consequences.

Russia can use these GUGI vessels to place wiretaps on undersea cables or collect intelligence to support contingency planning to disrupt NATO communications in the event of war.

Cyber-Physical Warfare as a Strategic Challenge

The term 'Cyber-Physical Warfare' relates to digital attacks that cause physical harm, especially to critical infrastructure like energy grids, water supplies, transportation networks, and communication systems, all of which depend on satellites and undersea cables. Cyber-Physical Warfare exploits interconnectedness of systems that create attack vectors spanning digital and physical domains; affords asymmetric advantage, whereby cyber capabilities offer disproportionate power to disrupt; and poses attribution challenges in that tracing the origin of cyber-attacks is often difficult, complicating response and deterrence strategies. The net effect is for cyber-attacks to cause tangible damage to physical assets and human well-being.

Most critical infrastructure entities assess cyber risk through a corporate lens, focussed on financial, reputational and technical aspects. The expanding potential of Cyber-Physical Warfare now suggests that cyber risk cannot be assessed in isolation from foreign policy and foreign interference objectives.

Recommendations

The recommendations are:

- Explicitly designate undersea cables and satellite systems as systems of national significance
- Assign a lead agency for seabed infrastructure protection
- Invest in sovereign undersea cable repair, monitoring and response capabilities
- Integrate cyber and physical risks into a unified cyber-physical risk framework as part of the Government's critical infrastructure risk management framework
- Mandate cyber-physical risk assessments as part of Critical Infrastructure Risk Management Plans
- Integrate satellite and undersea cable scenarios into national security and critical infrastructure preparedness and resilience exercises
- Strengthen collaboration with allies and industry on space and seabed infrastructure protection.

Conclusion

Australia's dependence on space-based and seabed infrastructure is growing faster than the policies and capabilities designed to protect it. The convergence of cyber and physical threats means that disruption to satellites or undersea cables could have immediate and far-reaching national consequences.

The window for preventive action is narrowing. Without urgent reform to governance, legislation, and capability development, Australia risks strategic surprise in a domain that underpins its economy, security, and sovereignty.