

# Securing the Seabed:

## A Canada–Japan Strategy for Undersea Cable Resilience

Jonathan Berkshire Miller

March 2026



**MIGS** Montreal  
Institute  
for Global  
Security

## Acknowledgements

The Montreal Institute for Global Security (MIGS) would like to express its sincere gratitude to the Asia Pacific Foundation of Canada for its generous support of this research through the Canada–Asia Joint Research Grants program. The Canada–Japan Subsea Cable Security Partnership (CJ-CABLE) project was made possible through their commitment to advancing policy-relevant research and strengthening Canada’s engagement in the Indo-Pacific.

MIGS is especially appreciative of the Foundation’s role in enabling meaningful dialogue, field research, and collaboration with partners across Japan. Their support facilitated critical exchanges with policymakers, experts, and institutions, which significantly enriched the analysis and recommendations presented in this paper.

We would like to thank the many local organizations, offices and institutes who contributed their expertise and perspectives throughout the project. Their contributions strengthened bilateral understanding and helped identify practical pathways for advancing Canada-Japan collaboration on subsea cable security and broader critical infrastructure protection. The analysis presented in this paper benefited from constructive dialogue and exchanges with representatives from:

- Embassy of Canada to Japan
- Ministry of Foreign Affairs of Japan
- Ministry of Economy, Trade and Industry
- Nippon Foundation
- Sasakawa Peace Foundation
- Nakasone Peace Institute
- International House of Japan
- Institute of Geoeconomics
- JIIA Center for Global Outreach
- University of Tokyo
- Temple University Japan
- United Nations University
- Fujitsu Future Studies Center
- Mainichi Newspaper
- Waseda University

## Executive summary

Undersea cables carry more than 95% of global data traffic and form the backbone of the global digital economy, supporting financial markets, military communications, energy systems, and everyday connectivity. Despite their importance, these systems remain vulnerable to physical disruption, cyber intrusion, and growing geopolitical competition. As tensions increase in the Indo-Pacific and new connectivity routes emerge in the Arctic, subsea cable security has become a critical issue for national security, economic resilience, and global stability.

Consultations held in Tokyo with Japanese government officials, industry leaders, and policy experts highlighted a shared recognition between Canada and Japan that subsea cable infrastructure is a strategic asset. Both countries face similar vulnerabilities and have strong incentives to strengthen cooperation to protect critical infrastructure and support the rules-based international order.

The threat environment is evolving. While past disruptions were primarily accidental, current risks increasingly include grey-zone activity, suspicious maritime behavior near cable routes, and cyber vulnerabilities at cable landing stations and network control systems. Even limited disruptions can have cascading economic and security consequences.

Canada and Japan already possess strong foundations for deeper cooperation through defence agreements, intelligence-sharing mechanisms, and aligned Indo-Pacific strategies. However, subsea cable security has not yet been fully integrated into bilateral cooperation frameworks.

To strengthen resilience, the report proposes a coordinated Canada–Japan dual-theatre approach spanning the Indo-Pacific and the Arctic:

- **Establish a permanent bilateral working group** on subsea cable security to coordinate intelligence sharing, joint threat assessments, and crisis response planning.
- **Develop harmonized security standards** addressing both physical resilience and cybersecurity for cable infrastructure.
- **Enhance maritime domain awareness**, including satellite monitoring, AIS data integration, and expanded Arctic surveillance capabilities.
- **Strengthen rapid repair capacity**, including agreements with cable repair operators and contingency planning for Arctic operations.
- **Promote joint research and technological innovation**, including autonomous inspection systems, AI-enabled anomaly detection, and secure network management technologies.

Strengthened cooperation on subsea cable security would enhance deterrence against grey-zone coercion, safeguard economic connectivity, and position Canada and Japan as leaders in shaping emerging international norms for the protection of critical infrastructure.

# A Policy Roadmap for Democratic Resilience in the Indo-Pacific and the Arctic

*This policy paper draws on insights from a week of meetings in Tokyo with Japanese government officials, representatives, industry leaders, and leading policy institutes, as part of a delegation organized by the Montreal Institute for Global Security. Across discussions with ministries, think tanks, and security practitioners, one theme consistently emerged: the protection of undersea cable infrastructure has moved from the technical margins of public policy to the strategic center of national security planning.*

---

## Introduction: From Invisible Infrastructure to Strategic Asset

Undersea cables rarely attract public attention. Buried beneath the seabed, they carry more than 95 percent of global data traffic and underpin the digital architecture of modern life. Subsea cables are used for financial transactions, communication by the military, operation of energy grids, as well as daily movement of data and information between various locations around the globe. However, despite providing such critical services, they remain vulnerable due to physical vulnerability, inadequate legal protections, and exposure to geostrategic risks.

It was also evident from the discussions in Tokyo that many of the policymakers in Japan see submarine cable infrastructure as a strategic asset rather than simply a passive commercial utility in a rapidly changing and highly competitive geostrategic environment. Japan's position is mirrored by those in Canada, who have come to realize that economic security, digital resilience, and engagement in the Indo-Pacific region have moved to the top of the list of priorities in Canadian policy discourse. There is a profound connection developing between the two countries: two of the world's leading democracies, which are geographically distant from each other but strategically aligned, have now recognized that infrastructure located beneath the ocean floor has become a domain of competition.

While the primary area of concern for this type of competition will likely be the Indo-Pacific region, it is also one of the areas of the world with the highest concentration of cable routes (in addition to high levels of marine traffic), and it is also located over several of the world's most contested bodies of water. In addition, the effects of climate change and changes to global shipping routes have created a second emerging front - the Arctic - that could potentially shape the future of global connectivity through new subsea cable routes. As the ice melts and new infrastructure emerges in the north, if appropriate governance structures and mechanisms to increase the resilience of subsea cable infrastructure are not put into place soon, then new vulnerabilities to exploitation could emerge.

Therefore, Canada and Japan face a common challenge: How can we protect subsea cable infrastructure in both the Indo-Pacific and the Arctic to enhance deterrence, increase resilience, and support the rules-based international order?

---

## The Evolving Threat Environment

For years, almost all the issues with cable disruptions were due to accidents - fishing trawlers dragging their anchors, earthquakes, or simply equipment failure. However, the threat landscape has changed over time. New types of threats exist today, including grey zone tactics, uncertain maritime behaviors, and the blending of cyber-physical threats.

In Europe, there is an unusual number of occurrences of undersea cables being damaged. This has caused concern about the use of "hybrid sabotage." The Estlink-2 power cable was severed in the Baltic Sea during December 2024 and along with several telecom cables, it was found to be damaged due to a tanker pulling on its anchor for the purpose of a deliberate act. It was also found that this was part of a larger group of similar incidents that involved tankers that were tied to Russia's "shadow fleet." Other cables in the Baltic Sea, including the C-Lion1 cable between Finland and Germany, were also damaged multiple times. NATO has increased patrols of the Baltic area in response to concerns that such incidents may be testing vulnerabilities in critical infrastructure.

Taiwan has had far more incidents than anywhere else in the world, and nearly all of them appear to be related to China's efforts to exert "gray zone" pressure. There have been numerous reports of vessels that have been suspected of cutting underwater cables. For example, the 2023 incident in which connections to the Matsu Islands were cut off, and at least five incidents in 2025 where cables were damaged by ships such as the Shunxin-39 and the Hong Tai 58 while they were located near the city of Taipei and the Penghu Islands. In many of the cases, the ships were seen to linger or make erratic maneuvers above the location of the cables. While it is impossible to attribute blame in most of these cases, the actions of the ships clearly indicate that some type of intentional interference occurred.

Japanese participants emphasized how difficult attribution is within the maritime domain. While suspicious vessel behavior around cable routes creates uncertainty and does not cross into the realm of armed conflict, even minor disruptions can create cascading effects upon financial markets and communication networks. This ambiguity is central to coercive strategies below the threshold of war.

Threats are no longer limited to being physical. Terrestrial landing stations - the terrestrial locations at which submarine cables connect to the domestic network - are susceptible to cyber intrusion, sabotage, or coordinated disruptions. Additionally, the merging of cyber and maritime domains

complicates existing governing structures which have traditionally divided responsibility for naval security from that of telecommunications oversight.

Although Canada may be physically removed from some of the areas of conflict in the Indo-Pacific, as a Pacific nation, Canada is not immune to these events. Canada's economy and intelligence apparatuses are deeply connected across the region. Therefore, any disruptions to East Asian cable networks will likely resonate immediately throughout Canada's markets and government systems. In addition, Canada's Northern geography presents a unique dimension. Projects connecting Canada to the rest of the world via cable across the Arctic, previously speculative, are becoming feasible. In the absence of any coordination between nations regarding the development of new Arctic cable routes, there is a high likelihood that these projects will create governance and security gaps similar to those present in other regions.

The primary strategic takeaway from the Tokyo meetings was that subsea cables are currently an element of geopolitical competition. Protecting them will require the shift from providing solely technical solutions to developing and implementing fully integrated policy solutions.

---

## Foundations for Cooperation

Both Canada and Japan have an institutionally strong base on which to develop further. Over the last ten years, bilateral defence cooperation has grown exponentially. Bilateral agreements on intelligence exchange; the transfer of defence technologies; and interoperable logistics, all support enhanced trust between Canada and Japan.

The current level of defence cooperation is a natural fit for cable security cooperation. Threat information regarding cables can be included within intelligence exchange mechanisms. Transfer of technology agreements will allow for cooperative development of monitoring systems and other secure components of infrastructure. Dialogue between military personnel can extend beyond maritime protection of the underwater environment of critical infrastructure.

Both Canada and Japan have stated Indo-Pacific strategies that are built around the theme of securing their economies through infrastructure resiliency and through strict adherence to international law and rules.

Japan's evolution of its national security now identifies the economy as one of several domains that will require strategic consideration and action by the Government of Japan. Canada's Indo-Pacific Strategy similarly states the importance of protecting critical infrastructure and supply lines. Thus, the alignment of policy is not simply a statement or rhetoric but structural. While there is currently a basis for cable security to become a part of the core bilateral agenda, it has not yet done so.

Establishing this as a core bilateral agenda would provide strategic agreement and convert this into practical cooperation.

---

## Policy Recommendations: A Dual-Theatre Framework

To move from alignment to action, Canada and Japan should adopt a coordinated policy framework that spans both the Indo-Pacific and the Arctic. The approach must integrate intelligence, industry, maritime security, and technological innovation.

First, the two nations need to develop a permanent bilateral working group whose purpose is to work towards resilience in subsea infrastructure. The working group should be composed of representatives from foreign affairs, defence, cybersecurity agencies, coast guards and telecommunications regulators, as well as several private sector operators. The working group should also produce joint threat assessments, share maritime and cyber intelligence related to cable routes and coordinate crisis response plans. Prior to a real-world event occurring, regular tabletop exercises simulating cable disruptions - both in Indo-Pacific choke points and Arctic environments - will allow for testing readiness and clarifying responsibilities.

Secondly, Canada and Japan should work collaboratively - and in tandem with other allies like the US - toward creating harmonized security standards for cable infrastructure. The security standards developed by the two countries should address both physical resilience (i.e., armoring, route redundancy, landing station hardening) and cybersecurity requirements for network management systems. The standards developed for the Arctic environment will need to take into consideration ice-resistant design, extreme weather resistance, and remote repair logistics. The use of a harmonized regulatory process will help to reduce friction for private operators and ensure that security is considered at the outset of each project.

Thirdly, increased maritime domain awareness must serve as the basis for protecting the cables. In the Indo-Pacific, this will require the integration of satellite imagery, Automatic Identification System (AIS) data and naval patrol reports to monitor suspicious activities near cable routes. Because surveillance capabilities in the Arctic remain more limited than in the Indo-Pacific, the focus for the two countries will be on increasing satellite-based surveillance capability, sharing hydrographic data and developing technologies that will enable the monitoring of ice-covered areas. Canada has significant experience in Arctic surveillance and Japan has advanced maritime monitoring technologies; therefore, the two countries can utilize their respective strengths through joint research and operational exchanges.

Fourthly, the capacity to rapidly repair damaged cables is crucial for ensuring the resilience and deterrence of cable infrastructure. Therefore, both countries should seek to enter into pre-negotiated standby agreements with global cable vessel operators to ensure that the operators will

deploy priority cable repair vessels in the event of a crisis. Coordinated naval or coast guard support for repair missions in contested waters in the Indo-Pacific theater will send a clear signal that interference will not provide a strategic advantage. In the Arctic, contingency planning must include the prepositioning of repair equipment in northern ports, agreements for ice capable support vessels, and tabletop exercises designed to simulate the challenges associated with operating in extreme environmental conditions.

Lastly, innovation should be a major component of the partnership. Joint R&D initiatives may focus on the use of autonomous underwater vehicles for cable inspection, the use of artificial intelligence (AI) enabled anomaly detection systems to identify suspicious maritime traffic patterns and secure firmware solutions to protect control systems from cyber compromise. The bilateral technology transfer framework provides a vehicle for the collaborative development of new technologies while protecting intellectual property. The universities and research institutions in both countries - especially those specializing in Arctic sciences and maritime engineering - should be integrated into the effort to create a pipeline of experts in this field.

Finally, Canada and Japan can use their cooperation to promote the creation of additional international norms. They can advocate for principles that prohibit the intentional interference with subsea cables and promote transparency in maritime operations near critical infrastructure, through forums such as the G7 and regional security dialogue mechanisms. Additionally, they can undertake capacity building programs for smaller Indo-Pacific and Arctic states that host cable landing points to build regional resilience and demonstrate positive leadership.

---

## Strategic Implications

Enhancing subsea cable security in Canada-Japan relations has implications far beyond protecting physical infrastructure.

Firstly, enhanced subsea cable security elevates deterrence in the "grey zone" because visible coordination, the sharing of intelligence, and rapid response capabilities diminish the attractiveness of ambiguous forms of coercion.

Secondly, enhanced subsea cable security increases economic resilience by ensuring reliable connectivity for financial markets, trade flows, and essential public services. Enhancing the resilience of subsea cables through early integration into the design process and governance structure of these systems will ensure that the economic interests of both Canada and Japan (and the global digital economy on which other allied nations rely) will be protected.

Thirdly, cooperation between Canada and Japan in both the Indo-Pacific region and the Arctic demonstrates that coordination among democracies does not need to be geographically limited.

Expanding cooperation into the Arctic will support Canada's interest in maintaining its sovereignty and supports Japan's increasing presence in the Arctic; it will further ensure that future infrastructure development in polar waters is governed by principles of openness, environmental responsibility, and rules-based cooperation.

Lastly, the enhancement of subsea cable security cooperation between Canada and Japan positions these two middle powers as standard setters in cable security. They are also powers connected through the strategic gateway to the Arctic and collaboration between Tokyo and Ottawa is growing over the months. When middle power countries act early and cooperatively in emerging areas of governance, they often have a significant role in shaping the norms and standards of practice in those areas prior to a crisis. Institutionalizing cooperation in subsea cable security now will provide Canada and Japan with an opportunity to establish such standards and practices.

The MIGS Tokyo consultations demonstrated that infrastructure security has become an integral part of geopolitical strategies and subsea cables represent the point where maritime competition, digital transformation, and economic interdependency converge. Treating subsea cables purely as technical assets underestimates their strategic significance.

---

## Conclusion

The week of discussions in Tokyo confirmed that Canada and Japan share not only threat perceptions but also strategic opportunity. Subsea cable security offers a concrete, practical avenue to deepen bilateral cooperation while advancing broader Indo-Pacific and Arctic objectives.

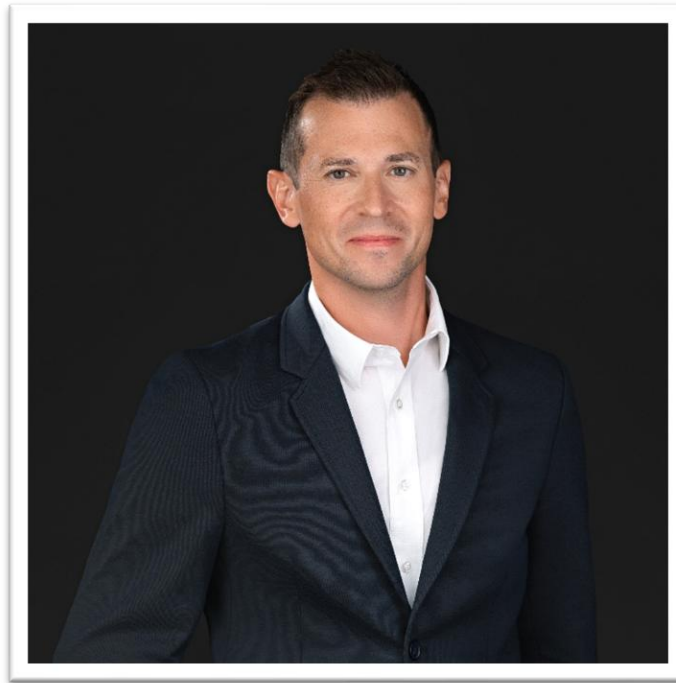
By institutionalizing intelligence sharing, aligning public-private standards, enhancing maritime awareness, investing in innovation, and shaping international norms, Canada and Japan can move from episodic dialogue to sustained partnership. Integrating Arctic collaboration into this framework ensures that emerging northern connectivity evolves within a secure and rules-based environment rather than replicating existing vulnerabilities.

Protecting undersea cables is ultimately about defending the connective tissue of democratic societies. Beneath the ocean surface lies the infrastructure that sustains economic prosperity, military readiness, and social cohesion. Through deliberate and coordinated action in both the Indo-Pacific and the Arctic, Canada and Japan can help ensure that this infrastructure remains resilient, secure, and governed by rules rather than coercion.

## Resources and additional reading material

1. Government of Canada, *Canada's Indo-Pacific Strategy*, Global Affairs Canada, 2022, [https://www.international.gc.ca/world-monde/international\\_relations-relations\\_internationales/indo-pacific-strategie-strategie-indo-pacifique.aspx](https://www.international.gc.ca/world-monde/international_relations-relations_internationales/indo-pacific-strategie-strategie-indo-pacifique.aspx).
2. Government of Canada, *Joint Statement on the Security and Resilience of Undersea Cables*, Global Affairs Canada, September 2024, <https://www.canada.ca/en/global-affairs/news/2024/09/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world.html>.
3. Government of Japan, *Free and Open Indo-Pacific (FOIP) Vision*, Ministry of Foreign Affairs of Japan, 2022, <https://www.mofa.go.jp/files/100330615.pdf>.
4. Government of Japan, *National Security Strategy*, Cabinet Secretariat of Japan, 2023, <https://www.cas.go.jp/jp/siryoku/221216anzenhoshou/nss-e.pdf>
5. Government of Canada, *Equipment and Technology Transfer Agreement between Canada and Japan*, Department of National Defence, January 2026, <https://www.canada.ca/en/department-national-defence/news/2026/01/minister-mcguinty-signs-an-equipment-and-technology-transfer-agreement-with-japan.html>.
6. Government of Canada, *Acquisition and Cross-Servicing Agreement (ACSA) with Japan*, Global Affairs Canada, 2018, <https://www.canada.ca/en/global-affairs/news/2018/04/canada-and-japan-sign-acquisition-and-cross-servicing-agreement-to-strengthen-military-cooperation.html>.
7. Government of Canada, *Cyber Security of Critical Infrastructure: A Canadian Perspective*, Communications Security Establishment (CSE), 2023, <https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2023-2024>
8. Government of Canada, 2026, *Canada-Japan Strategic Roadmap* <https://www.pm.gc.ca/en/news/backgrounders/2026/03/06/canada-japan-comprehensive-strategic-roadmap>
9. Government of Canada, *Arctic and Northern Policy Framework*, 2019, <https://www.rcaanc-cirnac.gc.ca/eng/1560523306861/1560523330587>.
10. Government of Japan, *Japan Arctic Policy*, Ministry of Foreign Affairs, 2023, [https://www8.cao.go.jp/ocean/english/index\\_e.html](https://www8.cao.go.jp/ocean/english/index_e.html)
11. Government of Canada, *National Shipbuilding Strategy Overview*, Public Services and Procurement Canada, 2023, <https://www.canada.ca/en/public-services-procurement/corporate/transparency/briefing-materials/standing-committee-public-accounts/2021-05-25/national-shipbuilding-strategy-overview.html>
12. Government of Canada, *Canada's Critical Infrastructure: Cyber and Physical Resilience*, Public Safety Canada, 2024, <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx>
13. Government of Japan, *Cybersecurity Guidelines for Critical Infrastructure*, National Center of Incident Readiness and Strategy for Cybersecurity (NISC), 2022, [https://www.nisc.go.jp/eng/pdf/cyber\\_guidelines.pdf](https://www.nisc.go.jp/eng/pdf/cyber_guidelines.pdf).

## About the Author



**Jonathan Berkshire Miller** is an internationally recognized expert in security, defence, and geoeconomics, advising governments, multinational corporations, and international organizations on geopolitical risk and strategic decision-making. He is co-founder and Principal of Pendulum Geopolitical Advisory in Ottawa and serves as a Senior Fellow - Indo-Pacific at the Montreal Institute for Global Security (MIGS) and Senior Fellow at the Macdonald-Laurier Institute. Miller also holds senior fellowships with the Japan Institute of International Affairs and the Asian Forum Japan and co-founded the Council on International Policy. With nearly two decades of experience across the public and private sectors, including work with the Canadian federal government on Asia-related economic and security issues, he is a frequent contributor to leading publications and a regular commentator in international media on global security and geopolitical affairs.

# MIGS Montreal Institute for Global Security

## About the Montreal Institute for Global Security

The Montreal Institute for Global Security (MIGS) is a Canadian think tank dedicated to strengthening democratic resilience and addressing emerging global security challenges. MIGS works at the intersection of geopolitics, technology, and human rights, producing policy research and convening global leaders to develop solutions to some of the most pressing threats facing democratic societies today. Through research, high level dialogues, and strategic partnerships, MIGS contributes to policy debates on issues such as authoritarian influence, transnational repression, emerging technologies, and international security cooperation. The institute engages policymakers, scholars, civil society leaders, and industry experts in Canada and internationally.

---

### Montreal Institute for Global Security

Montreal, Canada

[www.migsinstitute.org](http://www.migsinstitute.org)

[LinkedIn](#)

[X](#)

©2026 Montreal Institute for Global Security. All rights reserved. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the Montreal Institute for Global Security or its partners.