Webinar
on
Securing the Indo-Pacific's Digital Arteries
India-Australia Collaboration for Cyber and Maritime Resilience

27th August, Wednesday; 1700hrs AEST/1230hrs IST

1. Background

1.1 The Indo-Pacific has become the epicentre of great power competition, with submarine communication cables carrying over 95% of global intercontinental data emerging as critical instruments of geopolitical influence, economic leverage, and national security. These underwater arteries, vital to the 21st-century information economy, are increasingly contested as digital economies expand and artificial intelligence reshapes global commerce.

1.2. The rapid digitisation of critical infrastructure across sectors such as energy, transport, finance, and telecommunications has heightened the need for robust cybersecurity measures. In the Indo-Pacific region, securing underwater digital infrastructure especially subsea cables and ensuring cyber-physical security are paramount to maintaining economic and national security.

1.3. India and Australia's – the two key players with their strategic positioning, marked by ambitious infrastructure investments and multilateral security partnerships like the Quad, are pivotal in reshaping the region's digital architecture. India and Australia's maritime cooperation, anchored in shared Indo-Pacific priorities, lays a strong foundation for broader security partnerships. By leveraging joint naval exercises, such as Malabar and AUSINDEX, and integrating advanced technology-sharing platforms, both nations can address emerging threats like hybrid warfare and supply chain vulnerabilities over the next decade.

1.4. The fifth India-Australia Cyber Policy Dialogue (2022), under the 2020-2025 Framework Arrangement on Cyber and Cyber-Enabled Critical Technology Cooperation, builds on the Comprehensive Strategic Partnership elevated in 2020. This partnership, supported by the Australia-India Cyber and Critical Technology Partnership (AICCTP) awarding of $1.6 million in grant fund, fosters collaboration in cybersecurity, digital economy, and emerging technologies.[1]

1.5. Australia's expertise, through the Australian Cyber Security Centre (ACSC) and its corporate intelligence-sharing model, complements India's advancements, including CERT-In (Indian Computer Emergency Response Team) and NCIIPC (National Critical Information Infrastructure Protection Centre), which elevated both countries as Tier 1 as per the Global Cybersecurity Index 2024[2] highlighting their cybersecurity commitments. Bilateral frameworks

[1] https://www.nisr.org.au/article/australia-and-india-unite-to-drive-inclusive-digital-public-infrastructure
[2] https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

for cyber threat intelligence sharing, inspired by Australia's Cable Protection Zones (CPZ) and Quad coordination, can safeguard maritime networks and high-density cable routes within India's Exclusive Economic Zone (EEZ). Policy reforms, such as Telecom Regulatory Authority of India (TRAI) 2023 recommendations to eliminate Cable Landing Stations (CLS) licence fees, could attract Australian investment, leveraging India's strategic location as an East-West transit hub.

1.6. Maritime and cyber resilience in the Indo-Pacific is a shared priority, amplified by the Russia-Ukraine conflict's demonstration of hybrid warfare and China's alleged cyber operations. Through Indian Ocean Rim Association (IORA) and Quad, India and Australia can lead regional frameworks aligned with UNCLOS, fostering operational synergy and private-sector. This webinar explores these imperatives to strengthen bilateral and regional cyber and maritime security.

2. **Objectives**

- To explore opportunities for India and Australia to strengthen bilateral cybersecurity frameworks in response to evolving cyber threats.
- To evaluate the role of scientific and policy innovations in enhancing subsea cable resilience and cyber-physical infrastructure protection in the Indo-Pacific.
- Explore bilateral frameworks for cyber threat intelligence sharing and strategies to enhance maritime and cyber resilience, with a focus on India-Australia collaboration.

3. **Discussion Topics**

- How can India and Australia leverage AI and robotic systems to secure underwater digital infrastructure and reduce subsea cable vulnerabilities?
- What strategies can strengthen cyber-physical security for energy, transport, finance, and telecommunications amidst rising Advanced Persistent Threat (APT) threats?
- How can bilateral frameworks for cyber threat intelligence sharing, inspired by Australia's CPZ, enhance Indo-Pacific resilience?
- What role can IORA and Quad play in fostering maritime and cyber resilience through India-Australia collaboration?
- Looking forward, what opportunities exist for India-Australia security partnerships to expand beyond cyber and maritime domains, potentially incorporating space security, counter-terrorism, and supply chain defense collaborations for long-term regional stability?

4. Session Flow

Time (AEST)	Agenda
17:00 – 17:15	Welcome and Introduction
17:15 – 17:30	Panelists Opening Remarks
17:30 – 17:50	Q & A
17:50 – 18:00	Panelists Closing Remarks