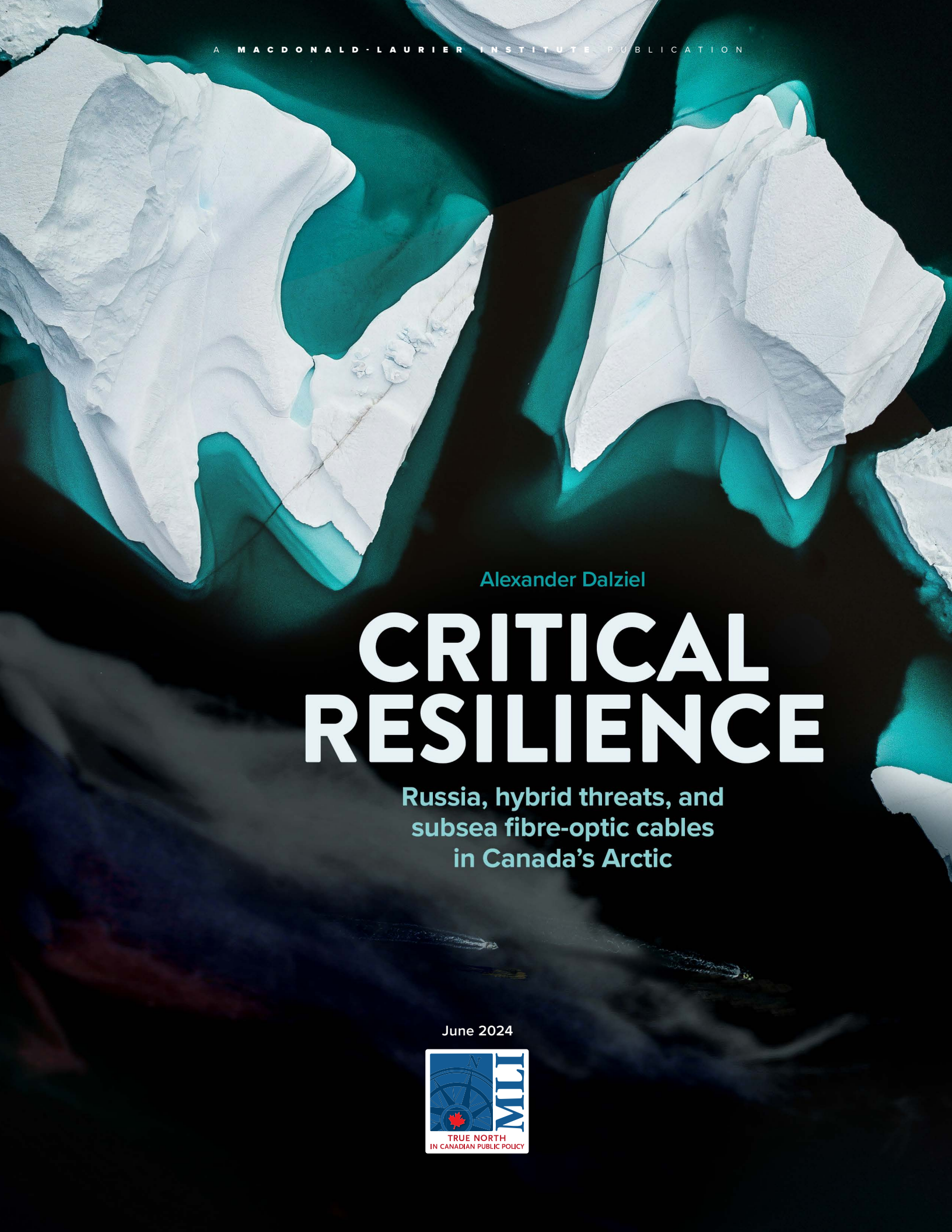

A MACDONALD-LAURIER INSTITUTE PUBLICATION

Alexander Dalziel

CRITICAL RESILIENCE

Russia, hybrid threats, and subsea fibre-optic cables in Canada's Arctic

June 2024

MLI
TRUE NORTH
IN CANADIAN PUBLIC POLICY

Contents

Cover design: Renée Depocas (photo: Annie Spratt)

Executive summary | *sommaire*

Neither governments nor the media have had very much to say to date about hybrid threats in the Canadian Arctic, especially about threats to critical infrastructure located there. There are several definitions of the term, but generally speaking, hybrid threats include a wide array of clandestine and deniable activities that are harmful and are carried out by civilians or states with the goal of undermining another state or an institution. In this paper the subject will be hybrid threats to submarine fibre-optic cables. The paper will attempt to shed more light on the challenges of keeping this critical infrastructure secure and the potential threats to it that may manifest over the next two decades. The paper's focus will be on hostile actions that attempt to covertly sabotage or interfere with the cables where the perpetrator does not want to be identified conclusively. As the paper indicates, it is important for countries to consider the threats, vulnerability, and risks their critical infrastructures face so that at the earliest stages possible they can build in resilience, which is the main deterrent and mitigation to hybrid threats.

The next decade will see more submarine fibre-optic cables installed in Canada's northern waters. Those cables will provide a data infrastructure that is critical to the region's security, economy, and society. Few investments are more important for the country to protect. That critical infrastructure will be built in a world dealing with climate change, geopolitical rivalry, more human activity than ever, and legal grey zones. Accordingly, over the next two decades threats to critical undersea infrastructure will likely increase steadily from their currently negligible level and are likely to be classified as low- to medium-threat, high-impact activities.

Currently this type of threat is largely nascent, but a large part of deterring hybrid threats over the long term is ensuring that the country builds its critical infrastructure with the necessary mitigations to address the potential risk of sabotage. A number of malign forces, including the People's Republic of China, are potential hybrid threat actors in Canada's Arctic, but Russia is likely to remain the main concern for Canada by virtue of its geopolitics, geography, and capabilities. The poor state of Canada-Russia relations, mainly due to the latter's war in Ukraine, creates some of the impetus for Russia to attempt to mount hybrid operations against this country. Certainly, Canadian official decision-

makers, business enterprises, and civil society should expect that Russia would consider taking hostile action in an attempt to influence Canada's international conduct. The Arctic is one place where there is the potential for such actions.

Case studies from the Nordic region show that it is very difficult for investigators to determine whether human-caused damage to critical subsea infrastructure is accidental or intentional, particularly in areas where other activities such as commercial fishing are occurring.

Dangers to submarine cables can be mitigated, not eliminated. Improving situational awareness and having response plans in place reduces the risks. The best way to improve situational awareness is to make sure the Canadian Arctic has an adequate array of sensors and operational platforms such as icebreakers and submarines. Also crucial is a whole-of-society approach to these threats that includes all levels of government, Inuit, First Nations, and the business and expert communities. Finally, law enforcement agencies like the Royal Canadian Mounted Police and Fisheries and Oceans Canada require investments to ensure that they can patrol and investigate incidents involving submarine fibre-optic cables amid the specific challenges of the Arctic. **MLI**

Jusqu'ici, ni les gouvernements ni les médias *n'ont manifesté un grand intérêt pour les menaces hybrides dans l'Arctique canadien, surtout celles qui planent sur ses infrastructures critiques. On peut définir ce terme de différentes façons, mais il englobe généralement une grande variété d'activités nuisibles, clandestines et contestables, réalisées par des individus ou des États dans le but de nuire à un autre État ou entité. Cette étude porte sur les menaces hybrides qui ciblent les câbles sous-marins à fibres optiques. Elle tente de mettre en évidence les difficultés à surmonter pour garantir la sécurité de cette infrastructure critique, étant donné les menaces qui la guettent pour les deux décennies à venir. Elle met l'accent sur les actions hostiles de sabotage ou d'interférence, opaques et volontairement anonymes. Selon cette étude, les pays doivent examiner les menaces, la vulnérabilité et les risques auxquels font face leurs infrastructures critiques afin de pouvoir renforcer leur résilience dès que possible : il s'agit là du principal moyen de dissuasion et d'atténuation contre les menaces hybrides.*

Plusieurs nouveaux câbles sous-marins à fibres optiques seront installés dans les eaux nordiques canadiennes au cours de la prochaine décennie. Cette infrastructure de données sera cruciale pour la sécurité et l'économie de la région, ainsi que pour la société : il y a peu d'investissements plus importants pour protéger le pays. Cette infrastructure critique sera érigée dans un monde confronté aux changements climatiques, aux rivalités géopolitiques et à une intensification jamais vue des activités humaines et se retrouvera

dans une zone grise sur le plan juridique. Dans ces conditions, les dangers qui menacent les infrastructures sous-marines critiques ne feront sans doute qu'augmenter au cours des deux décennies à venir, par rapport à leur niveau négligeable actuel, de sorte que ces dernières seront probablement classées comme une activité à risque faible ou moyen, à fort impact.

À l'heure actuelle, ce type de danger n'est qu'embryonnaire. Toutefois, pour une bonne part, contrer les menaces hybrides à long terme nécessitera du pays qu'il se protège du risque de sabotage en érigeant des infrastructures critiques qui intègrent les mesures d'atténuation requises. Si plusieurs puissances malveillantes, notamment la République populaire de Chine, risquent de poser des menaces hybrides dans l'Arctique canadien, c'est toutefois la Russie qui demeurera probablement la principale source de préoccupation du Canada sur le plan géopolitique, géographique et capacitaire. En effet, l'état dégradé des relations Canada-Russie, principalement en raison de la guerre menée par la Russie contre l'Ukraine, pourrait donner une certaine impulsion aux opérations hybrides de la Russie. Les responsables et décideurs, les entreprises commerciales et la société civile du Canada doivent s'attendre à ce que la Russie envisage des mesures hostiles pour tenter d'influer sur la conduite du Canada sur la scène internationale. L'Arctique est l'un des endroits où de telles actions peuvent être menées.

D'après certaines études de cas réalisées dans la région nordique, il est extrêmement complexe pour les chercheurs d'établir si les dommages causés par l'homme aux infrastructures sous-marines critiques sont accidentels ou intentionnels, surtout dans les zones où d'autres activités sont réalisées, comme la pêche commerciale.

Les dangers qui guettent les câbles sous-marins peuvent être réduits, mais pas supprimés. D'où la nécessité d'optimiser la connaissance de la situation et de compter sur des plans d'intervention pour diminuer les risques. Or, le moyen le plus sûr d'accroître cette connaissance est d'affecter à l'Arctique canadien un ensemble suffisant de capteurs et de plates-formes opérationnelles comme les brise-glaces et les sous-marins. Il est également essentiel de mobiliser l'ensemble de la société, y compris tous les paliers de gouvernement, les Inuits et les Premières Nations, ainsi que les communautés d'affaires et d'experts. Enfin, il faut investir dans les organismes chargés de l'application de la loi, comme la Gendarmerie royale du Canada et Pêches et Océans Canada, afin de pouvoir patrouiller et enquêter sur les incidents liés à des câbles sous-marins à fibres optiques, et ce, en tenant compte des difficultés propres à l'Arctique. **MLI**

Introduction

The Canadian Arctic is changing. Climate change and Indigenous governance are transforming the lives of northern Canadians at the same time as the world's geopolitical situation is presenting new threats to the country's security. Despite those realities, discussions of hybrid threats (see sidebar, page 8) remain few. Their relevance, however, will increase as investments in critical infrastructure grow. One piece of infrastructure that could be particularly affected is submarine fibre-optic cables.

To date, hybrid threats have not formed a significant part of either public policy debate or the specialist literature about the Canadian Arctic. As defence analysts Gaëlle Rivard Piché and Bradley Sylvestre observe, hybrid threats are rarely included in discussions of Canadian Arctic security (Rivard Piché and Sylvestre 2023). That situation needs to change in order to ensure that Canada's infrastructure is built in such a way as to be as resilient as possible to the range of threats it faces, both natural and human. Thus, the range of targets for hybrid threats will be greater. This paper draws attention to the connection between critical infrastructure and hybrid threats in the Arctic by examining one potential threatening state, the Russian Federation.

Undersea cables are critical infrastructure

Subsea fibre-optic cables are arguably the cornerstone of critical international infrastructure; they are equivalent in importance to financial institutions (which in fact depend on them to conduct transactions) (Davenport 2015). As one engineer puts it, submarine cables will be the "uncontested key enabling technology of the global network" (Chesnoy 2015). They are highly reliable and relatively low cost compared to the major alternative technology, satellite

communications. They move data some 10 times faster than satellite; as of 2015, they could carry 20 terabytes per fibre cable, which outcompetes satellites by a factor in the tens of thousands (Chesnoy 2015; Doğan and Cetikl 2023). Such volume is crucial for handling the burgeoning data flows that are being generated by inter-object networks such as the Internet of Things.

It is well recognized internationally that subsea fibre-optic cables are critical. Not only did the UN deem them critical in 2010, but according to the U.S. Department of Defense, cable landing sites (see below) are among the "most critical of infrastructures" (Davenport 2015). A report commissioned by the European Parliament states that "protecting submarine cables is far too essential a domain of international politics to remain a technical addendum to security analysis" and their governance is a "truly cross-cutting" issue (Bueger, Liebetrau, and Franken 2022). The NATO Maritime Centre of Excellence recognizes that the impossibility of perfect security means that "the protection of [critical infrastructure] CI is essentially a multidimensional risk management practice" and a shared private-public responsibility (Doğan and Cetikl 2023).

A definition of hybrid threats

There are various definitions for hybrid threats (see Appendix A). For the purposes of this paper, hybrid threats are acts or attempted acts of sabotage that the perpetrator conducts covertly in hopes of evading detection and responsibility. Hybrid threats can be carried out by states or by civilians operating legally or illegally at a state's behest. While deniable, it is nonetheless ambiguously apparent who is likely responsible, which is done purposefully to prompt the state on the receiving end to change its policies.

Subsea fibre-optic cables are a major investment and are a prized asset to the communities they serve – some local, some global. They are certainly well worth protecting. They have a usual lifespan of at least 25 years and we are currently at the early stages of their investment and construction period in the Canadian Arctic. For critical infrastructure such as this, the best time to talk about building in resilience is at the beginning, so that security is fully integrated into their architecture (Hathaway 2019; 2020).

Scope of the assessment

This report will concentrate on the physical threats to infrastructure hardware (see Sidebar 2). Hybrid threats to submarine cables fall into two groups: disruption and exploitation. Disruption entails a variety of covert activities conducted at the ocean's surface, underwater, or on land to sabotage the physical infrastructure. Exploitation involves physically compromising the subsea cable infrastructure at some point to gain access to the data it is carrying. Such "tapping" could occur on the cables themselves, but because such an operation is very difficult to undertake and is detectable, it is less of a threat (Goodman and Wayland 2022). More likely is a compromise at a landing station (i.e., the place the cable comes out of the water and connects to land-based cables) conducted by an "insider" with access to the facility.

This paper will look at how divers, submarines, surface vessels, fishing nets, anchors, insiders, and so on can damage the cables and landing stations. It will argue that the increasing presence of subsea cables in Canada's North gives saboteurs a new opportunity to damage this infrastructure, even as they deny doing so.

The focus of this paper is not a denial that other threats exist and are pertinent. In fact, cyber saboteurs operating remotely present an acute threat to submarine cables, whether they are siphoning off or corrupting data. They can do so by hacking (in technical terminology, conducting computer network exploitation (CNE) to intercept data transmissions) or, more aggressively, interfering with software in order to disrupt the network's hardware and thereby disrupt its activities (in other words, conducting a computer network attack (CNA)). Countries need to deploy a specific set of security and mitigation strategies to respond to CNE and CNA attacks (Goodman and Wayland 2022, 7–8). Physical threats, particularly those in the Arctic, entail different prevention, detection, mitigation, and response tools. It is these that the paper will explore.[1]

To examine the nature of this threat, the paper will focus on Russia. That is not because Russia poses the only potential threat. China is also striving for more presence in the Arctic, rapidly building the capacity to work beneath the waves and in the ice, and has a track record of coercive behaviours at sea that fit the descriptions of hybrid threat; it is certainly worthy of more study (Tetsuo and Kuok 2023: 04:27; Urbina 2023; Huebert 2023). At the same time, non-

state actors such as violent extremists or organized criminals could also be potential threats (Bueger and Edmunds 2017), especially as civilian maritime activity in the Canadian North becomes more frequent and more international.

That acknowledged, Russia remains the primary threat, if only because of its range of access, motives, intentions, strategic goals, and capabilities. It sees Canada as acting contrary to its interests. It is signalling that it is unhappy with other Arctic countries. At the same time, the Arctic is assuming more and more importance in Russia's geostrategy. Moreover, if China (the PRC) is to engage in more activities in the Arctic, there are good reasons to think that Russia will be critical to the PRC's pursuit of its objectives, and thus Russia may be implicated in potential PRC hybrid operations in the Arctic. Finally, part of the reason for concentrating on Russia is analytical: we have a body of examples of potential Russian involvement in damage to submarine fibre-optic cables in the Nordic-Baltic region. These cases provide insights for analysts trying to identify the characteristics of hybrid threats to this infrastructure and their applicability to Canada's north, regardless of the perpetrator.

Submarine fibre-optic cables: The hardware

Cables, amplifiers, and landing stations are the key elements in the submarine fibre-optic cable networks. Along the cables at about every 70 kilometres are amplifiers that boost the signal they are carrying. Branch units can split off to serve locations along the main route. The cable end-points are at landing stations, some of which are full data centres (Chesnoy 2015).

The installation, maintenance, and repair of subsea cables are carried out by a specialized fleet of about 60 vessels worldwide.

The cables are multi-use. In addition to transmitting digital data, they can collect seismic and oceanographic data such as water temperature and sea-level change, useful for a range of environmental, commercial, civil, and military applications (Lentz 2015).

Subsea cables in the Canadian Arctic

The Canadian North is in the early stages of a subsea fibre-optic cable infrastructure expansion. As part of the federal government's priority to improve broadband connectivity in rural areas, it has earmarked some C$4 billion for investments through the Canada Infrastructure Program, the Universal

Broadband Fund, and the Canadian Radio-television and Telecommunications Commission's (CRTC) Broadband Fund. Developers can use that money for investments in cable, wireless, and satellite networks across Canada, including in the North (Innovation, Science and Economic Development Canada 2022). This priority enjoys support from provincial and territorial governments and from Indigenous groups (Canada 2019; CanNor 2019; ITK 2019 and 2021; Delaunay 2017; Wright 2023).

Several projects are underway. The initial phase of the Eastern Arctic Underwater Fibre Optic Network (EAOUFON) in Hudson Bay led by the Kativik Regional Government runs from the municipalities of Chisasibi to Puvirnituq in Quebec, and a phase 2, extending it to Salluit, became operational in early 2024 (Kativik Regional Government 2023 and 2024); Quinn 2022). Another plan, led by CanArctic Inuit Networks, would have as many as four segments, starting with a link from Goose Bay in Labrador to Iqaluit in Nunavut (Wright 2023). The Government of Nunavut has explored other initiatives to connect more points in the territory (Nunavut 2022; Pelletier 2024). Furthermore, terrestrial fibre-optic cables now reach the coast in Inuvik in the Northwest Territories, and another project, Kivalliq Hydro-Fibre, will connect Manitoba to Chesterfield Inlet on the western shore of Hudson Bay in Nunavut (Crown-Indigenous Relations and Northern Affairs Canada 2024; Kivalliq Inuit Association 2021). For each of these projects there is the potential for undersea extensions to communities in the coastal and archipelagic parts of the Northwest Territories (NWT) and Nunavut.

In addition, two transoceanic cable projects, Far North Fibre and Polar Connect, are looking to take advantage of northern Canadian waters. Far North Fibre envisages running a cable some 14,000 kilometres from Norway through the Northwest Passage (NWP) and Bering Strait to Japan. The project includes potential for trunk lines to land points along the NWP. It aims to be fully up and running by 2027 (Far North Fibre 2023). Polar Connect, which is at an earlier phase of development, would run north of Greenland and likely through Canada's exclusive economic zone (EEZ) (Middleton and Rønning 2024). Both projects point to industry's interest in the shorter distances that trans-Arctic routes provide and speak to the high likelihood that the coming decades will see this interest turned into finished projects.

A final area of potential development is in specific natural resources projects. The intense data needs of the mining sector, for instance, will further

increase with digitalization, remote and autonomous equipment, and artificial intelligence, and projects will benefit from a fibre-optic backbone. For example, the oil and gas sector has developed its subsea connectivity in the installation of a combined electrical and fibre-optic network for the Norwegian Breidabblik offshore oil field (Alcatel 2023). Similar connectivity will be required should subsea mining ever occur in Canadian jurisdictions.

Security in the Canadian Arctic is evolving

The subsea fibre-optic infrastructure will be constructed in a deteriorating security climate. Four specific conditions ensure that the way threats could unfold in Canada's North are diverse. These conditions are climate change, the scope for human activities, geopolitics, and gaps in the international legal regime. More humans, more infrastructure, and more types of activities are altering the security picture in Canada's Arctic.

First, climate change is melting sea ice in Arctic waterways. According to the latest edition of *Canada's Changing Climate Report*, sea-ice coverage has decreased in the Canadian Arctic some 5 to 20 percent per decade since 1968; sea ice thickness is also decreasing. Over the longer term, the main climate models see these trends continuing. In the Canadian Arctic sea ice is retreating more slowly than in other parts of the Arctic, and the waterways of the archipelago and the waters on the northern extents of the Greenland-Canada maritime border will be some of its last strongholds. Nonetheless, the Beaufort Sea and Baffin Bay will likely have "extensive" ice-free summer seasons by 2050 (Bush, Bonsal, Derksen et al. 2022).

Second, these changing climate conditions will expand the range of economic activities and forms of human presence in the Canadian North. These factors will increase the sailing season in parts of Canada's Arctic waters. In line with the Canada-specific ice factors mentioned above, a year-round navigable Northwest Passage is not likely before 2100, and thus determining the effects of a significantly higher volume of commercial shipping is beyond the time horizon of this paper. However, maritime transit without the support

of an ice breaker may be feasible for part of the season by 2050 (Marsh Risk Management Research 2014). And other human maritime activities, notably fisheries, tourism, and scientific research by those not from the North will become more frequent over the next two decades.

For the purposes of this paper, fisheries are especially worthy of note. The potential for more extensive fishing activities on the Central Arctic Ocean, as well as (legally or illegally) within Canada's extended economic zone in places like Baffin Bay or the Beaufort Sea, is likely to increase. As of 2023, some 41 percent of the vessels plying Arctic waters were fishing vessels – by far the largest category; that number reflected a growth of 26.3 percent from 2013. The scientific community does not yet have a handle on fish stocks in the Arctic Ocean and adjacent waters, but these are assumed to be large, especially as more southern species move north as water temperatures rise (Environment and Climate Change Canada 2023).

Third, international competition in the Arctic is intensifying. Russia, China, and the US all have Arctic strategies and are seeking to protect and advance their interests there (White House 2022; China 2018; Russian Federation 2023b; Huebert 2019). Furthermore, this competition is characterized by complex economic interdependencies (Pohl, Ponczek, and Wigell 2023), a situation that lends itself to the deployment of hybrid threats (Gressel 2019). Adversaries may well undertake covert, deniable activities in Canada's Arctic to try to coercively and malignly influence Canadian decision-making, social stability, and political legitimacy.

Fourth, there are gaps in what is a complicated legal regime for this infrastructure. Cables are often subject to the laws of multiple jurisdictions. Because submarine cables run mostly in international waters, large portions of them are covered by international law (Davenport 2015; Bueger and Liebitrau 2021). Specifically, the United Nations Convention on the Law of the Sea (UNCLOS) describes the rights and obligations of states when it comes to the protection and installation of undersea infrastructure. The rules are complex and involve freedom of navigation, extended economic zones (EEZs), and the sovereign rights of coastal states and those of other countries. As professors Christian Bueger and Timothy Edmunds (2017) describe it, it is a "trans-national environment" complicated by what Bueger and Tobias Liebetrau (2021) depict elsewhere as the multi-use character of the sea, where many different human activities take place including fishing, oil and gas exploration, shipping, and

scientific research and telecommunications, with a variety of rights and obligations according to each area of activity. According to law-of-the-sea specialist Tara Davenport (2015), this has resulted in a patchwork of legal jurisdictions that has left "significant gaps" around the security of the undersea hardware making it vulnerable to interference and espionage activities. This makes for a number of grey zones in which those involved in hybrid threats can operate.

> *At one time the Arctic was hard to access and contained few important targets. Now, access is opening up and potential targets increasingly plentiful.*

These factors are changing how the threats will manifest in the Canadian Arctic. A key contention of this paper is that threats to the region are becoming more likely. At one time the Arctic was hard to access and contained few important targets. Now, access is opening up and potential targets increasingly plentiful. Using a framework developed by professor and expert on Northern policy Whitney Lackenbauer (2021), there is an increasing likelihood of threats manifesting in and not just transiting through the Arctic. In other words, the North American Arctic will become a potential theatre, not just a waypoint, for hostile activities against Canada. Hence, policy-makers must reconsider the types of threats that infrastructure in the Artic faces and the strategies and institutions needed to protect against them.

The likelihood of hybrid threats – particularly those that require a physical presence, such as sabotage – comes from a very low baseline. But this paper will draw attention to the long-term horizons involved in critical infrastructure investments, and argue for developing deterrence, mitigation, and response strategies with these time horizons in mind. In the case of subsea cables, the cable itself can be expected to last 25 years. Thus, one cannot simply assume that risks that seem improbable today will not be much more likely in 10- or 20-years' time. The fact that suspected events are already occurring makes the timing for considering this threat in the Canadian Arctic propitious.

It is to these suspected incidents we will now turn.

Cables under threat: Nordic case studies

Several case studies illustrate the types of threats submarine fibre-optic cables face. Elsewhere in the world undersea infrastructure is already the target of potential acts of hybrid warfare. This paper will now examine a small but growing body of cases emerging from the Nordic and Baltic regions over the last four years in which Russia or those operating on behalf of Russia are the primary suspects in damage to undersea infrastructure. Four incidents have occurred, two in northern waters off the coast of Norway and two in the Baltic Sea. These incidents follow public reports of the Russian Navy engaging in activities near transoceanic cable routes off the coast of the United States in 2015 and off Ireland in 2022 (Reuters 2015; Mills 2023; Chouinard and Hales 2020). These incidents form the empirical basis for the subsequent analysis of potential Russian hybrid threat activity.

In the Norwegian cases, Russian fishing vessels severely damaged undersea cables. The first incident, in April 2021, saw a large portion of a joint scientific-military subsea cable network off the Vesterålen Islands ripped away by fishing nets. In January 2022, a second incident saw the cable connecting Svalbard to the Norwegian mainland severed, again by fishing gear. Some of the same vessels were present in both cases. Ultimately, however, Norwegian police suspended their investigations of the incidents due to a lack of evidence and deemed them accidents (Fredriksen 2022).

Similarly, the Baltic Sea has seen two major events. The first was the September 2022 destruction of the Nord Stream natural gas pipeline connecting Russia and Germany. In this case, it is clear that the pipeline was intentionally sabotaged but the culprit behind the damage has yet to be confidently identified. However, one of the leading explanations is that Russian actors were involved (Reuters 2024; Kirby 2024).

Next, the Baltic Connector incident occurred in October 2023 when a container ship dragged its anchor and damaged a digital cable between Sweden and Estonia and severed a cable and a gas pipeline between Finland and Estonia (as well as a cable between the Russian mainland and its enclave of Kaliningrad). The vessel was Hong Kong-registered and seemingly owned by a Chinese-Russian group. That an accident caused the damage remains one hypothesis, but the distance of the anchor drag (over 150 kilometres) and the

ship's subsequent unusual port calls have led marine security experts to consider it credible that the act was intentional, although at whose behest is still not publicly known (Kärmas 2024).

These episodes reveal two basic realities for anyone attempting to conduct a deniable hostile act against subsea fibre-optic cables. First, civilian activities like fishing and maritime shipping in the vicinity of the cables provide opportunities for anonymous saboteurs to disrupt physical subsea infrastructure. A hybrid operation conducted at sea can be masked by considerable other maritime "noise": accidental damage to cables occurs frequently. In fact, there are about 150 incidents per year worldwide of damage caused by seismic disturbances, anchors, and fishing nets (Doğan and Çetikl 2023). Moreover, the cables' routes are usually available publicly so that navigators can avoid them – or, for those with hostile intentions, locate them exactly.

Second and consequently, determining responsibility is difficult, not because immediate responsibility cannot be attributed, but because of the investigatory challenges distinguishing between intentional and accidental causes. Thus, deniability is complemented by a perception of impunity. Therefore, when there is a lot of civilian activity taking place during a period of geopolitical tension, that combination of circumstances offers considerable opportunities for hybrid operations to take place (Beuger and Edmunds 2017).

> *Ice and poor weather conditions throughout much of the year would necessitate subsea sabotage.*

From the Nordic episodes we can extrapolate to the Canadian Arctic, where ice and poor weather conditions throughout much of the year would necessitate subsea sabotage, though only the most sophisticated state actors – mostly navies – are capable of taking such action. Advances in remotely operated or even autonomous submarine technologies – for instance those associated with oceanic research or subsea mining – might be repurposed for hostile acts. In such cases, one benefit to the perpetrator is that they rely on a more physically distant base of operations.

Fishing activities stand out as the most plausible platform in the Canadian Arctic for hybrid activities initiated from the water's surface in part because these activities will be the most prevalent over the next few decades. The guise of accidental ensnarement of cables by fishing gear due to illegal fishing or by foreign vessels transiting Canada's EEZ to the Central Arctic Ocean would be both feasible and plausibly deniable. In 2036 the International Agreement to Prevent Unregulated Fishing in the High Seas of the Central Arctic Ocean, which places a moratorium on commercial fishing in that area, will be up for renewal. Consequently, analysts of hybrid threats see this as a key date; that is the year they will learn what sort of international agreement, if any, is going to be in force for the subsequent years (Arctic Council 2021).

Russia's role in subsea hybrid threats in the Canadian Arctic

There are four key reasons why analysts see Russia as a potential hybrid threat actor under the waters of Canada's Arctic. First, it is being assertive in claiming its legitimacy in the Arctic Ocean. Second, its strategic documents demonstrate that Russia believes it is within its rights to take action against countries it deems hostile. Third, it has the tools and technology to undertake complex missions. Fourth, it is in the midst of a strategic rivalry with Canada in which it sees Canada as a threat to core Russian interests. This rivalry is likely to persist for some time. The paper will explore each of these points in turn.

Russia's geopolitics in the Arctic

The Arctic is becoming increasingly important to Russia as it pivots from an export-based economy focused on Europe to one oriented towards Eurasia and the Asia-Pacific, and as its politics become more confrontational against the EU, the US, and NATO – and thus Canada. In addition, international maritime politics, presence, and influence are becoming increasingly important to Russia (Monaghan and Connolly 2023). The result is a fusion of the main themes of Russian policy in the Arctic Ocean. To dissect this

development, we need to look at Russia's posture on the Arctic Ocean and its "Eurasian" geoeconomic strategy.

Building on decades of commitment to the Arctic dating back to the Soviet period, Russia is re-emphasizing its global oceanic profile and further accentuating its maritime and Arctic strategy by tying them closely to the country's future economic potential. For instance, its 2023 Foreign Policy Concept (FPC) document states the importance of the maritime domain to Russia's strategic interests (Buchanan 2023). The Russian Federation's 2022 Maritime Doctrine (MD) sees the "world ocean" as a growing area of priority.

As part of this vision, the Arctic Ocean has gained prominence in Russian strategic thinking. The MD deems the Arctic Ocean a "vital" interest of the Russian Federation (the same term it uses to describe its interests in Ukraine), outranking the importance for Russia of the Atlantic and Pacific oceans. In the FPC, the Arctic is prioritized second only to the "near abroad" of neighbouring states. The region is central to Russia's strategic objectives of creating a "Great Eurasian Partnership" that would blend the continental and the maritime, and in which northern waterways would connect Russia with China, India, and Asia-Pacific countries.

The Arctic Ocean is also central to Russia's economic prosperity agenda. Russia's national security and socio-economic agendas are aligned as expressed, for instance, in its 2021 National Security Strategy (NSS). Core among these are developing a Russian-controlled Northern Sea Route (NSR) as a waterway for transoceanic shipping, and harvesting mineral and energy resources from the Arctic Ocean's seabed. Russia is among those at the forefront of international ambition to exploit undersea mining and energy reserves.

Russia's strategic documents map the rising importance of the Arctic to the highest levels of the Russian leadership, but there are also some concrete indicators. Russia's war in Ukraine and its subsequent isolation from key energy export markets in Europe has led to the NSR seeing its highest shipping volumes to date. Russia is pushing to make the NSR navigable year-round and has rolled back regulations in an attempt to spur development of the adjacent coast (Humpert 2023a and b; Zelenaya 2022).

Hybrid war and subsea cables

Russia's ideas and agenda are taking shape in an international context that the Russian leadership sees as hostile. It believes that the collective West has a general and active hostility towards it. Russia sees itself as the target of a "hybrid war" (Russian: *гибридная война*) by the United States and its allies, who, it alleges, are trying to contain Russia using their informational, economic, diplomatic, intelligence, and military capabilities (Russian Federation 2021, sections 6, 7; Russian Federation 2023a, 8, 11, 13; Russian Federation 2022, 20, 22). Russia claims that other states are militarizing the Arctic, and that the region is a space of "global competition" that has military and economic dimensions (Russian Federation 2023a, section 50.2; Russian Federation 2022, 50).

It is crucial to note that Russia's international conduct is structured around the concepts of the balance of power and reciprocity. If it thinks it is the target of hybrid warfare, it is likely to respond in kind (Russian Federation 2023a, section 12). Russia's strategic documents mention asymmetric "hybrid" activities. They grant the state significant latitude to conduct activities that will forward (in Russia's perception) these objectives. Key statements where Russia justifies its right to respond in kind include the FPC's declaration (Section 14, 26) that it will use "all means necessary" to pursue its defence and development, as well its stated readiness to deploy "asymmetrical" responses to "unfriendly acts." Similar enabling language is present in the Maritime Doctrine (Section 32.2), which discusses combining non-military and military measures to respond to security "challenges and threats" and in the National Security Strategy (Section 40.2), which mentions the use of unspecified "other measures" to prevent threats to the Russian Federation.

Russian strategic documents also indicate that digital infrastructures might be a target. They acknowledge the pre-eminence of information technologies in contemporary life, social and economic development, and national security. The informational content flowing along these infrastructures is described as a critical component of contemporary warfare, integral to information dominance (Grisé et al. 2022). The NSS (Sections 52, 55, 57.1, 57.3, and 57.13) alleges that foreign intelligence agencies target critical maritime information infrastructure for sabotage. Again, it is important for readers to keep in mind the core idea of reciprocity in Russian thinking in this context.

Means and opportunities

Russia possesses advanced specialized capabilities that enable it to sabotage submarine cables. The Russian Navy's Main Directorate for Deep Sea Research (best known by its Russian acronym, GUGI) and the Intelligence Directorate of the Main Staff of the Russian Navy are responsible for subsea sabotage. To conduct its activities, GUGI possesses a fleet of specialized submarines. These currently consist of four mini-subs and two larger "motherships" that can transport, launch, and recover the mini-subs. Notably, these vessels are dual-use, capable of rescue and research missions as well as sabotage and espionage. In addition, the Russian Navy's fleet possesses surface vessels for subsea research and intelligence gathering (Kaushal 2023).

Moreover, the country's commercial fishing and merchant fleets are likely available for covert intelligence gathering and operations, as they were in Soviet times (Kaushal 2023). Investigative reporting by Nordic journalists (Camut 2023) describes Russian fishing and research vessels being used for intelligence activities close to critical maritime infrastructure such as wind farms in the North Sea. And the Baltic Connector incident suggests that commercial cargo vessels may also be involved in state-backed deniable operations (Dalziel and Vanhanen 2023).

> *"Hybrid threats against submarine fibre-optic cables … will become more feasible over the next 20 years.*

While hybrid threats against submarine fibre-optic cables in Canada's Arctic waterways would be among the most difficult operations to execute, they will become more feasible over the next 20 years. As the sea ice melts and these waters become navigable for longer stretches of the year, there will be an increasing amount of maritime traffic. Fisheries and commercial shipping, for instance, are likely to be of interest to a range of foreign players, including Russia and China. The increased traffic will also increase the feasibility of using plausible civilian covers for "accidental" and deniable disruptions as their vessels transit Canada's EEZ on the way to the Central Arctic Ocean, for example.

The threat to Canada's Arctic

Canada and Russia, Arctic powers both, find themselves on opposite sides of a geopolitical rivalry. Moscow almost certainly sees Canada as part of a US-led concert of countries aiming to contain and constrain it, and thus an obstacle to Russia accomplishing its main strategic objectives in Ukraine and the Arctic. The Arctic is among the highest international priorities for the Russian leadership. At one time, diplomacy, science, and business in the Arctic was a primary contact point for Canadian and Russian officials and citizens. While many factors will determine how likely it is that Russia will attempt to sabotage infrastructure in Canada's Arctic, this paper analyzes the language in Russia's strategic documents to interpret its threat perception of Canada. This analysis will help to frame the factors that might lead to Russia undertaking hybrid activities in Canada's Arctic.

Moscow sees Canada's membership in NATO, the presence of the Canadian military in Latvia, and Canada's support for Ukraine as all running counter to Russia's interests. Canada's material and rhetorical support for Ukraine run counter to Russia's main foreign policy goal (National Defence Canada 2024b). Canada's imposition of a steadily widening group of sanctions on Russian individuals and companies is a particular source of tension with Moscow: it reacted vociferously, for example, to Canada's seizure under the sanctions regime of an Antonov An-124 heavy lift aircraft registered to a Russian company in Toronto in June 2023 (Justice Canada 2017; Global Affairs Canada 2024; Reuters 2023). Canada's decision to support sending seized Russian central bank assets to Ukraine is also certain to garner sharp Russian criticism (Axworthy 2024; Fabrichnaya and Falconbridge 2023).

Although Russia's most recent strategic documents do not refer to Canada specifically (it was explicitly named in the 2016 FPC), Canada is an obvious if unnamed country among the group that Russia describes as most hostile towards it in the 2023 FPC document (Section 13, 62–64). Canada clearly belongs as, in the FPC's language, it is a United States' satellite, is an "Anglo-Saxon" country that is a member of a "small group" of countries pushing imperious notions of rules-based international order (RBIO) and desperately trying to perpetuate a failing hegemony over world affairs. Moscow is open about having added Canada in March 2022 to its list of "unfriendly" countries

(TASS 2023), and Canada is the subject of detailed Russian state reports alleging it tolerates "Russophobia" (Russian Federation 2024).

Moreover, Canada is likely one of the regional states Russia accuses of "militarizing" the Arctic and limiting Russia's sovereignty there – acts that the strategic documents state will require "counteraction" from Russia (Russian Federation 2023a, section 50.2). In addition, language in the FPC (2023a, section 23.6; Dalziel 2024) and in the MD (Russian Federation 2022, section 50.11) about "stepping up" efforts – not necessarily aggressively, but signalling vigour and determination – to delineate maritime boundaries is certainly directed at Canada (and the US and Denmark, as well as China, though probably indirectly), as the two countries' Arctic continental shelf claims overlap in a number of places.

The documents do not entirely rule out Russia's cooperation with Canada in the Arctic, for instance on settling the limits of the continental shelf (Russian Federation 2022, section 50.11). Nonetheless, the overall thrust of these documents along with more general Russian statements show a deteriorating relationship. In this regard, Canadian decision-makers should expect that among the options available to it, Russia would consider taking hostile actions to correct Canada's "unfriendly course" (2024a, section 64). In light of the factors described above in Section 3, the Arctic is one potential location for such actions.

Recommendations

Hybrid threats to submarine fibre-optic cables in the Canadian Arctic will become increasingly probable if the current trends in climate change, economic activity, and geopolitical competition persist over the cables' 25-year lifespan. Canada can take a number of steps to ensure that those threats remain a low probability during that time. By taking the actions outlined below, Canada can reduce the likelihood that Russia could successfully sabotage the cables – and can raise the potential costs for Russia and other countries that might contemplate doing so in Canada's North. In fact, these

steps are useful for deterring, detecting, and responding to a range of threats to Canada in the Arctic, including conventional military, environmental, and economic security. Importantly, taking steps to make the North and its infrastructure more secure is not a matter only for the military – or indeed only for the federal government: all levels of government, including Inuit and First Nations' treaty-rights holders, along with the business sector and civil society need to be involved to ensure comprehensive security for submarine cables (Bueger and Liebetrau 2021).

> *Taking steps to make the North and its infrastructure more secure is not a matter only for the military – or indeed only for the federal government.*

Three actions are key for Canada to take. The first is to improve the sensor network in the Arctic, particularly in the ocean. Second, Canada should boost the regular presence of the Canadian Coast Guard and the Canadian Armed Forces as well as fishery patrols in the region. Third, intelligence and law enforcement should be trained and assigned to detect, assess, and investigate hybrid threats. Finally, Canada should develop a plan that involves stakeholders from across society to prevent, mitigate, and respond to hybrid threats. We will briefly discuss these actions below.

Last year, reports from the Senate of Canada (2023) and Parliament (House of Commons 2023) called for improved sensors in Canada's Arctic waters, and subsequently the 2024 Canadian defence policy commits to enhancing shipborne and satellite sensing technologies (National Defence Canada 2024a). But the government should also look at installing fixed subsea sensors, including integrating detection capabilities into the cables themselves (see Sidebar 2), and adding a floating network of buoys to add further to its ability to detect potential threats. If the government were to go further and optimize the Arctic and Offshore Patrol Vessels and the new Polar and medium-class icebreakers (Canadian Coast Guard 2019; Royal Canadian Navy 2024) to

carry remote and autonomous "mini" submarines to gather subsea data, doing so would advance its awareness of Arctic activities and improve the federal government's investigatory capacity should an incident occur.

We also recommend that as quickly as possible the government replace the Victoria class submarines with those with better under-ice capabilities and expedite research into the feasibility of purchasing autonomous and semi-autonomous vessels and aircraft for the CCG and CAF. The government should also quickly implement the Defence policy plan outlined in *Our North, Strong and Free* (National Defence Canada 2024a) to develop a more extensive network of "northern operational support hubs" for refuelling and resupply of vessels and aircraft.

If Canada is to detect and react to hybrid threats it will need to invest in intelligence and law enforcement. Canada must develop expertise built around Russia-related knowledge, knowledge of maritime industry, and knowledge of society and governance domestically and internationally if it is to build an effective strategic and operational intelligence. Canada should also bolster its law enforcement capacity to enhance the ability of the Department of Fisheries and Oceans to conduct fisheries patrols in northern waters. RCMP investigators should be equipped with the knowledge, skills, and remit to work with international counterparts and the private sector, especially in the United States and the Nordic countries on suspected incidents of hybrid activity.

Canada can strengthen its resilience and deter hybrid attacks by enhancing its prevention and response strategies. If Canada can react quickly to repair any damage that occurs to subsea cables it will decrease the attractiveness of this infrastructure as a target for hybrid operations. Moreover, on the international stage, Canada should explore how cooperation with other NATO countries could improve the security of the critical infrastructure located in the North (NATO 2023). Filling any gaps in international law with regards to submarine cables is also important, in part to ensure that authoritarian countries do not have undue influence in shaping these laws. That, in turn, will help to ensure that international dialogue on the security of this critical infrastructure is in line with a rules-based, accountable ethos.

Conclusion

We can no longer afford to be complacent about national security in the Arctic. The inhabitants of the region are working hard to build the critical infrastructure to advance their economic opportunities and protect their communities. Submarine fibre-optic cables are but one of the critical infrastructures that will require security, and the time to think long-term about protecting them from the range of threats they will face is now.

This paper has looked at one dimension of threat, that presented by foreign states looking to covertly sabotage underwater cables. It has pointed to the essential character of this infrastructure to global telecommunications and the development of Canada's North. By looking at case studies from the Nordic region, aspects of how one potential threat actor, the Russian Federation, might pursue such activities in the Canadian North has been explored. Attention to the dynamics of relations with authoritarian governments in Russia, the People's Republic of China and elsewhere will be imperative for governments in Canada. Hybrid threats that require physical presence in the Arctic remain the purview of an elite range of foreign actors, and the ongoing harshness of the northern climate will make executing them an operational challenge. Keeping them low-probability threats for the multi-decade lifespans of this infrastructure will demand work now.

All levels of government, the business community and the peoples of the North can work together to ensure the security and continuity of a backbone digital infrastructure like submarine cables. As different governmental and civil societal organizations have recommended, core to this will be improving awareness in the Canadian Arctic through cooperation and integrating technologies such as sensors, aircraft, maritime vessels and the cables themselves. In addition, this paper recommends paying special attention to enhancing the training for federal authorities in investigating suspected incidents of covert sabotage. Furthermore, partnerships with the US, Nordic countries, and NATO, as well as work to ensure an accountable framework of international law, will improve the conditions for Canada to build submarine fibre-optic cable networks in the North to last. MLI

About the author

Alexander Dalziel is a senior fellow at the Macdonald-Laurier Institute with over 20 years of experience in Canada's national security community. Previously, he held positions with the Privy Council Office, Canada School of Public Service, Department of National Defence, and Canada Border Services Agency. During that time, he worked across multiple operational and strategic domains. Dalziel holds bachelor's and master's degrees in history from Memorial University of Newfoundland and Labrador, as well as certificates in Russia and Baltic Area Studies from the University of Eastern Finland and in European Studies from the University of Bonn. MLI

The author would like to acknowledge the support of the Hecht Foundation and the Macdonald-Laurier Institute. The author also benefited from conversations with industry representatives and scholars.

References

Alcatel. 2023. "Alcatel Submarine Networks DC/FO subsea control cable infrastructure is in operation for oil production at Equinor Breidablikk field." Available at: https://web.asn.com/media/data/files_user/72/PDF/Press Release Breidablikk DCFO.pdf.

Arctic Council. 2021. "An Introduction To: The International Agreement To Prevent Unregulated Fishing In The High Seas Of The Central Arctic Ocean." Available at: https://arctic-council.org/news/introduction-to-international-agreement-to-prevent-unregulated-fishing-in-the-high-seas-of-the-central-arctic-ocean/.

Arctic Council. 2024. "The Increase in Arctic Shipping 2013–2023." Arctic Shipping Status Report #1: 2024 Update. Protection of the Arctic Marine Environment [PAME]. Available at https://pame.is/images/03_Projects/ASSR/ASSR_1_-_2024_update.pdf.

Axworthy, Lloyd, and Fen Osler Hampson. 2024. "The G7 Can Prove Its Commitment to Ukraine by Seizing Russian Assets." *Globe and Mail*, January 16, 2024. Available at https://www.theglobeandmail.com/opinion/article-the-g7-can-prove-its-commitment-to-ukraine-by-seizing-russian-assets/.

Buchanan, Elizabeth. 2023. "It's Russia's (Maritime) World – We're Just Living in It." Commentary. RUSI, October 2, 2023. Available at https://rusi.org/explore-our-research/publications/commentary/its-russias-maritime-world-were-just-living-it.

Bueger, Christian, and Timothy Edmunds. 2017. "Beyond Sea Blindness: A New Agenda for Maritime Security Studies." *International Affairs* 93, 6: 1293–1231.

Bueger, Christian, and Tobias Liebetrau. 2021. "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network." *Contemporary Security Policy* 42, 3: 391–413. Available at https://www.tandfonline.com/doi/abs/10.1080/13523260.2021.1907129 [paywall].

Bueger, Christian, Tobias Liebetrau, and Jonas Franken. 2022. *Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU*. European Parliament. Available at https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf.

Bush, Elizabeth, Barrie Bonsal, Chris Derksen, et al. 2022. *Canada's Changing Climate Report in Light of the Latest Global Science Assessment*. CCR 2022 Supplement. Government of Canada. Available at https://changingclimate.ca/site/assets/uploads/sites/2/2022/03/CCCR-2022-Supplement-Final.pdf

Camut, Nicolas. 2023. "Russia Uses Civilian Boats to Spy in the North Sea." *Politico*, April 19, 2023. Available at https://www.politico.eu/article/russia-uses-civilian-ships-to-spy-in-the-north-sea-reports/.

Canada. 2019. *Pan-Territorial Chapter: Arctic and Northern Policy Framework*. Government of Canada. Available at https://www.eia.gov.nt.ca/sites/eia/files/2019-06-10_anpf_-_pan-territorial_chapter_-_en_-_final.pdf.

Canadian Coast Guard. 2019. "Canadian Coast Guard's New Icebreakers." Backgrounder, July 2019. Government of Canada. Available at https://www.canada.ca/en/canadian-coast-guard/news/2019/08/canadian-coast-guards-new-icebreakers.html.

Canadian Northern Economic Development Agency [CanNor]. 2019. *Pan-Territorial Growth Strategy: Working Together for a Better Future*. Government of Canada. Available at https://www.cannor.gc.ca/eng/1562247400962/1562247424633.

Chesnoy, José. 2015. "Presentation of Submarine Fiber Communication." In José Chesnoy (ed.), *Undersea Fiber Communication Systems* (Elsevier Science and Technology): 3–52.

China. 2018. *China's Arctic Policy*. State Council of the People's Republic of China, January 26, 2018. Available at http://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm.

Chouinard, Paul, and Doug Hales. 2020. *The National Critical Infrastructure Interdependency Model—Volume VII: Characterizing the Information and Communications Technology Sector*. Defence Research and Development Canada.

Crown-Indigenous Relations and Northern Affairs Canada. 2024. "Minister Vandal Announces Federal Funding Towards Kivalliq Hydro-Fibre Link to Advance Clean Energy Transition and Broadband Service Delivery to the Kivalliq Region." News release. Government of Canada. Available at https://www.canada.ca/en/crown-indigenous-relations-northern-affairs/news/2024/03/minister-vandal-announces-federal-funding-towards-kivalliq-hydro-fibre-link-to-advance-clean-energy-transition-and-broadband-service-delivery-to-th.html.

Dalziel, Alexander, and Henri Vanhanen. 2023. "Undersea, Under Threat." *Inside Policy*, November 6, 2023. Macdonald-Laurier Institute. Available at https://macdonaldlaurier.ca/undersea-under-threat/.

Dalziel, Alexander. 2024. "Russia's Tough Talk on Arctic Sovereignty Must Be Taken Seriously." *Geopolitical Monitor*, March 4, 2024. Available at https://www.geopoliticalmonitor.com/russias-tough-talk-on-arctic-sovereignty-must-be-taken-seriously/.

Davenport, Tara M. 2015. "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis." *Catholic University Journal of Law and Technology* 24, 1: 57–109, article 4. Available at https://scholarship.law.edu/jlt/vol24/iss1/4.

Delaunay, Michael. 2017. "Submarine Cables: Bringing Broadband Internet to the Arctic, a Life Changer for Northerners?" In Lassi Heininen, Heather Exner-Pirot, and Joël Plouffe (eds), *Arctic Yearbook 2017* (Northern Research Forum). Available at https://arcticyearbook.com/arctic-yearbook/2017/2017-briefing-notes/250-submarine-cables-bringing-broadband-internet-to-the-arctic-a-life-changer-for-northerners.

Doğan, Diren, and Deniz Çetikl. 2023. "Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment." In Mustafa Poyraz (ed.), 3rd *Maritime Security Conference Proceedings: Maritime Security in the Scope of NATO's New Strategic Concept.* (Maritime Security Centre of Excellence (MARSEC CoE)): 41–42. Available at https://www.marseccoe.org/publications/#single/0.

Environment and Climate Change Canada. 2023. *Status of Key Fish Stocks: Canadian Environmental Sustainability Indicators*. Government of Canada. Available at https://www.canada.ca/en/environment-climate-change/services/environmental-indicators/status-key-fish-stocks.html.

Fabrichnaya, Elena, and Guy Faulconbridge. 2023. "What and Where Are Russia's $300 Billion in Reserves Frozen in the West?" Reuters, December 28, 2023. Available at https://www.reuters.com/world/europe/what-where-are-russias-300-billion-reserves-frozen-west-2023-12-28/.

Far North Fiber. 2023. "Far North Fiber Project." Presented at Arctic Partnership Week 2023, Korea Maritime Institute (December 12, 2023).

Fredriksen, Benjamin. 2022. "Kabelmysteriene." *NRK*, June 26, 2022. Available at https://www.nrk.no/nordland/xl/russiske-tralere-krysset-kabler-i-vesteralen-og-svalbard-for-brudd-1.16007084.

Global Affairs Canada. 2024. "Canadian Sanctions Related to Russia." Government of Canada. Available at https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/russia-russie.aspx?lang=eng.

Goodman, Matthew P., and Matthew Wayland. 2022. *Securing Asia's Subsea Network: U.S. Interests and Strategic Options.* CSIS Brief, April 2022. Center for Strategic and International Studies. Available at https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options.

Gressel, Gustav. 2019. *Protecting Europe against Hybrid Threats*. European Council on Foreign Relations. Available at https://ecfr.eu/publication/protecting_europe_against_hybrid_threats/.

Grisé, Michelle, Alyssa Demus, Yuliya Shokh, et al. 2022. *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation*. RAND Corporation, August 18. Available at https://www.rand.org/pubs/research_reports/RRA198-8.html.

Hathaway, Melissa. 2019. *Patching Our Digital Future Is Unsustainable and Dangerous.* CIGI Papers no. 219 – June 2019. Centre for International Governance Innovation. Available at https://www.cigionline.org/static/documents/documents/Paper%20no.219web.pdf.

Hathaway, Melissa. 2020. "Why Digital Infrastructure Must Be Resilient." Opinion. Centre for International Governance Innovation, July 27, 2020. Available at https://www.cigionline.org/articles/why-digital-infrastructure-must-be-resilient/.

House of Commons. 2023. *A Secure and Sovereign Arctic: Report of the Standing Committee on National Defence*. 44th Parliament, 1st Session, April 2023. House of Commons of Canada. Available at https://www.ourcommons.ca/DocumentViewer/en/44-1/NDDN/report-3/.

Huebert, Rob. 2019. "The New Arctic Strategic Triangle Environment." Available at https://www.cgai.ca/breaking_the_ice_curtain.

Huebert, Rob. 2023. "China is on a relentless mission to control Canada's Arctic waters." Available at https://www.theglobeandmail.com/opinion/article-china-is-on-a-relentless-mission-to-control-canadas-arctic-waters/.

Humpert, Malte. 2023a. "Russia to Begin Year-Round Shipping on the Entire Northern Sea Route in 2024." *High North News*, May 24, 2023. Available at https://www.highnorthnews.com/en/russia-begin-year-round-shipping-entire-northern-sea-route-2024.

Humpert, Malte. 2023b. "China Pushes Northern Sea Route Transit Cargo to New Record." *High North News*, December 18, 2023. Available at https://www.highnorthnews.com/en/china-pushes-northern-sea-route-transit-cargo-new-record.

Hybrid Centre of Excellence [Hybrid CoE]. 2024. "Hybrid Threats as a Concept." European Centre of Excellence for Countering Hybrid Threats. Available at https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

Innovation, Science and Economic Development Canada. 2022. *High-Speed Access for All: Canada's Connectivity Strategy*. Government of Canada. Available at https://ised-isde.canada.ca/site/high-speed-internet-canada/en/canadas-connectivity-strategy/high-speed-access-all-canadas-connectivity-strategy.

Inuit Tapiriit Kanatami [ITK]. 2019. *Arctic and Northern Policy Framework, Inuit Nunangat*. ITK. Available at https://www.itk.ca/wp-content/uploads/2019/09/20190907-arctic-and-northern-policy-framework-inuit-nunangat-final-en.pdf.

Inuit Tapiriit Kanatami [ITK]. 2021. *The Digital Divide: Broadband Connectivity in Inuit Nunangat*. ITK Quarterly Research Briefing 3, Summer 2021. Available at https://www.itk.ca/wp-content/uploads/2021/08/ITK_Telecomms_English_08.pdf.

Justice Canada. 2017. *Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law). (S.C. 2017, c. 21)*. Government of Canada, Justice Laws Website. Available at https://laws.justice.gc.ca/eng/acts/j-2.3/FullText.html.

Kärmas, Mihkel. 2024. "Balticconnector Case More Sabotage than an Accident, Experts Say." *ERR News*, February 16, 2024. Available at https://news.err.ee/1609255413/balticconnector-case-more-sabotage-than-an-accident-experts-say.

Kativik Regional Government. 2023. *Kativik Regional Government and Its Fibre Optic Network Planned Between Kuujjuaq and Kawawachikamach*. Kativik Regional Government. Available at https://www.krg.ca/en-CA/assets/current-news/KRG_Community_Information.pdf.

Kativik Regional Government. 2024. "Kativik Regional Government Announces Activation of EAUFON-2 Fibre-Optic Link to Nunavik Communities on Hudson Strait." Phase 2 Announcement. Kativik Regional Government. Available at https://www.krg.ca/en-CA/EAUFON-2-announcment.

Kaushal, Sidharth. 2023. "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure." Commentary. *RUSI*, May 25, 2023. Available at https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.

Kirby, Paul. 2024. "Sweden Shuts Down Nord Stream Blasts Inquiry." *BBC News*, February 7, 2024. Available at https://www.bbc.com/news/world-europe-68225599 .

Kivalliq Inuit Association [KIA]. 2021. "Kivalliq Hydro-Fibre Link Takes Next Important Steps in its Development." KIA, May 4, 2021. Available at https://www.kivalliqinuit.ca/kivalliq-hydro-fibre-link-takes-next-important-steps-in-its-development.

Lackenbauer, P. Whitney, 2021. "Threats Through, To, and In the Arctic: A Canadian Perspective." In Duncan Depledge and P. Whitney Lackenbauer (eds.), *On Thin Ice? Perspectives on Arctic Security* (North American and Arctic Defence and Security Network): 35–47. Available at https://www.naadsn.ca/wp-content/uploads/2021/04/Depledge-Lackenbauer-On-Thin-Ice-final-upload.pdf.

Lentz, Stephen. 2015. "New applications for submarine cables." In *Undersea Fiber Communication Systems* 2016, pages 301-340.

Marsh Risk Management Research. 2014. *Arctic Shipping: Navigating the Risks and Opportunities.* Marsh and McLennan Companies. Available at https://www.safety4sea.com/wp-content/uploads/2014/09/pdf/Arctic_Shipping_Lanes_MRMR_August_2014_US.pdf.

Middleton, Alexandra, and Bjørn Rønning. 2024. "Arctic Cables: Digital Sovereignty and Geopolitics." *Global Outlook: Submarine Telecoms Forum* 134: 69–72. Available at https://issuu.com/subtelforum/docs/subtel_forum_134.

Mills, Walker D. 2023. "Maritime Sabotage: Protecting Europe's Soft Underbelly." *Irregular Warfare Initiative*, March 19, 2023. Available at https://irregularwarfare.org/articles/maritime-sabotage-protecting-europes-soft-underbelly/ .

Monaghan, Andrew, and Richard Connolly. 2023. *Moscow's Maritime Strategy: Establishing Russia as a Leading Seafaring State.* Keenan Cable 83, June 2023. Kennan Institute and Wilson Center. Available at https://www.wilsoncenter.org/publication/kennan-cable-no-83-moscows-maritime-strategy-establishing-russia-leading-seafaring?collection=32543.

National Defence Canada. 2017. *Strong, Secure, and Engaged: Canada's Defence Policy*. Government of Canada. Available at https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html.

National Defence Canada. 2024a. *Our North, Strong and Free: A Renewed Vision for Canada's Defence*. Government of Canada. Available at https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

National Defence Canada. 2024b. "Canadian Donations and Military Support to Ukraine." Government of Canada. Available at https://www.canada.ca/en/department-national-defence/campaigns/canadian-military-support-to-ukraine.html.

North Atlantic Treaty Organization [NATO]. 2023. "NATO Stands up Undersea Infrastructure Coordination Cell." NATO, February 15, 2023. Available at https://www.nato.int/cps/en/natolive/news_211919.htm.

Nunavut. 2022. "GN Reaches Milestone with Internet Fibre Link." Government of Nunavut. Available at https://www.gov.nu.ca/en/newsroom/gn-reaches-milestone-internet-fibre-link-2022-06-10.

Pelletier, Jeff. 2024. "Nunavut Seeks Money to Connect to Nunavik's Fibre Optic Network." *Nunatsiaq News*, March 8, 2024. Available at https://nunatsiaq.com/stories/article/nunavut-seeks-money-to-connect-to-nunaviks-fibre-optic-network/.

Pohl, Jens Hillebrand, Cordelia Buchanan Ponczek, and Mikael Wigell, 2023. "Strategic Capitalism: Implementing Economic Security Through Industrial Policy." In Alessandro Gili and Davide Tentori (eds.), *The Comeback of Industrial Policy: The Next Geopolitical Great Game* (Italian Institute for International Political Studies [ISPI]): 187–209. Available through https://www.ispionline.it/en/publication/the-comeback-of-industrial-policy-the-next-geopolitical-great-game-145627.

Quinn, Eilís. 2022. "$123.9 Million Additional Funding Announced for High-Speed Internet in Arctic Quebec." *Eye on the Arctic*, June 22, 2022. Radio Canada International [RCI]. Available at https://www.rcinet.ca/eye-on-the-arctic/2022/06/22/123-9-million-additional-funding-announced-for-high-speed-internet-in-arctic-quebec/.

Raine, John. 2019. "War or Peace? Understanding the Grey Zone." Online Analysis, April 3, 2019. International Institute for Strategic Studies [IISS]. Available at https://www.iiss.org/en/online-analysis/online-analysis/2019/04/understanding-the-grey-zone/.

Reuters. 2015. "U.S. Concerned by Russian Operations Near Undersea Cables: NY Times." Reuters, October 25, 2015. Available at https://www.reuters.com/article/idUSKCN0SK02G/.

Reuters. 2023. "Russian Foreign Ministry Summons Canadian Envoy Over Plane Confiscation." Reuters, June 15, 2023. Available at https://www.reuters.com/world/russian-foreign-ministry-summons-canadian-envoy-over-plane-confiscation-2023-06-15/ .

Reuters. 2024. "Nord Stream Insurers Deny Policies Covered War Risks in UK Lawsuit." Reuters, April 18, 2024. Available at https://www.reuters.com/world/europe/nord-stream-insurers-say-policies-did-not-cover-war-risks-kommersant-reports-2024-04-18/.

Rivard Piché, Gaëlle, and Bradley Sylvestre. 2023. *Vulnerabilities and Hybrid Threats in the Canadian Arctic: Resilience as Defence.* Hybrid CoE Working Paper 24: 6, 9 (May). Available at https://www.hybridcoe.fi/wp-content/uploads/2023/05/20230529-Hybrid-CoE-Working-Paper-24-Canadian-Arctic-WEB.pdf.

Royal Canadian Navy. 2024. "Harry DeWolf Class." Government of Canada. Available at https://www.canada.ca/en/navy/corporate/fleet-units/surface/harry-dewolf-class.html.

Russian Federation. 2021. "National Security Strategy of the Russian Federation." Russian Federation. Available at http://publication.pravo.gov.ru/Document/View/0001202107030001.

Russian Federation. 2022. *Maritime Doctrine of the Russian Federation*. Russia Maritime Studies Institute, July 31, 2022. Translated at https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Russia%20Maritime%20Studies%20Institute/20220731_ENG_RUS_Maritime_Doctrine_FINALtxt.pdf?sv=2017-04-17&sr=b&si=DNNFileManagerPolicy&sig=2zUFSaTUSPcOpQDBk%2FuCtVnb%2FDoy06Cbh0EI5tGpl2Y%3D.

Russian Federation. 2023a. *The Concept of the Foreign Policy of the Russian Federation*. Russian Federation, Ministry of Foreign Affairs, March 31, 2023. Available at https://mid.ru/en/foreign_policy/fundamental_documents/1860586/.

Russian Federation. 2023b. Об Основах государственной политики Российской Федерации в Артике на период до 2035 год ["About the Foundations of the State Politics of the Russian Federation in the Arctic for the Period until 2035"]. Released March 5, 2020; amended in 2023.

Senate of Canada. 2023. *Arctic Security Under Threat: Urgent Needs in a Changing Geopolitical and Environmental Landscape*. Report of the Standing Senate Committee on National Security, Defence and Veterans Affairs. Senate of Canada. Available at https://sencanada.ca/content/sen/committee/441/SECD/reports/2023-06-28_SECD_ArcticReport_e.pdf.

TASS. 2023. "Какие страны входят в список недружественных России стран." TASS, August 3, 2023. Available at https://tass.ru/info/18435143.

Tetsuo, Kotani, and Lynn Kuok. 2023. "Japan's Policy Towards Grey-Zone Activities in the Indo-Pacific." *Japan Memo* podcast. International Institute for Strategic Studies [IISS], October 16, 2023. Available at https://www.iiss.org/podcasts/japan-memo/2023/10/japans-policy-towards-grey-zone-activities-in-the-indo-pacific/.

Urbina, Ian. 2023. "The Crimes Behind the Seafood You Eat." *New Yorker*, October 9, 2023. Available at https://www.newyorker.com/magazine/2023/10/16/the-crimes-behind-the-seafood-you-eat.

White House. 2022. *National Strategy for the Arctic Region*. United States, White House. Available at https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Strategy-for-the-Arctic-Region.pdf.

Wright, Trevor. 2023. "CanArctic Signs MOU with Alaskan Company to Bring Fibre to Iqaluit." *Nunavut News* (April 17, 2023). Available at https://www.nunavutnews.com/news/canarctic-signs-mou-with-alaskan-company-to-bring-fibre-to-iqaluit-7282476.

Zelenaya, Olexandra. 2022. "Russia Slashes Environmental Protections as War Rages, Economic Crisis Looms." *Moscow Times*, July 1, 2022. Available at https://www.themoscowtimes.com/2022/06/25/russia-slashes-environmental-protections-as-war-rages-economic-crisis-looms-a77562.

Endnote

1 The paper's concentration on hybrid threats does not mean that active warfare is not a threat to submarine cables. Indeed, one should assume that in the case of an overt armed conflict an adversary would consider them priority targets, and a country whose infrastructure was damaged or destroyed by another might consider it an act of war. This paper will not explore that question but instead will concentrate on cases where the perpetrator is purposely attempting to remain anonymous (or nearly so), where the attack cannot quite be considered overt and open, and where lack of conclusive attribution of the attackers dampens the response of the country being attacked.

Appendix A: Hybrid threat definitions

What is a hybrid threat? There are a number of current definitions. The Hybrid Centre of Excellence in Finland defines hybrid threats as "harmful activities that are planned and carried out with malign intent" (Hybrid CoE 2024). It adds that "[t]hey aim to undermine a target, such as a state or an institution, through a variety of means" and that hybrid threats "describe a wide array of harmful activities with different goals, ranging from influence operations and interference all the way to hybrid warfare." The benefit of this definition is that it offers a wide perspective on the many different situations in which civilian and state resources can covertly sabotage another country's infrastructure.

Other institutions and experts speak of "grey zone" activities. For instance, John Raine of the International Institute of Strategic Studies (IISS) describes hybrid threats as "hostile actions" that are "clandestine or deniable," and fit into the "features of the difficult, new peace as much as the new warfare," as a "crude form of competition" (Raine 2019). His analysis is useful in that, if extended, it does not exclude covert sabotage during war, but still provides a way to discuss hostile acts that are not designed to tip countries into open warfare when they'd prefer to remain peaceful, albeit very competitive.

Finally, in Canadian public policy documents, the hybrid threat concept is discussed in 2017's *Strong, Secure, Engaged* defence policy. It devotes a paragraph to explaining threats that fall below the threshold of open warfare. But as Rivard Piché and Sylvestre point out, the concept has not had much traction in discussions of Arctic security, an observation reinforced by the 2024 Canadian defence policy, which generally mentions hybrid threats only obliquely and sparsely when referring to foreign influence and interference (National Defence Canada 2017 and 2024a; Rivard Piché and Sylvestre 2023).

> “Canada shall be the star towards which all men who love progress and freedom shall come.”
>
> **– Sir Wilfrid Laurier**

Critically acclaimed, award-winning Institute

The **Macdonald-Laurier Institute** focuses on the full range of issues that fall under Ottawa’s jurisdiction.

- Winner of the Sir Antony Fisher International Memorial Award (2011)
- Templeton Freedom Award for Special Achievement by a Young Institute (2012)
- Prospect Magazine Award for Best North America Social Think Tank (2018)
- Short-listed for the Templeton Freedom Award (2017)
- Cited by five present and former Canadian Prime Ministers, as well as by David Cameron, then British Prime Minister.
- *Hill Times* says **Brian Lee Crowley** is one of the 100 most influential people in Ottawa.
- *Wall Street Journal*, *Economist*, *Foreign Policy*, *Globe and Mail*, *National Post* and many other leading publications have quoted the Institute’s work.

WHERE YOU’VE SEEN US

CTV

cpac FOR THE RECORD

CORUS ENTERTAINMENT

CBC news

FP Foreign Policy

tvo

The Economist

WALL STREET JOURNAL

THE HILL TIMES

THE GLOBE AND MAIL
CANADA’S NATIONAL NEWSPAPER • FOUNDED 1844

NATIONAL POST

GOOD POLICY
is worth fighting for.

WHAT PEOPLE ARE SAYING ABOUT **MLI**

MLI has been active in the field of indigenous public policy, building a fine tradition of working with indigenous organizations, promoting indigenous thinkers and encouraging innovative, indigenous-led solutions to the challenges of 21st century Canada.

– The Honourable **Jody Wilson-Raybould**

I commend Brian Crowley and the team at **MLI** for your laudable work as one of the leading policy think tanks in our nation's capital. The Institute has distinguished itself as a thoughtful, empirically based and non-partisan contributor to our national public discourse.

– The Right Honourable **Stephen Harper**

May I congratulate **MLI** for a decade of exemplary leadership on national and international issues. Through high-quality research and analysis, **MLI** has made a significant contribution to Canadian public discourse and policy development. With the global resurgence of authoritarianism and illiberal populism, such work is as timely as it is important. I wish you continued success in the years to come.

– The Honourable **Irwin Cotler**

MACDONALD-LAURIER INSTITUTE

TRUE NORTH
IN CANADIAN PUBLIC POLICY

323 Chapel Street, Suite 300,
Ottawa, Ontario K1N 7Z2
613-482-8327
info@macdonaldlaurier.ca

macdonaldlaurier.ca