NETWORK SIGNALLING UNDER UNCERTAINTY: LESSONS FROM THE BALTIC SEA FOR A CANADIAN UNDERSEA CABLE POSTURE

Nicole Jackson

Simon Fraser University, Canada

Abstract

Undersea communication cables have become strategic infrastructure because they sit at the intersection of economic connectivity, military resilience, and information stability. Generally, privately financed and operated, and routinely damaged by accidents, they carry almost all international data traffic and are increasingly probed through ambiguous, below-threshold disruption. The paper therefore provides a forward-looking assessment of risks and governance gaps in cable security. It argues that cable security is best understood as a problem of resilience governance under uncertainty. It also argues that network signalling under uncertainty can reduce leverage created by ambiguous incidents when attribution remains probabilistic. It develops a framework in which governments, operators, local authorities, regulators, Northern and Indigenous governments, and communities signal collectively through operations, law, repair readiness, and public communication. Empirically, the paper treats Canada's Arctic and North Pacific approaches as the core case and the Baltic Sea and adjacent North Sea as a learning environment. It uses Baltic incidents and NATO–EU responses to identify building block practices and to specify what a credible Canadian signalling posture could require. This includes cooperation with Japan and the Republic of Korea to extend this logic into the wider North Pacific.

The corresponding author states that there is no conflict of interest.

1. Introduction

Undersea cables carry almost all international data traffic and underpin cloud services, financial markets, public administration, and military communications. Yet they are generally privately financed and operated, difficult to monitor, and routinely damaged by accidents. They are therefore a revealing case of a wider governance challenge: how states and societies manage strategically important infrastructure when disruption is hard to interpret, authority is dispersed, and facts remain incomplete.

Well over 95 per cent of intercontinental data traffic is estimated to travel through submarine fibre systems, which also support cloud services, financial markets, and military communications (TeleGeography, 2023; Bueger & Liebetrau, 2021). They run through an environment that is difficult to monitor and is in practice rarely protected at the seabed, which makes them attractive in contemporary hybrid competition (Mazarr, 2015). Most disruptions stem from accidents or natural hazards. Yet recent work on Europe by the International Institute for Strategic Studies links this dependence to a growing pattern of suspected Russian sabotage and other hostile activity against critical infrastructure, including pipelines and data cables (International Institute for Strategic Studies, 2024). Investigations and repairs are expensive, complex, and slow. Damage occurs underwater, evidence is often partial, and actors can exploit legal and jurisdictional seams, especially in Exclusive Economic Zones (Burnett, Davenport, & Beckman, 2013). Governments must decide how to act, and what to say publicly, when they cannot quickly prove intent and misinformation and disinformation fill the gap (Rid & Buchanan, 2015).

This paper asks how Canada can build a credible signalling posture on cable security in its Arctic and North Pacific approaches. It also asks what elements of European practice, developed in the Baltic Sea and adjacent North Sea with NATO and the EU, can plausibly travel into that environment. It examines cable security as a problem of resilience governance under uncertainty, not infrastructure protection alone. *The central claim is that Canada can reduce the leverage created by ambiguous incidents through 'network signalling under uncertainty': coordinated multi-actor, multi-channel actions that show adversaries that ambiguity will not translate into leverage even when attribution remains probabilistic.* A Canadian signalling posture can therefore be built by

SFU LIBRARY DIGITAL PUBLISHING

adapting selected building blocks from the Baltic NATO-EU context to Canada's geography, institutional density, and Indigenous governance.

The paper focuses on Canada's Arctic and North Pacific approaches, including emerging trans-Arctic cable routes through Canadian northern waters and the approaches and landings of trans-Pacific cables on the British Columbia coast. These are corridors where new undersea projects, sparse governance, limited redundancy, and growing great power activity intersect most sharply. The paper compares this setting with the Baltic Sea and adjacent North Sea. This is a shallow-water, institutionally dense environment close to Russia in which ambiguous incidents involving pipelines and cables have tested NATO-EU responses (Edwards & Seidenstein, 2025; International Institute for Strategic Studies, 2024). The comparison is used to identify which practices can travel across these settings. It also highlights the conditions under which they may do so: convergence of threat perceptions, existing institutional linkages, and compatibility with Canadian geography and Indigenous/federal governance.

Canada's Arctic and North Pacific approaches are vast, persistent monitoring is uneven, and northern and coastal communities often have limited redundancy. While Canada has not yet experienced a publicly confirmed hostile attack on an undersea cable, recent domestic outages have shown how quickly single-link failures can cascade into governance problems. Telecom outages in northern Canada during the 2023 wildfire season, when communities in the Northwest Territories and Yukon lost services for extended periods, highlighted how connectivity failures can disrupt evacuations, emergency coordination, and basic economic activity (Cecco, 2023; Northwestel, 2023). At the same time, projects such as the proposed Far North Fiber trans-Arctic cable and new Arctic and northern broadband links are projected to place high-value undersea infrastructure in remote waters where detection and repair are difficult (Dalziel, 2024; Kim et al., 2025).

The analysis is theory-building and exploratory rather than a formal causal test. It draws on official documents, investigative reporting, and policy and think-tank analysis to identify which building block practices may travel, which require adaptation, and which do not. The paper does not include classified material or original interviews, so any inferences about actors' intentions or capabilities are necessarily cautious.

The paper proceeds in five sections after the introduction. Section 2 develops the conceptual framework of resilience governance under uncertainty, network signalling under uncertainty, staged attribution, and policy diffusion. Section 3 uses the Baltic Sea and adjacent North Sea as a learning environment to identify Europe's emerging signalling posture and the building blocks it contains. Section 4 examines Canada's Arctic and North Pacific exposure and governance gaps under the same categories later used for posture design. Section 5 sets out a Canadian signalling posture across four areas: integrated detection and staged attribution; vessel behaviour monitoring and administrative consequence; industry and repair coordination; and societal signalling and information planning. It then considers the posture's international extension through selective partnerships. The conclusion returns to the paper's theoretical and policy implications.

2. Conceptual Framework

2.1 Resilience governance under uncertainty

This paper treats cable security as a problem of resilience governance under uncertainty. Resilience governance under uncertainty is the capability of institutions and societies to decide and act when evidence is incomplete and stakes are high. It highlights how authorities coordinate, how responsibilities are allocated, how information flows, and how public communication is managed when facts are contested or unclear (Boin & McConnell, 2007; Dunn Cavelty, 2018). In other words, it examines how uncertainty can be governed, as opposed to endured, in grey zone environments.

Undersea cables are a complicated case because four features coincide. First, attribution often remains probabilistic. Damage occurs underwater, evidence is often partial, and adversaries can exploit legal seams in Exclusive Economic Zones and flags of convenience (Burnett et al., 2013). Second, the threat environment is hybrid. Adversaries can combine physical interference, legal grey zone tactics, and information operations around incidents (Mazarr, 2015). Third, dependence is high. Submarine fibre optic cables carry most of the international data traffic and support financial systems, cloud services, and military communications, especially in regions with limited redundancy (International Cable Protection Committee, 2009; Brunner & Suter, 2009; Edwards & Seidenstein, 2025). Accidental damage is frequent and usually benign, but a

pattern of normal disruption can create cover for deliberate, deniable interference (Starosielski, 2015). Fourth, most undersea cables are privately owned and operated, often by large United States based technology firms, which create strategic dependencies and questions about national and allied autonomy over critical connectivity (Dalziel, 2024; Kim et al., 2025).

In this setting, resilience governance under uncertainty is inherently whole-of-government and whole-of-society. In Canada, federal and territorial governments, the Canadian Armed Forces and Coast Guard, regulators, private cable owners and repair firms, Indigenous governments and organisations, local authorities, and communities all hold parts of the problem. The central question is whether these actors can detect anomalies, preserve and share evidence, coordinate attribution and consequences, and maintain public trust when they may never obtain courtroom grade proof of hostile intent.

2.2 Network signalling under uncertainty

This paper develops the concept of network signalling under uncertainty to explain how cable security's problem of ambiguity can be managed through coordinated crisis response and posture. Building on the grey-zone and deterrence literature, it refers to patterned, observable actions by multiple actors across legal, operational, and societal channels that shape how others interpret ambiguous incidents when attribution remains probabilistic. In undersea cable disruptions, network signals are meant to show that interference will be noticed, managed, and repaired. They also show that legal and administrative measures will impose costs where possible, that communities and operators have redundancy, and that attempts at coercive leverage will be neutralised even when attribution remains probabilistic. Capabilities and governance arrangements matter insofar as they are made visible and interpreted through such moves. Purely internal actions that leave no observable trace are not treated as signals.

Network signalling under uncertainty departs from classic deterrence signalling (Freedman, 2004; Nye, 2017) in three respects. It shifts attention from centralised, state driven threats to governed uncertainty, from single senders to a network of state, private, and Indigenous actors, and from discrete, one-off messages to patterned responses across operational, legal, and societal channels that shape expectations over time (Gartzke & Lindsay, 2019). It therefore connects resilience governance under uncertainty and hybrid conflict into a single

analytical problem: how institutions manage ambiguity under conditions of uncertainty in ways that reduce adversary payoff (Mazarr, 2015). Governing uncertainty becomes a matter of how well these networks send clear, credible signals amid incomplete information – i.e. network signalling under uncertainty.

Of course, network signalling under uncertainty must also anticipate an adversary's reasoning. In a probe and test mode, an (adversarial) actor causes limited damage to test detection and response. If governance is fragmented, public communication hesitant, or allied coordination slow, probes may appear cheap and informative. In a campaign of pressure mode, repeated ambiguous disruption may be used to raise perceived risk, stress alliances, and erode confidence in government. If affected states treat each event as an isolated accident, that campaign can produce leverage even when physical damage is modest (Giles, 2025; Edwards & Seidenstein, 2025). In this paper, a network signalling posture means the durable, visible policy expression of network signalling under uncertainty. A *network signalling posture on cable security* is therefore designed to undercut both logics by raising detection probability, shortening decision and repair cycles, and helping to ensure that even ambiguous incidents trigger proportionate, coordinated responses and coherent public communication.

2.3 Staged Attribution and policy diffusion as enabling concepts

Staged attribution and policy diffusion are enabling concepts that make network signalling under uncertainty operational. Staged attribution shows how this organising logic works under evidentiary pressure, while policy diffusion explains how practices travel across regions and are recombined in new settings.

To work in uncertain contexts, network signalling requires staged attribution. This is a pre-agreed ladder that links evidence thresholds to decision authorities, operational measures, and public lines. This paper's analysis suggests adapting the ADAC framework, developed to support attribution of foreign information manipulation and interference, to the undersea cable context (Palmertz et al., 2025).

ADAC distinguishes four broad evidence categories — technical, behavioural, contextual, and legal or ethical — and links them to confidence levels and response options. Translated to cable security, four stages emerge: anomaly,

suspicious interference, probable hostile activity, and high confidence attribution. Each stage combines different evidence types and activates specific internal actions and, where appropriate, external communication. The aim is not to force premature certainty, but to prevent paralysis and narrative drift by ensuring that even low-confidence signals generate structured internal responses.

For practitioners, staged attribution implies rapid processing of operator data and sensor feeds at the anomaly stage. It also requires fusion of technical indicators with behavioural and contextual information as cases escalate, as well as specialist analytic capacity to integrate intelligence, allied reporting, and open-source evidence into defensible assessments. These assessments can support administrative and diplomatic measures even when criminal proof is unavailable (Rid & Buchanan, 2015; Bager et al., 2023). Agreed confidence terminology and communication playbooks are also necessary so that assessments can be shared across agencies, with allies, and, where appropriate, with the public without understatement or overclaiming.

Policy diffusion explains how a credible signalling posture on cable security in Canada can be built from practices developed elsewhere. What travels across regions is not a complete institutional model, but a set of building block practices that can be recombined in different settings (Börzel & Risse, 2014; Stone, 2012). In Europe, four clusters are most relevant: *integrated detection and staged attribution; vessel behaviour monitoring and administrative consequence; industry and repair coordination; and societal signalling and information planning.* These are the same four clusters used later in the paper to analyse Europe's emerging signalling posture, diagnose Canadian governance gaps, and outline a Canadian posture.

These building blocks move through alliances such as NATO, regional organisations such as the European Union, minilateral coalitions such as the Joint Expeditionary Force (JEF) in Northern Europe, industry and standard-setting bodies, and epistemic communities of practitioners. Scholars show that diffusion is most likely where threat perceptions converge and institutional linkages already exist. Here these include shared concerns about Russian sabotage and Chinese hybrid operations, Canada's NATO membership and its partnerships with Japan and the Republic of Korea, and the EU–Canada digital partnership (NATO, 2022; European Commission & Government of Canada, 2023).

The paper therefore concentrates on two theatres: the Baltic Sea and adjacent North Sea as a high-frequency, institutionally dense environment, and Canada's Arctic and North Pacific approaches as a sparse, lower-frequency environment with strong Northern and Indigenous governance. The aim is to clarify how network signalling under uncertainty can be understood and operationalised through these four clusters, and to show which practices travel, which require adaptation, and which do not.

3. The Baltic Sea as a Learning Environment: Risk, governance friction and Europe's Emerging Signalling Posture

3.1 Hybrid leverage and governance friction

The Baltic Sea is a useful learning environment where repeated ambiguous incidents have exposed both hybrid leverage and governance friction in a dense institutional setting. The Baltic Sea has experienced frequent, ambiguous incidents involving cables and pipelines. It is located within a dense institutional ecosystem that includes NATO, the EU, and minilateral groupings. It also lies close to Russian ports and naval bases and has generated a visible policy learning process from operational initiatives to NATO and EU frameworks and national legal reforms (Edwards & Seidenstein, 2025; Giles, 2025; International Institute for Strategic Studies, 2024). The Baltic Sea's comparatively shallow seabed, narrow straits, and busy shipping lanes are crossed by energy and data cables that connect the Nordic and Baltic states to Germany, Poland, and the United Kingdom. Disruption here could isolate parts of the region or reroute traffic through less trusted corridors. The Baltic Sea, like the adjacent North Sea with its heavy traffic and shallow waters, is highly networked and highly exposed (International Institute for Strategic Studies, 2024; Financial Times, 2026). Undersea cables are mostly owned by private consortia, many with United States technology firms in dominant roles. This fact shapes European debates on strategic autonomy and the need for hybrid cable–satellite architectures that can reduce dependence on foreign operators (Dalziel, 2024; Kim et al., 2025; Cabroni & Gilli, 2026).

While most incidents in this region have ultimately proved to be accidents, there has been an increase in deliberate or strongly suspicious disruption. Explosions that damaged the Nord Stream pipelines in September 2022, followed by damage to the Balticconnector gas pipeline and associated telecommunications cable

between Finland and Estonia in October 2023, forced governments and alliances to improvise responses even when investigations remained incomplete and jurisdictional seams in Exclusive Economic Zones and flags of convenience complicated accountability (Adomaitis & Ahlander, 2025; Associated Press, 2025; Braw, 2025; Edwards & Seidenstein, 2025; Pancevski, 2025). Officials and analysts have documented them as part of a widening pattern of disruptive activity against critical infrastructure since Russia's full-scale invasion of Ukraine (Edwards & Seidenstein, 2025; International Institute for Strategic Studies, 2024). Their assessments underline that ambiguity may be functional rather than incidental. Small, ambiguous incidents can generate disproportionate political and administrative strain, consume investigative bandwidth, and create political risk around public attribution. When mandates are unclear and evidentiary thresholds are mismatched across agencies and allies, ambiguity becomes a weapon that delays consequences and encourages repetition.

The Baltic Sea also demonstrates a pattern of outsourced hybrid disruption. Russia and aligned actors often operate through commercial vessels, proxies, and criminal networks that complicate legal thresholds and political decision making (Giles, 2025). For cable incidents, the problem is not only who did it, but whether a state can act proportionately and credibly when it cannot, or chooses not to, make full attribution public. Adversaries can impose costs through low visibility actions while defenders face higher evidentiary and political burdens to impose consequences.

3.2 Europe's Emerging Signalling Posture

By 2024–2025, Europe's response was beginning to assemble the same four building blocks set out in section 2: integrated detection and staged attribution, vessel behaviour monitoring and administrative consequence, industry and repair coordination, and societal signalling and information planning. The subsection below traces each in turn and shows how they combine into an emerging signalling posture under uncertainty.

International law provides baseline protections for underwater cables, but scholars and practitioners have argued that existing frameworks lag operational reality, especially when incidents occur in Exclusive Economic Zones and when perpetrators operate through vessels of convenience or ambiguous conduct (Burnett et al., 2013; NOAA Office of General Counsel, 2020; Sari, 2025).

Practical governance in Europe therefore depends largely on domestic authorities, administrative tools, and coordinated allied responses.

Integrated detection and staged attribution begin with shared situational awareness and structured coordination. NATO established a Critical Undersea Infrastructure Coordination Cell to fuse information from member states, navies, coast guards, and industry into a shared picture of threats to cables and pipelines (NATO, 2023c). In January 2025, allies launched Baltic Sentry, a sustained effort to increase NATO presence and monitoring over critical undersea infrastructure. NATO navies now deploy underwater drones, artificial intelligence, and situational awareness tools to monitor key routes and deter sabotage. In parallel, United States and EU navies have begun to experiment with Distributed Acoustic Sensing (DAS) on fibre optic submarine cables, turning dark fibres (unused fibre strands within a fibre-optic cable) into wide area underwater sensing systems that can detect anomalies in real time (Boschetti & Falco, 2025). These efforts do not physically guard every cable and may face diminishing returns in heavily patrolled areas, but they raise the perceived probability of detection, create a recognisable pattern of maritime presence, and embed critical infrastructure protection in daily operations (Boschetti & Falco, 2025).

Vessel behaviour monitoring and administrative consequence rely on maritime presence, suspicious-vessel tracking, and legal or administrative levers below the threshold of criminal proof. NATO set up Commander Task Force Baltic, based in Rostock, to coordinate maritime monitoring and presence in the Baltic Sea with a focus on shadow fleets and undersea installations (NATO, 2024). The United Kingdom-led Nordic Warden initiative reinforces this posture in the northern North Sea and Norwegian approaches operating as a Joint Expeditionary Force (JEF). Nordic Warden uses an AI-enabled reaction system to fuse satellite and AIS (Automatic Identification System) data to track suspicious vessels and threats to critical undersea infrastructure. This illustrates how a minilateral coalition can plug specialised hybrid tools into a wider NATO posture (UK Ministry of Defence, 2025; NATO, 2025; Borger, 2025). Some countries, such as Germany, have also pursued bilateral and G7 initiatives, including the 2025 G7 Declaration on Maritime Security and Prosperity (Group of Seven, 2025; Pancevski, 2025).

Industry and repair coordination treat repair capacity and operator coordination as operational and industrial problems as well as security issues. At the policy

level, the European Commission and the High Representative have adopted Joint Communications on strengthening the security and resilience of undersea cables, often described as an EU cable security action plan (European Commission & High Representative, 2024, 2025). This plan establishes a resilience cycle approach of prevention, detection, response and recovery, and deterrence, and commits the EU and member states to mapping critical cables and landing sites. It also commits to integrated risk assessments, strengthening security and redundancy requirements for new cable projects, improving cross border information sharing with operators, and exploring reserve repair capacity and streamlined repair arrangements, including measures targeting shadow fleets and flags of convenience (Virkkunen, 2025; Girardi & Tan, 2025). Globally, the International Advisory Body for Submarine Cable Resilience, created by the International Telecommunication Union in partnership with the International Cable Protection Committee, brings together governments, operators, and technical experts to promote good practice on cable protection zones, repair processes, data sharing, and resilience standards (International Telecommunication Union (ITU) & International Cable Protection Committee, 2024). NATO has also supported the Hybrid Space and Submarine Architecture to Ensure Information Security of Telecommunications (HEIST) concept. HEIST envisages hybrid networks that combine undersea cables, fibre-based monitoring tools, and satellite links, allowing early detection of disruption and rapid rerouting of priority traffic through space-based capacity if key transoceanic cables are cut (Boschetti & Falco, 2025; NATO, 2025).

Societal signalling and information planning make these measures visible and legible to publics, operators, and partners. Recent European policy assessment argues that this agenda will only be effective if it is embedded in a broader strategy that links cable security and resilience to industrial competitiveness, diversified supply chains, and long-term investment, rather than treating it as a narrow security challenge (Folkman, Chihaia, & Hernandez, 2025). In this sense, Europe's evolving response combines operational initiatives, legal experimentation, industry coordination, and broader public framing of cable security and resilience in ways that amount to an emerging signalling posture under uncertainty.

3.3 Which Building Blocks Travel

Taken together, these initiatives show Europe assembling a signalling posture across four linked functions: integrated detection and staged attribution; vessel behaviour monitoring and administrative consequence; industry and repair coordination; and societal signalling and information planning. Each of these functions is now visible in practice, even if unevenly.

Integrated detection and staged attribution are visible in NATO fusion cells, maritime presence, and real-time sensing experiments. Vessel behaviour monitoring and administrative consequence appear in shadow fleet scrutiny, AIS-based tracking, and measures directed at flags of convenience. Industry and repair coordination appear in EU mapping, reserve repair planning, ITU–industry standards, and hybrid cable-satellite resilience concepts. Societal signalling and information planning appear in EU Joint Communications and the broader effort to make cable security legible to publics, operators, and partners. Alliances, regional organisations, regulators, and operators are sending mutually reinforcing signals (Girardi & Tan, 2025). Even without perfect protection or instant attribution, their combined effect is to make ambiguous incidents less useable as sources of leverage. For example, responses to Nord Stream and the Balticconnector were sometimes slow and fragmented. Their public messaging was cautious and at times inconsistent across national and EU levels, and debates over attribution and escalation produced delays (Reuters, 2023; International Institute for Strategic Studies, 2024). Nevertheless, repeated ambiguous attacks and improvised NATO–EU responses reveal how a signalling posture and its supporting governance arrangements are being assembled in real time, though still unevenly and with persistent gaps and frictions.

From a diffusion perspective, some of these building block practices may travel to Canada, including staged attribution logics, evidence categories, vessel behaviour monitoring, and early repair planning work. Others require adaptation, including EU legal templates to Canadian and Indigenous frameworks and monitoring concepts to long Arctic approaches. Some do not travel at all since Canada cannot replicate the Baltic's dense institutional ecosystem or its patrol density. The Baltic story, in other words, shows how alliances begin to govern ambiguity under conditions of uncertainty rather than eliminate it.

In sum, the Baltic Sea offers a useful learning environment because repeated ambiguous incidents have exposed visible governance gaps and prompted the partial assembly of a signalling posture across integrated detection and staged

attribution, vessel behaviour monitoring and administrative consequence, industry and repair coordination, and societal signalling and information planning. That posture remains uneven and contested, but it is precisely this combination of recurring incidents, incomplete attribution, and adaptive response that makes the region useful for Canada without making it a template.

4 Canada's Arctic and North Pacific Exposure, Risk Patterns, and Governance Gaps

Canada's Arctic and North Pacific approaches face similar hybrid risk, governance friction, and signalling demands as the Baltic Sea, but under vastly different structural conditions. They combine emerging high-value infrastructure with a sparse monitoring and governance environment, thin redundancy, and strong Northern and Indigenous governance. This sharply tests whether building block practices from the Baltic Sea can apply. This section examines Canada's pattern of risk and governance gaps through the same four categories used in section 3 to analyse Europe's emerging signalling posture and in section 5 to design a Canadian posture: integrated detection and staged attribution; vessel behaviour monitoring and administrative consequence; industry and repair coordination; and societal signalling and information planning.

4.1 Integrated Detection and Staged Attribution

Integrated detection and staged attribution are most difficult where Canada's approaches are largest, sparsest, and least persistently observed. Canada spans three maritime approaches, but the Arctic and North Pacific present the most difficult monitoring and response conditions. Where the Baltic Sea illustrates network signalling under uncertainty in an institutionally dense environment, Canada's Arctic and North Pacific approaches operate in a sparse setting with emerging infrastructure, real outages and occasional probes, and much thinner governance, monitoring, and response capacity.

Domestic debates in Canada reflect both unease and renewed attention. Commentators warn that Canada risks being caught unprepared in an Arctic crisis and highlight tensions between long term capability investments and near-term hybrid risks (Rigby & Sands, 2023; Huebert, 2022). The 2024 defence policy update Our North, Strong and Free commits substantial new spending with a strong focus on Northern monitoring, NORAD modernisation, and all domain

awareness (Department of National Defence, 2024). At the same time, reporting on potential cuts or reallocations in intelligence and analytical capacity has raised concerns that key functions for attribution and coordination could still be constrained (The Hill Times, 2026). Canada's security and intelligence community has been explicit that state and non-state actors increasingly target critical infrastructure and exploit interference below the threshold of war (Canadian Security Intelligence Service (CSIS), 2025). While not every cable break is sabotage, the operating environment now includes more probing and attempts to create strategic effect without escalation. Yet Canada does not yet have dedicated undersea monitoring systems or routine patrol patterns that focus specifically on seabed infrastructure in its Exclusive Economic Zone. The Auditor General has warned that maritime domain awareness in the Arctic remains incomplete (Office of the Auditor General of Canada, 2022).

Canada's strategic context also includes alliance dynamics. NATO has become more relevant to Arctic security because all Arctic states except Russia are now members, which creates potential to extend Euro-Atlantic resilience practices northward. At the same time, Arctic operations are shaped by sovereignty sensitivities and legal debates over internal waters and access, so any Canadian signalling posture must plug into alliance structures without compromising domestic legal positions on Arctic waters (Byers, 2013; Charron & Fergusson, 2018).

4.2 Vessel Behaviour Monitoring and Administrative Consequence: Legal, Administrative, and Ownership Constraints

Vessel behaviour monitoring and administrative consequence are constrained by the scale of Canadian approaches, rising great power activity, and an unevenly developed legal and administrative toolkit. Here, administrative consequence means measures such as inspections, reporting obligations, port-access conditions, safety restrictions, and other regulatory actions that can be imposed on suspicious vessels even when criminal proof is unavailable. Similar to Europe, Canada's challenge is increasingly shaped by great power competition layered on top of environmental and commercial change. Analysts have observed deepening Sino-Russian coordination in Arctic affairs and military activity across the wider North-Pacific (Huebert, 2019; Klimenko, 2019). Reporting points to expanded Chinese and Russian naval, coast guard, and research vessel operations near North American approaches, including in and around the Bering

Sea (Fraser, 2023). Reconnaissance of seabed topography, acoustic conditions, and cable approaches is a plausible extension of such activity, even if specific intentions are often opaque (Giles, 2024; Kim et al., 2025). Studies of Sino-Russian cooperation in Arctic resource and shipping projects note that these ventures create dual use opportunities to survey seabed corridors and experiment with infrastructure that could later support pressure on Western connectivity (Landauer, Swanström, & Goodsite, 2025).

There is also evidence that other states are interested in Canada's undersea approaches. In 2022, the Canadian Armed Forces discovered and retrieved several Chinese monitoring buoys deployed in Arctic waters, reportedly tracking submarine activity and oceanographic data under the polar ice. They were detected and removed as part of Operation LIMPID, Canada's routine monitoring of its air and maritime domains (Chase, 2023; Fraser, 2023). Their presence does not prove an imminent campaign against cables. However, it does confirm Beijing's strategic interest in the Arctic seafloor and illustrates the operational challenges of persistent monitoring across vast Northern approaches. Combined with alleged Russian involvement in Baltic and North Sea infrastructure incidents and Chinese linked cable disruptions around Taiwan, these developments suggest that if governance and monitoring gaps persist, Arctic and North Pacific routes could be subject to pressure in the future (International Institute for Strategic Studies, 2024; Tseng, 2023; Focus Taiwan, 2025).

Even when suspicious activity is detected, Canada faces legal, administrative, and ownership constraints that weaken vessel behaviour monitoring, administrative consequence, and broader signalling coherence. Beyond the territorial sea, Canada does not yet appear to have a cleanly articulated enforcement toolkit for deliberate cable interference. Ottawa depends heavily on privately owned systems, including the Topaz trans-Pacific cable and privately operated Arctic and Northern links (Google Cloud, 2022; Dalziel, 2024). In practice, this means that suspicious vessel behaviour may be visible without producing a clear or timely path to consequence.

When cable disruption occurs, Canadian action depends on coordination and rapid information sharing between federal and territorial governments, industry operators, and local communities, including Indigenous leadership (Middleton, Bratt, & Lackenbauer, 2020). Yet there is no single focal point for network signalling under uncertainty. Responsibility is spread across departments and

levels of government, and exercises remain limited. This fragmentation undermines Canada's ability to mount coherent network signalling, because signals are weaker, slower, and more easily misinterpreted if authorities are not aligned.

4.3 Industry and Repair Coordination: Repair, Redundancy, and Operator Dependence

Industry and repair coordination are shaped by climate, distance, the expansion of northern connectivity infrastructure, and the thin redundancy of northern and trans-Pacific systems. Climate change is opening waters that ice once covered at the same time as new connectivity projects place high-value infrastructure in remote areas with limited redundancy and slow repair options (AMAP, 2017; Intergovernmental Panel on Climate Change, 2019; Kivalliq Inuit Association, 2020; Dalziel, 2024; Kim et al., 2025).

Canada is entering a new phase of Arctic connectivity. Regional projects such as the Kivalliq Hydro Fibre Link and proposed trans-Arctic systems such as Far North Fiber and SednaLink, are designed to link Northern communities and route traffic between Europe, Asia, and North America through Arctic and sub-Arctic waters (Kivalliq Inuit Association, 2020; Dalziel, 2024; Kim et al., 2025). On the Pacific side, Canada's only direct trans-Pacific subsea cable, Topaz, links British Columbia to Japan and is privately owned and operated by Google Cloud (Google Cloud, 2022). These systems reflect strategic connectivity ambitions but also enlarge the potential hazard and attack surface in regions where outages can isolate communities, disrupt governance, and complicate emergency response (TeleGeography, 2023; Kim et al., 2025).

Recent incidents in Atlantic Canada, the North, and neighbouring Alaska show why this matters even when no hostile actor is involved. Accidental and deliberate cuts to undersea and terrestrial systems have left communities without internet or mobile service for days or weeks, with limited redundancy and slow repair, which turns single points of failure into governance problems (Cecco, 2023; Northwestel, 2023; Cabin Radio, 2024; Walker, Simmons, & Irwin, 2019; Casper, 2025; CityNews Halifax, 2025). Storms, ice, fires, and human interference expose the same weaknesses in infrastructure and repair posture.

Digital dependence amplifies these vulnerabilities. As defence and public services become more data-intensive and experiment with AI-enabled systems, loss of connectivity becomes a compounding risk that can degrade decision support, logistics, and the ability to coordinate responses across distance (Department of National Defence, 2023). Climate change and infrastructure expansion are not separate issues. Warming seas, new cables, and limited redundancy interact in ways that concentrate risk in places that are hard to monitor and repair. Visible investments in redundancy, backup communications including satellite options, and climate robust systems therefore signal that disruptions, whether accidental or hostile, are unlikely to create lasting leverage. Underinvestment advertises exploitable weaknesses. From a network signalling perspective, accidents and natural hazards are part of the same governance test as deliberate interference, because they reveal whether Canada can detect, repair, and communicate around undersea incidents in ways that sustain public trust and deny leverage.

This governance challenge is amplified by defence and public administration's growing reliance on digital and AI-enabled systems. Canada's Defence Artificial Intelligence Strategy frames AI adoption as foundational to future operational effectiveness and assumes secure, high-volume connectivity to support data-intensive decision support and command and control (Department of National Defence, 2023). As defence and public services become more data-intensive, cable disruption becomes not only an economic risk but also a systems risk for emergency response, governance continuity, and crisis management, especially in northern regions where redundancy is thin and climate change is increasing both environmental stress and activity levels (AMAP, 2017; Intergovernmental Panel on Climate Change, 2019).

4.4 Societal Signalling and Information Planning: Northern and Indigenous/Community Resilience and the Information Environment

Societal signalling and information planning are central to Canada's signalling posture because undersea disruption in the North will be experienced first as a community, governance and communication problem. Indigenous governance and whole-of-society resilience are structurally central in this context (Government of Canada, 2019; Lackenbauer & Lajeunesse, 2018) and resilience governance in Northern Canada is inherently whole-of-society. Federal departments, the Canadian Armed Forces, and the Coast Guard are central, but

they do not own most of the infrastructure at risk or provide the first line of response. Northern municipalities, Inuit, First Nations, and Métis governments and organisations, regional service providers, and private cable and telecom operators collectively determine whether remote communities can maintain basic connectivity, emergency services, and public trust during an incident (Government of Canada, 2019; Middleton et al., 2020).

Canada's Arctic and Northern Policy Framework already recognises this reality by foregrounding Indigenous rights, self-determination, and partnership (Government of Canada, 2019). The United Nations Declaration on the Rights of Indigenous Peoples Act and the Inuit Nunangat Policy further commit Ottawa to co-developing approaches with Indigenous governments and organisations on issues that include infrastructure and security (Government of Canada, 2021; Government of Canada, 2022). For cable security, this has concrete implications. Indigenous and local authorities have detailed knowledge of environmental conditions, vessel patterns, and community vulnerabilities. They are often the first to notice anomalies in connectivity or maritime activity and are among the most credible voices for local populations during crisis communication (Rodon, 2014; Clark & Joe Strack, 2017). When that knowledge is fed into national attribution and response processes, it shortens decision cycles and improves situational awareness under uncertainty.

Community-level preparedness and civilian infrastructure are equally important. Northern communities routinely track weather, ice, and traffic for hunting, travel, and safety reasons that long predate current security debates. Structured mechanisms that channel these observations into federal and allied reporting systems, for example unusual vessel behaviour near landing sites, unexplained changes in signal quality, or visible damage to coastal infrastructure, can raise detection probability and provide contextual evidence for staged attribution (Arctic Council, 2015; ICC (Inuit Circumpolar Council), 2016). Local radio, community broadband networks, and small satellite links give functional redundancy and channels for authoritative information when primary connectivity fails (Middleton et al., 2020). If a major cable goes down, the ability of local actors to switch to backup communications, prioritise essential services, and communicate clearly with residents will decide whether disruption remains a manageable inconvenience or becomes a governance crisis.

These Northern and Indigenous roles are part of network signalling under uncertainty. They form the societal layer of the signalling posture described earlier. For an adversary, the question is whether a cable break will isolate communities, cause visible governance failures, or erode trust. For hazards and accidents, the question is whether disruption cascades into broader crises. Visible investments in community level redundancy, Indigenous-led monitoring, and local crisis communication signal that Northern communities are not easy targets for coercion or prolonged disruption. At the same time, these roles need resources, clear mandates, and co-designed procedures that respect Indigenous data governance and local priorities, including the principle that participation in national security related processes must be negotiated rather than presumed (Rainie, Rodriguez Lonebear, & Martinez, 2017). Without that support, Northern and Indigenous actors remain central to network signalling under uncertainty but poorly integrated into Canada's overall network signalling posture. The next section therefore asks how building block practices drawn from the Baltic Sea and related Euro-Atlantic experience could be adapted to close Canada's governance gaps.

5. From Baltic Sea Lessons to a Canadian Network Signalling Posture on Cable Security

The Baltic Sea experience suggests a set of building block practices that can be adapted to Canada's Arctic and North Pacific context. The preceding section showed how repeated ambiguous incidents pushed European actors toward integrated detection and staged attribution, vessel behaviour monitoring and administrative tools, closer coordination with operators and repair chains, and more deliberate signalling to publics and partners (International Institute for Strategic Studies, 2024; Edwards & Seidenstein, 2025; European Commission & High Representative, 2024, 2025; Girardi & Tan, 2025). Building on those four clusters, this section identifies the elements of a Canadian signalling posture. The first four subsections follow the same categories, the fifth extends them internationally, and the sixth considers trade-offs, costs, and near-term priorities.

5.1 Integrated detection and staged attribution

European practice centres on shared situational awareness and structured escalation. In the Baltic Sea, NATO's Critical Undersea Infrastructure Coordination Cell and the EU cable action plan move away from ad hoc incident

handling towards common pictures and pre-planned ladders (NATO, 2023c; European Commission & High Representative, 2024, 2025). A Canadian posture could adapt this by defining clear stages from anomaly to high confidence attribution, linked to specific authorities and options, and by combining technical, behavioural, contextual, and legal evidence in a structured way.

Routinised operator reporting, engagement with Northern and Indigenous authorities who may observe relevant anomalies, and arrangements with allies to share pattern of life data would feed these stages (Palmertz et al., 2025; CSIS, 2025). Shared confidence terminology and communication playbooks would help ensure that even ambiguous incidents generate structured analysis and coordinated responses rather than one off reactions. This would make it more likely that ambiguity is governed rather than simply endured.

A Canadian posture would also need to integrate satellite sensing, information sharing across agencies and allies, and staged incident management into an Arctic scale all domain awareness strategy, so that technical, behavioural, contextual, and legal evidence can move quickly between operators, departments, and communities (Office of the Auditor General of Canada, 2022; Department of National Defence, 2023, 2024; Palmertz et al., 2025).

5.2 Vessel behaviour monitoring and administrative consequence

Baltic practice also highlights the value of maritime pattern of life monitoring and administrative levers. NATO presence missions, national tracking of shadow fleets, and EU proposals on flags of convenience all point to an approach in which suspicious behaviour triggers scrutiny and restrictions even without a viable criminal case (Edwards & Seidenstein, 2025; Virkkunen, 2025; Reuters, 2023). Canada could extend its dark vessel detection experience to cable-relevant areas near landing sites and planned Arctic routes, treating vessel tracks, anchoring patterns, and behaviour in cable protection zones as inputs for safety and security (Standing Committee on Fisheries and Oceans, 2023).

Administrative tools might range from inspections and port access conditions to heightened reporting requirements and coordination with insurers or classification societies. Taiwan's tightening of rules on anchoring, AIS use, and penalties for negligent damage offers a model that combines safety and deterrence (Tseng, 2023; Focus Taiwan, 2025). Maritime safety rules and

administrative measures can therefore raise the cost of suspicious behaviour even when courtroom-level proof is unavailable. As Asia Pacific Foundation of Canada analysis stresses, however, legal and monitoring tools must also work together if states want to raise the cost of suspicious behaviour without courtroom grade proof in every case (Kim et al., 2025).

For Canada, this line of effort would also require legal signalling. That would include modernising legislation for the Exclusive Economic Zone and key infrastructure, clarifying offences and investigative powers, setting higher penalties for deliberate damage, and defining authorities for inspection and interdiction. It would borrow where useful from Taiwanese experience on anchoring rules and AIS obligations in sensitive areas (NOAA Office of General Counsel, 2020; Sari, 2025; Tseng, 2023; Focus Taiwan, 2025; U.S. Department of Homeland Security, 2024). In network-signalling terms, this shows that Canada should not treat incidents in sensitive areas as unimportant background noise.

5.3 Industry and repair coordination as strategic assets

The Baltic experience and EU planning treat repair capacity and operator coordination as core resilience issues. They track repair assets, contract arrangements, and response timelines (European Commission & High Representative, 2024, 2025; Girardi & Tan, 2025). However, studies show that only a small number of specialised repair ships serve hundreds of cables and that it is far easier to damage a cable than to repair it (Kim et al., 2025; U.S. Department of Homeland Security, 2024).

For Canada, which relies on privately owned systems and has no repair vessels dedicated to the Arctic, repair should be treated as a strategic asset. A standing undersea infrastructure resilience forum could bring together operators, repair firms, regulators, security agencies, Indigenous and territorial representatives, and relevant federal departments. It could map repair capacity, agree to incident reporting and evidence preservation protocols, and clarify repair priorities in multi-incident scenarios. Integrating community level redundancy planning with these national repair strategies would shorten decision cycles and signal that disruption is likely to be brief and managed rather than an enduring source of leverage.

Experiments with satellite backup for remote communities and hybrid cable-satellite concepts would gradually combine cable and satellite resilience. Experimental hybrid architectures such as HEIST, which combine cable-based monitoring with satellite backup and automated rerouting of priority traffic, suggest that over time cables and satellites should be planned as complementary layers rather than alternatives (Boschetti & Falco, 2025; Kim et al., 2025).

5.4 Societal signalling and information planning

Baltic Sea experience also shows how legal reforms, operational posture, and public communication interact. EU law proposals, national changes to criminal and administrative offences, and visible NATO patrols have been accompanied by cautious but deliberate messaging about attribution and thresholds (International Institute for Strategic Studies, 2024; Edwards & Seidenstein, 2025). For Canada, societal signalling could formalise roles for Indigenous governments, Northern municipalities, and community organisations in early warning, incident reporting, redundancy planning, and crisis communication, which would make visible the Northern and Indigenous resilience capacities described in the previous section and reduce the scope for disinformation (Government of Canada, 2019; Middleton et al., 2020). Undersea incidents often generate competing narratives and deliberate misinformation. Disruption or manipulation of data flows can directly affect democratic resilience and public debate (Nadarajah, 2025). Clear internal maps of information flow across agencies, operators, and communities, pre-bunked lines for likely narratives, and joint communications drills involving federal, territorial, Indigenous, and allied interlocutors would support credible messaging.

Distinguishing operational attribution, used to protect and repair, from public attribution, used to signal and sanction is important. Rehearsing that distinction in exercises would be central to network signalling under uncertainty (CSIS, 2025; Edwards & Seidenstein, 2025). In this sense, societal signalling and information planning are not add-ons to a Canadian posture. They are part of how that posture would become visible and credible to communities, partners, and adversaries alike.

5.5 International extension: bridge partnerships with Japan and the Republic of Korea

Selective partnerships with Japan and the Republic of Korea can extend a Canadian signalling posture beyond domestic waters. NATO–EU complementarity and engagement with partners form an international layer of network signalling under uncertainty. Canada cannot build a credible signalling posture on cable security on a purely national basis because the cables it relies on cross the Arctic and the North Pacific. Many are privately owned, and key systems that matter for Canadian resilience are operated by United States and other foreign firms (Google Cloud, 2022; Dalziel, 2024; Kim et al., 2025). Strategic autonomy therefore depends not only on domestic governance, but also on how Canada embeds itself in wider governance and repair networks. European formats such as the Joint Expeditionary Force, which has built Nordic Warden as a standing response option for threats to cables and pipelines in Northern European waters, underline the value of flexible coalitions that sit between national assets and NATO's collective posture (UK Ministry of Defence, 2025).

Existing frameworks provide useful reference points. On the Euro-Atlantic side, EU–Canada digital and security partnerships highlight cooperation on secure connectivity and hybrid threats (European Commission & Government of Canada, 2023, 2024). On the Indo-Pacific side, EU–Japan and EU–Republic of Korea partnerships make secure undersea cables and hybrid resilience explicit priorities (European Commission & Government of Japan, 2023; European Union & Republic of Korea, 2023). NATO has institutionalised relationships with Japan and the Republic of Korea through Individually Tailored Partnership Programmes that stress resilience and emerging technologies, while Canada has deepened its own security cooperation with both states and adopted an Indo-Pacific Strategy (NATO, 2023a, 2023b; Global Affairs Canada, 2016, 2022, 2023). These political frameworks sit alongside practical efforts to harden undersea infrastructure, including NATO's deployment of underwater drones and situational awareness tools, the 2025 G7 Declaration on Maritime Security and Prosperity, and United States Department of Homeland Security analysis highlighting the limited size and vulnerability of the global cable repair fleet (Group of Seven, 2025; NATO, 2025; Pancevski, 2025; U.S. Department of Homeland Security, 2024; European Commission & High Representative, 2024, 2025; Girardi & Tan, 2025; Boschetti & Falco, 2025).

European experience suggests focusing on specific deliverables rather than new grand architectures. For Canada, Japan, and the Republic of Korea, a practical international extension of a Canadian signalling posture could begin with three

elements. A North Pacific and Arctic cable security and resilience working group at senior official level would share threat indicators and suspicious vessel patterns. It would also develop common language for hybrid incidents and attribution confidence levels and agree basic routines for exchanging declassified evidence packages that can support joint public messaging. Joint tabletop and field exercises involving cable operators, repair firms, and governments would test responses to scenarios that combine ambiguous cable incidents, natural hazards, and disinformation surges, and would produce shared playbooks for who speaks when evidence is partial, but patterns are strong (Girardi & Tan, 2025). Mutual support for repair and trusted corridor governance would cover regulatory fast tracking, port access, and security escorts for repair ships in higher risk or remote areas. Joint work on basic standards for trusted cable corridors in the North Pacific and Arctic space would build on EU–Japan work on secure connectivity but adapt it to Canadian waters and North American approaches (Kim et al., 2025; European Commission & Government of Japan, 2023). Recent proposals for a Canada–Japan–Korea trilateral framework on Arctic defence and critical minerals show that all three governments already see this triangle as a venue for managing strategic infrastructure risks, which strengthens the case for cooperation explicitly focused on cables (Asia Pacific Foundation of Canada, 2025).

These steps would extend Canada's signalling posture, grounded in network signalling under uncertainty, beyond the North Atlantic into the wider Arctic and North Pacific continuum and support its strategic autonomy. By diversifying partners, shaping norms, and improving visibility over cables operated by foreign firms, Ottawa could reduce the risk of accidents, natural hazards, or adversarial probes translating into long-lasting dependence or leverage. Closer alignment with emerging European and North American standards on secure connectivity and hybrid resilience would also reduce fragmentation across theatres and make Canadian signals more legible to both adversaries and partners (European Commission & High Representative, 2024, 2025; Group of Seven, 2025).

5.6 Trade-offs, costs, and three near-term priorities

Any Canadian signalling posture on cable security will face hard trade-offs. Intrusive monitoring and data fusion can raise concerns about privacy, commercial confidentiality, and overreach. Stronger regulatory and legal tools may meet resistance from operators worried about cost, liability, or competitive

disadvantage. Over-interpreting patterns risks threat inflation, distorted priorities, damaged credibility, and unwanted escalation if ambiguous incidents are framed too quickly as deliberate attacks (Nye, 2017; Giles, 2024). Deeper integration of Indigenous and community observations into national attribution processes must respect Indigenous rights, self determination, and evolving frameworks for Indigenous data governance (Rainie et al., 2017). Effective public signalling depends on declassifying some evidence without compromising sensitive sources and methods. Resources for seabed sensors, monitoring assets, analytic capacity, community redundancy, and international partnerships will compete with other defence and public spending priorities (Standing Senate Committee on National Security, Defence and Veterans Affairs, 2022; Department of National Defence, 2024).

Cost is a central constraint. Cable repair operations are expensive and slow, and the global repair fleet is limited (Kim et al., 2025; U.S. Department of Homeland Security, 2024). Many signalling measures, from additional sensors to exercises and new coordination mechanisms, require sustained funding. There is a risk of diminishing returns if Canada tries to do everything at once. The deterrent value of each extra measure will fail if repair readiness, redundancy, and governance are not in place. Satellite systems are a promising complement for basic connectivity in remote communities, but they cannot yet replace subsea fibre for high-capacity traffic (Boschetti & Falco, 2025).

Whole-of-government resilience is therefore partly about managing these trade-offs transparently. Measures that are seen as legitimate and procedurally fair are more likely to be sustainable and to command the trust of operators, communities, and allies. A credible signalling posture on cable security also depends on treating intelligence assessment capacity as critical infrastructure. Without robust, all-source analytical capability, there can be no pattern recognition, timely attribution, or coherent public narrative (CSIS, 2025; Palmertz et al., 2025).

Given political and fiscal realities, not all elements of a comprehensive posture can be built at once. In the next two to three years, three reforms stand out as both analytically desirable and politically plausible. They also line up with Baltic and Asia Pacific lessons. First, Canada could designate a clear federal lead and create an interdepartmental cell for undersea infrastructure to coordinate incidents, consult with operators, and integrate Northern and Indigenous inputs, drawing

on Baltic examples of central coordination hubs while adapting them to Canadian federal and Indigenous governance (Dalziel, 2024; Government of Canada, 2019). Second, it could pilot an undersea incident staged attribution and communications protocol, with joint exercises that test evidence sharing and public messaging under uncertainty and link the ADAC style ladder to real Canadian actors and legal constraints (Palmertz et al., 2025; Edwards & Seidenstein, 2025). Third, it could extend dark vessel detection and maritime domain awareness tools to cable critical areas and update the legal toolkit around them, aligning Canadian practice with Baltic and Indo Pacific moves on vessel monitoring and administrative measures while clarifying investigative powers and penalties in defined zones around key infrastructure (Standing Committee on Fisheries and Oceans, 2023; NOAA Office of General Counsel, 2020; Kim et al., 2025).

These steps on their own would not create a full posture, but they would move Canada from incident-by-incident reactions toward a more deliberate network signalling posture under uncertainty, grounded in the realities of its geography, alliances, and resource constraints.

6. Conclusion

Undersea cables expose a strategic paradox. They are generally privately financed and operated, routinely disrupted by accidents and natural hazards, and increasingly implicated in hybrid competition. Yet they underpin economic activity, public administration, and defence. This paper asked how Canada can build a credible signalling posture on cable security in its Arctic and North Pacific approaches, and what lessons from the Baltic Sea and adjacent North Sea can travel into that environment. Its answer is that Canada should treat cable security as a problem of resilience governance under uncertainty and build a signalling posture that reduces the leverage created by ambiguous incidents even when attribution remains probabilistic.

The Baltic comparison shows that some building block practices do travel. These include integrated detection and staged attribution, vessel behaviour monitoring and administrative consequence, industry and repair coordination, and societal signalling and information planning. They do not travel as a complete institutional model. Rather, they travel selectively, and only under conditions in which threat perceptions converge, institutional linkages exist, and the practices

can be adapted to Canadian geography, sparse monitoring, and Indigenous and federal governance rather than copied from a denser Baltic environment. Patrol density, legal templates, and alliance routines cannot simply be transplanted.

For Canada, the resulting posture has four linked elements. First, integrated detection and staged attribution can connect operator reporting, community observations, intelligence, and allied information into a more disciplined escalation ladder. Second, vessel behaviour monitoring and administrative consequence can raise the cost of suspicious conduct in sensitive areas without requiring criminal proof in every case. Third, industry and repair coordination must be treated as strategic assets, because redundancy, repair readiness, and backup communications determine whether disruption becomes leverage. Fourth, societal signalling and information planning can make Northern and Indigenous resilience visible through crisis communication, redundancy, and locally grounded early warning. In this framework, Indigenous and community actors are not simply recipients of protection, but part of the posture itself.

The analysis also suggests that Canada's international strategy should be selective and practical. Bridge partnerships with NATO, the European Union, Japan, and the Republic of Korea can extend Canada's posture outward through exercises, evidence-sharing routines, repair cooperation, and trusted corridor governance. But such partnerships supplement rather than substitute for domestic monitoring, legal tools, repair planning, and community resilience. The goal is not to militarise every outage, but to ensure that Canada is neither isolated in crisis nor over-dependent on decisions taken elsewhere.

The broader implication is that cable security is not only a technical protection problem. It is a governance problem in which public and private actors must coordinate, decide, and communicate under conditions of uncertainty. Undersea cables are one especially revealing case, but similar problems are likely to arise in other critical infrastructure sectors and grey-zone environments where assets are dispersed, privately operated, and politically consequential. The paper's contribution is therefore not to claim a single transferable model, but to show how building block practices can be recombined into a credible signalling posture that reduces coercive advantage under ambiguity and probabilistic attribution.

Because the analysis is theory-building and document-based, its claims are about plausible posture design and policy transfer rather than measured deterrent

effects. Even so, the comparison points to a practical near-term agenda for Canada. Ottawa could designate a federal lead for undersea incidents, pilot a staged attribution and communications protocol, improve monitoring and administrative tools around cable-critical areas, strengthen repair and redundancy planning, and embed Indigenous and community actors as core partners in the posture. If Canada treats the North Atlantic, Arctic, and North Pacific as a connected continuum of undersea risk, it will not eliminate disruption. It can, however, make both accidents and hostile interference less useful as sources of leverage.

References

Adomaitis, N., & Ahlander, J. (2025, August 21). What is known about the Nord Stream gas pipeline explosions? *Reuters*.

AMAP. (2017). *Snow, water, ice and permafrost in the Arctic (SWIPA) 2017*. Arctic Monitoring and Assessment Programme.

Arctic Council. (2015). *Arctic Marine Strategic Plan (AMSP) 2015–2025: Implementation plan*. Protection of the Arctic Marine Environment.

Asia Pacific Foundation of Canada. (2025). *A Canada–Japan–Korea trilateral framework for Arctic defence and critical minerals*. Asia Pacific Foundation of Canada.

Associated Press. (2025, January 28). At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard. *AP News*.

Bager, M., et al. (2023). *Hybrid threats: A comprehensive resilience ecosystem*. Publications Office of the European Union.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: The limits of crisis management in the new world of risk. *Journal of Contingencies and Crisis Management, 15*(1), 50–59.

Borger, J. (2025, January 19). Nato flotilla assembles off Estonia to protect undersea cables in Baltic Sea. *The Guardian*.

Börzel, T. A., & Risse, T. (Eds.). (2014). *From Europeanisation to diffusion*. Routledge.

Boschetti, A., & Falco, E. (2025). *Per aspera ad astra: Protecting submarine communications cables in the era of next generation satellites?* IEP@BU Policy Brief No. 52. Institute for European Studies, Boston University.

Braw, E. (2025, November 26). How the Baltic Sea nations have tackled suspicious cable cuts. *Atlantic Council*.

Brunner, E., & Suter, M. (2009). *International submarine cables and the oceans: Connecting the world*. UNEP–WCMC & International Cable Protection Committee.

Bueger, C., & Liebetrau, T. (2021). Security, infrastructure, and the sea: Critical infrastructure at sea as a new security problem. *European Journal of International Security, 6*(3), 339–358.

Burnett, D. R., Davenport, T., & Beckman, R. (2013). Overview of the international legal regime governing submarine cables. In D. R. Burnett, R. Beckman, & T. Davenport (Eds.), *Submarine cables: The handbook of law and policy* (pp. 61–90). Brill Nijhoff.

Byers, M. (2013). *International law and the Arctic*. Cambridge University Press.

Cabin Radio. (2024, January 16). What exactly was Northwestel dealing with? *Cabin Radio*.

Cabroni, G., & Gilli, A. (2026). *Per aspera ad astra: Undersea cables, satellites for telecommunications and the European strategic autonomy* (Policy Brief No. 52). IEP@BU – Institute for European Policymaking, Bocconi University.

Canadian Security Intelligence Service. (2025). *CSIS public report 2024*. Canadian Security Intelligence Service.

Casper, J. (2025, September 4). At last, Quintillion completes Arctic cable repair. *Broadband Breakfast*.

Cecco, L. (2023, June 10). Exhausted crews battle Canadian wildfires as experts issue climate warning. *The Guardian*.

Charron, A., & Fergusson, J. (2018). *NORAD: In perpetuity and beyond*. McGill–Queen's University Press.

Chase, S. (2023, February 21). Canadian military found Chinese monitoring buoys in the Arctic. *The Globe and Mail*.

CityNews Halifax. (2025, February 19). Bell says subsea cable from Cape Breton to Newfoundland was deliberately cut—twice. *CityNews Halifax*.

Clark, D., & Joe Strack, J. (2017). Keeping the "co" in the co management of Northern resources. *Northern Public Affairs, 5*(1), 71–74.

Dalziel, A. (2024). *Critical resilience: Russia, hybrid threats and subsea fibre optic cables in Canada's Arctic*. Macdonald–Laurier Institute.

Department of National Defence. (2023). *Canada's defence artificial intelligence strategy*. Government of Canada.

Department of National Defence. (2024). *Our North, Strong and Free: A renewed vision for Canada's defence*. Government of Canada.

Dunn Cavelty, M. (2018). Critical infrastructure in the digital age: Vulnerabilities, threats, and responses. In T. V. Paul, D. W. Larson, & H. W. Risse (Eds.), *The Oxford handbook of energy security* (pp. 427–444). Oxford University Press.

Edwards, C., & Seidenstein, N. (2025). *The scale of Russian sabotage operations against Europe's critical infrastructure*. International Institute for Strategic Studies.

European Commission, & Government of Canada. (2023). *EU–Canada digital partnership*. European Commission.

European Commission, & Government of Canada. (2024). *EU–Canada security and defence partnership*. European External Action Service.

European Commission, & Government of Japan. (2023). *EU–Japan digital partnership*. European Commission.

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2024). *Joint communication on a joint EU approach for strengthening the security and resilience of submarine cables*. European Commission.

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2025). *Joint communication to strengthen the security and resilience of submarine cables*. European Commission.

European Union, & Republic of Korea. (2023). *EU–Republic of Korea security and defence partnership*. European External Action Service.

Financial Times. (2026, January 5). Baltic countries on alert after series of suspicious undersea cable outages. *Financial Times*.

Focus Taiwan. (2025, December 9). Taiwan extends penalty range for damaging subsea cables, pipelines. *Focus Taiwan*.

Folkman, V., Chihaia, M. S., & Hernandez, I. (2025). *Beyond the action plan: Towards a holistic strategy for a competitive and secure subsea infrastructure in Europe*. European Policy Centre.

Fraser, D. (2023, February 22). Canadian military says it has tracked, stopped China surveillance in Arctic waters. *CBC News*.

Freedman, L. (2004). *Deterrence*. Polity Press.

Gartzke, E., & Lindsay, J. R. (Eds.). (2019). *Cross domain deterrence: Strategy in an era of complexity*. Oxford University Press.

Girardi, B., & Tan, S. (2025). *Response and resilience: Government strategies for securing subsea infrastructure in Europe and Asia (Key findings from expert workshop, Singapore, 30 October)*. The Hague Centre for Strategic Studies & RSIS.

Giles, K. (2024, May 1). Russian disruption in Europe points to patterns of future aggression. *Chatham House*.

Giles, K. (2025, April). *Risk of contagion: Will Russia's mayhem campaigns spread to US infrastructure?* Center for the Presidency and Congress.

Global Affairs Canada. (2016). *Canada–Japan joint declaration on political, peace and security cooperation*. Government of Canada.

Global Affairs Canada. (2022). *Canada's Indo Pacific strategy*. Government of Canada.

Global Affairs Canada. (2023). *Canada–Republic of Korea joint statement on cooperation in the Indo Pacific*. Government of Canada.

Google Cloud. (2022, April 6). Introducing Topaz—the first subsea cable to connect Canada and Asia. *Google Cloud*.

Government of Canada. (2019). *Canada's Arctic and Northern Policy Framework*. Government of Canada.

Government of Canada. (2021). *United Nations Declaration on the Rights of Indigenous Peoples Act, S.C. 2021, c. 14*. Government of Canada.

Government of Canada. (2022). *Inuit Nunangat policy*. Government of Canada.

Group of Seven. (2025, March 14). *G7 declaration on maritime security and prosperity*. Group of Seven.

Huebert, R. (2019). A new Cold War in the Arctic?! The old one never ended! *Arctic Yearbook*, 1–4.

Huebert, R. (2022). Health security, environmental security, and hard security in the Arctic: A complex relationship. *The Journal of Intelligence, Conflict and Warfare, 5*(1), 90–95.

ICC (Inuit Circumpolar Council). (2016). *Community based monitoring and Indigenous knowledge in a changing Arctic: A review for the Sustaining Arctic Observing Networks (Final report to SAON)*. Inuit Circumpolar Council.

International Cable Protection Committee. (2009). *Submarine cables and the oceans: Connecting the world*. International Cable Protection Committee & UNEP–WCMC.

International Institute for Strategic Studies. (2024). *The scale of Russian sabotage operations against Europe's critical infrastructure*. International Institute for Strategic Studies.

Intergovernmental Panel on Climate Change. (2019). *Special report on the ocean and cryosphere in a changing climate*. Author.

International Telecommunication Union, & International Cable Protection Committee. (2024). *International Advisory Body for Submarine Cable Resilience: Terms of reference and workplan*. International Telecommunication Union.

Kim, J., Kim, H., & Terasawa, M. (2025, May 16). The world's subsea cables are under threat. Can Canada help protect them? *Asia Pacific Foundation of Canada*.

Kivalliq Inuit Association. (2020). *Kivalliq hydro fibre link project*. Kivalliq Inuit Association.

Klimenko, E. (2019). The geopolitics of a changing Arctic. *SIPRI Background Paper*.

Lackenbauer, P. W., & Lajeunesse, A. (2018). *China's Arctic ambitions and what they mean for Canada*. University of Calgary Press.

Landauer, M., Swanström, N., & Goodsite, M. E. (2025). Mineral resources in the Arctic: Sino-Russian cooperation and the disruption of Western supply chains. In N. Swanström & F. B. Månsson (Eds.), *The "new" frontier: Sino-Russian cooperation in the Arctic and its geopolitical implications*. Institute for Security and Development Policy.

Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict*. U.S. Army War College Press.

Middleton, B., Bratt, D., & Lackenbauer, P. W. (2020). *Canada and the maritime Arctic: Boundaries, shelves, and waters*. North American and Arctic Defence and Security Network.

Nadarajah, H. (2025). *Democratic resilience and maritime security: Protecting undersea cables and digital infrastructure*. Asia Pacific Foundation of Canada.

NATO. (2022). *NATO 2022 strategic concept*. NATO.

NATO. (2023a). *Individually tailored partnership programme between NATO and Japan*. NATO.

NATO. (2023b). *Individually tailored partnership programme between NATO and the Republic of Korea*. NATO.

NATO. (2023c). *Critical Undersea Infrastructure Coordination Cell* [Fact sheet]. NATO.

NATO. (2024, October 22). *Commander Task Force Baltic Established*. Allied Maritime Command.

NATO. (2025, January 14). *NATO launches 'Baltic Sentry' to increase critical infrastructure security*. NATO.

NOAA Office of General Counsel. (2020). *Submarine cables and law of the sea: Legal framework and emerging issues*. National Oceanic and Atmospheric Administration.

Northwestel. (2023, August 8). Statement from Northwestel President Curtis Shaw on northern telecommunications during the current wildfires. *Northwestel*.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71.

Office of the Auditor General of Canada. (2022). *Report 4—Arctic waters: Canadian Coast Guard*. Office of the Auditor General of Canada.

Pancevski, B. (2025, January 27). Suspected sabotage of deep-sea cable triggers first NATO led response. *The Wall Street Journal*.

Palmertz, B., Isaksson, E., & Pamment, J. (2025, January 31). *A framework for attribution of information influence operations (Deliverable D1.2)*. ADAC.io / European Union Horizon Programme.

Rainie, S. C., Rodriguez Lonebear, D., & Martinez, A. (2017). Indigenous data sovereignty in the United States. *International Indigenous Policy Journal, 8*(2).

Reuters. (2023, October 19). NATO boosts Baltic patrols after undersea infrastructure damage. *Reuters*.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.

Rigby, V., & Sands, C. (2023, August 23). Arctic security awakening: A wake-up call for Canada? *Max Bell School of Public Policy, McGill University*.

Rodon, T. (2014). "Working together": The dynamics of multilevel governance in Nunavut. *Arctic Review on Law and Politics, 5*(2), 250–270.

Sari, A. (2025). *Protecting maritime infrastructure from hybrid threats: Legal options (Hybrid CoE Research Report No. 14)*. European Centre of Excellence for Countering Hybrid Threats.

Standing Committee on Fisheries and Oceans. (2023). *Dark vessel detection and maritime domain awareness*. House of Commons of Canada.

Standing Senate Committee on National Security, Defence and Veterans Affairs. (2022). *Arctic security, preparedness, and surveillance*. Senate of Canada.

Starosielski, N. (2015). *The undersea network*. Duke University Press.

Stone, D. (2012). Transfer and translation of policy. *Policy Studies, 33*(6), 483–499.

TeleGeography. (2023). Do submarine cables really carry 99% of international data traffic? *TeleGeography Blog*.

The Hill Times. (2026, February 4). Potential PCO intelligence cuts 'counterintuitive and risky,' say national security experts. *The Hill Times*.

Tseng, K. Y. (2023, March 1). Taiwan moves to increase penalties for damaging undersea internet cables. *Focus Taiwan*.

U.S. Department of Homeland Security. (2024). *Priorities for DHS engagement on subsea cable security & resilience*. U.S. Department of Homeland Security.

UK Ministry of Defence. (2025, January 6). Joint Expeditionary Force activates UK led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet. *UK Ministry of Defence*.

Virkkunen, H. (2025, January 20). EVP Virkkunen: Hybrid threats in the Baltic Sea [Speech]. *European Commission*.

Walker, W., Simmons, R., & Irwin, J. (2019). Communicating climate uncertainty in the Arctic: Risk, resilience, and infrastructure. *Polar Record, 55*, e23.

Acknowledgement

The author gratefully acknowledges the support of the Asia Pacific Foundation and thanks Hema Nadarajah, Erin Williams, and Mei Terasawa for their contributions to IS 402/880, Global Security Governance, whose Fall 2025 focus on hybrid conflict in the North Pacific and the High North helped shape the questions addressed in this paper. The author also acknowledges support from a Mobilizing Insights in Defence and Security (MINDS) Fellowship, which supported work at the NATO Defence College (NDC) in Spring 2025, including research on NATO and the Arctic with members of Senior Course Committee No. 2 and valuable discussions with colleagues in the research unit, especially Soojeong Choi, on cable security. The author is grateful as well to the anonymous referees for their thoughtful and constructive comments, which substantially improved the manuscript. All remaining errors are the author's own.

This work is licensed under a Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 International License.

© (NICOLE JACKSON, 2026)

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/