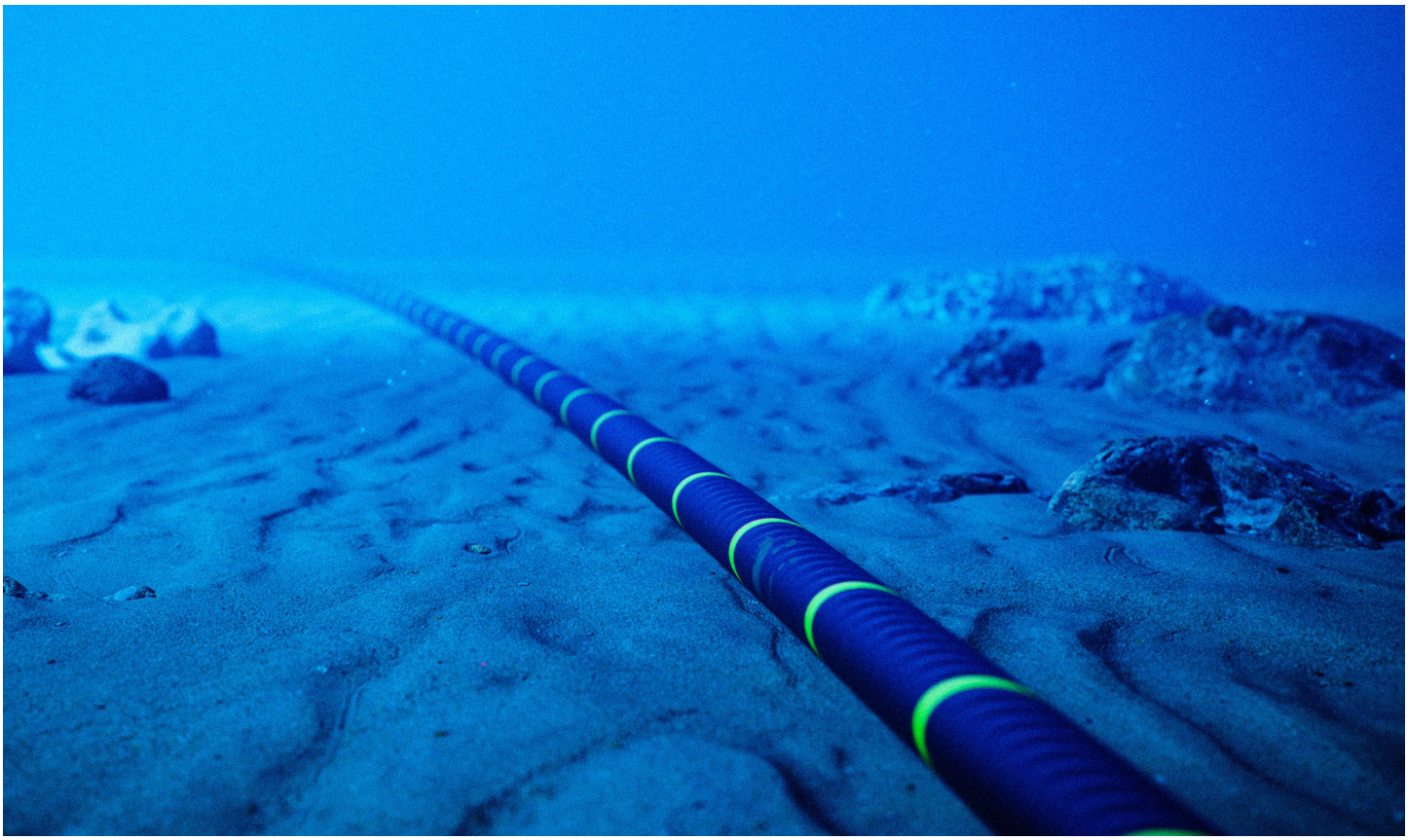
Report



May 2024

Protecting Undersea Infrastructure in the North American Arctic

Lessons from Incidents in the Baltic Sea and High North

By Heather A. Conley, Sophie Arts, Kristine Berzina, and Frida Rintakumpu

G | M | F
IDEAS LEADERSHIP HOPE

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

This publication was sponsored by the Homeland Defense Institute (HDI) and was finalized in May 2024. The views in this publication do not necessarily represent the views of the United State Air Force Academy, North American Aerospace Defense Command and United States Northern Command, the Department of Defense, or the United States government.

May 2024

Executive Summary

In response to recent incidents damaging undersea energy infrastructure and communication cables in the Baltic Sea and High North, NATO countries have intensified their focus on critical undersea infrastructure (CUI) protection on the national, bilateral, and multilateral levels.

Allies in the North American Arctic can build on important NATO initiatives but, given distances and the unique operating environment in this theater, the responsibility for protecting CUI assets in territorial waters will fall primarily to the United States, Canada, and the Kingdom of Denmark.

CUI in the North American Arctic is currently limited. But climate change, the green energy transition, and greater reliance on artificial intelligence (AI) will increase the demand and opportunity to expand communication cables and energy infrastructure in the region. At the same time, increased traffic and resource exploration heighten the vulnerability of these assets, especially to deliberate attack from Russia and the People's Republic of China (PRC). Both powers rely on dual-use assets that increase plausible deniability, and they continue to develop undersea warfare capabilities.

To enhance resilience and protect CUI in the North American Arctic, the United States and its NATO allies are strongly encouraged to:

- urgently upgrade US as well as NATO allies' situational awareness and presence in the air, space, and undersea domain, cooperating closely with the private sector
- prioritize and upgrade the role of NATO's Allied Maritime Command (MARCOM) to conduct CUI threat assessments and identify assets that are especially vulnerable due to their strategic importance, location, complicated ownership structure, or symbolic value
- expand US and NATO response options to counter hybrid threats and deter CUI attacks; consider establishing an additional maritime high-readiness force
- increase NATO's presence to protect and defend nearby assets during and after Russian and PRC naval maneuvers
- build on NATO's Digital Oceans Initiative to enhance and integrate unmanned systems and AI information processing tools into exercises and operations
- identify counterparts in other national governments to ensure quick and seamless information sharing following CUI incidents
- deepen public-private cooperation as well as government oversight over privately owned CUI to incentivize the private sector's CUI resilience (e.g. fortifying cables, integrating monitoring capabilities, and ensuring adequate repair capabilities)

- clarify responsibilities of CUI protection and defense across the civil, military, and private sectors, including the transition of responsibilities from the Department of Homeland Security to the Department of Defense in crisis situations

- train and exercise crisis decision-making processes with the involvement of all relevant actors (including the private sector and state and local authorities) on the national, bilateral (Canada and the Kingdom of Denmark), minilateral, and multilateral levels

- clarify and enhance legal frameworks to respond to CUI incidents in territorial and international waters, and share best practices across all sectors

- use pro-active strategic communication to outline legal and military authority in responding to CUI incidents, attributing attacks, and enhancing deterrence against future threats

May 2024

Introduction

A recent uptick in incidents of damaged gas pipelines and undersea communication cables in the Baltic Sea and High North has heightened concerns about critical infrastructure threats and raised awareness about the unique challenges of protecting and defending these assets in often highly trafficked waterways. They have also demonstrated the difficulty of responding to incidents quickly and adequately to make repairs, investigate and attribute the damage, and prosecute responsible parties. Even in cases where clear evidence points to the perpetrator, it often remains difficult to demonstrate intent. The involvement of commercial and nongovernmental actors complicates efforts to hold a nation-state accountable and often leaves only criminal processes to prosecute an actor suspected of damaging relevant infrastructure.

Ambiguity and plausible deniability make hybrid attacks attractive for adversaries such as Russia and the People's Republic of China (PRC), both of which use cyber operations and electronic warfare (EW). Such rivals may also engage in kinetic attacks against infrastructure by non-military means, especially outside other nations' territorial waters, to impose costs while minimizing the risk of escalation.

Critical undersea infrastructure (CUI), which encompasses energy infrastructure, including pipelines, liquefied natural gas (LNG) terminals, and offshore wind farms, as well as communication infrastructure and fiber-optic cables on the ocean floor, makes an easy target for attack. CUI that transits international waters and heavily trafficked areas is easily damaged (deliberately or accidentally) by as simple a tool as dragging an anchor. Kinetic attacks on undersea infrastructure, especially by non-military vessels, can often be passed off as unintentional.

Russia and the PRC have the civil-military and commercial capabilities to attack CUI. Both have also focused on hydrographic mapping and undersea technologies that allow them to identify targets. Other adversaries could follow their playbook—unilaterally or in coordination with Moscow and Beijing.

It can be challenging to protect CUI in international waters when any commercial vessel can pose a threat, and developing appropriate responses to undersea gray zone threats conducted by civil or commercial players is difficult. This complicates deterrence against hybrid threats, an issue that NATO and its member states are increasingly grappling with. Short of more effective deterrence against undersea threats, detection must be the highest priority. It also serves as the basis for any further civil-military action to deny and defend against attacks, and develop other criminal, diplomatic, and military response options.

This report looks at recent incidents resulting in damage to undersea infrastructure in the Baltic Sea and High North to examine vulnerabilities; assess current national, bilateral, minilateral, and multilateral efforts to enhance resilience, defense, and deterrence against CUI threats; and to draw lessons for the North American Arctic. The research and recommendations are based on open-source literature, strategy documents, and interviews with government and military stakeholders, as well as with experts, in the United States, Canada, and Northern Europe.

1. Case Studies: Recent Undersea Infrastructure Incidents

Since 2022, three prominent incidents resulting in damage to undersea infrastructure have captured policymakers' and experts' attention and highlighted the threat potential against CUI in a period of heightened tensions with Russia and the PRC. Whether or not deliberate human interference caused the damage, all three incident sites—a fiber optic cable connecting Norway and the Norwegian archipelago Svalbard, the Nord Stream pipelines connecting Russia and Germany, and the Balticconnector pipeline between Estonia and Finland—bear special symbolic or strategic significance that could have made them appealing targets for NATO adversaries.

1.1. 2022 Svalbardfiberen Incident

On January 7, 2022, one of two subsea fiber optic cable connecting the Svalbard Satellite Station with mainland Norway was severed[1] between 130 and 230 kilometers (70 and 124 nautical miles) from Longyearbyen. At the site of the break, outside the territorial waters around Svalbard, but within its Fisheries Protection Zone (FPZ), at an approximate depth of 700 meters (2300 feet), the cable was buried, as is standard in waters shallower than 1500 meters (4921 feet). The cable, Svalbardfiberen, which is owned and maintained by state-owned Space Norway,[2] transmits large volumes of data from the satellite station SvalSat to mainland Norway. According to journalist Malte Humpert, the "station is of crucial importance as it is one of only two in the world which can communicate with satellites in polar orbits".[3]

Since the second cable connecting Svalbard with Norway remained intact and the affected cable was only partially damaged, resulting in the loss of power but not connectivity, the incident did not cause a total system failure but only in a "temporary lack of redundancy".[4] Eleven days after the incident, on January 18, 2022, data traffic was restored,[5] by connecting the damaged cable to an alternate power source.

This helped Space Norway bridge the time until it could repair the cable, a process that took nearly 18 months since cable repair ships and operators are limited in number and not readily available. After the incident, Norway joined the Atlantic Private Maintenance Agreement to ensure faster access to maintenance support.

Investigation

The Norwegian police launched an investigation to determine what caused the cable damage. Norwegian officials initially blamed the incident on human interference, but no conclusive evidence of this has been made public.[6] On March 21, 2022, the police dismissed the incident due to lack of evidence, arguing a criminal offense could not be confirmed.[7]

According to a January 2023 paper by Norwegian think tank NUPI, "Norwegian media outlets were quick to indulge in theories about intentional, man-made damage, seeing the break in light of the tense political situation between Russia and NATO-states, and the fact that Russian trawlers navigated over the cable in the time before the connection was broken."[8] This incident followed less than a year after the subsea cable to the Lofoten-Vesterålen (LoVe) Ocean Observatory in northern Norway was ruptured. In this earlier case, part of the 4.3 kilometer-long (2.7 miles) stretch of cable missing from the site was later discovered 11 kilometers (6.8 miles) away, leading

to the assessment that "[m]ost likely a vessel [had] pulled the cable out of position".[9] According to High North News, the cable damaged in 2021 was primarily used for "marine monitoring, but it also collected intelligence information for the Norwegian Armed Forces".[10] The damage of two Norwegian-owned and operated undersea cables in such short sequence fueled speculation about the cause and the potential involvement of Russia, although no connection was ever established.

Significance of Svalbard

Svalbard holds an important symbolic and geostrategic position that could make it a target. The archipelago, located fewer than 1300 miles north of Norway, and 800 miles from Russia's Kola peninsula, could play a critical role in controlling the Kremlin's strategic submarine access to the North Atlantic. The Svalbard Treaty of 1920 confirmed Norwegian sovereignty over the archipelago, established Svalbard as a free economic zone, and precluded any military use of the island for "warlike purposes".[11] Russia has, without grounds, occasionally questioned Norway's adherence to this last principle in response to peacetime activities of the Norwegian coast guard and navy around Svalbard. Norway and Russia also have diverging views on the former's sovereign rights within the FPZ around Svalbard, which has led to confrontations.[12]

Russians constitute the second-largest population group after Norwegians in Svalbard and, while the Soviet Union unconditionally recognized Norway's sovereignty in 1924, it "made several attempts to gain special status on Svalbard in the aftermath of World War I and later in 1944".[13] Russia maintains a presence in Barentsburg and recently announced that it would develop, with the BRICS+ countries, its own science station in Pyramiden. These activities are not prohibited by the Svalbard treaty as long as they do not support military activities.

Broader Policy Response

Following the Svalbardfiberen incident, Svalbard's governor and its emergency preparedness council conducted a risk assessment and updated emergency preparedness plans for the archipelago.[14] As NUPI's brief elaborates, this included scenario planning in case Svalbard's second undersea cable were damaged, which would result in a loss of civil connectivity and stop dataflow between SvalSat and the mainland.[15] While satellite phone communication would still be possible, a failure of both cables would affect commercial air traffic. The impact on military and emergency services would be limited, and they could continue to some extent.

Plans for the construction of another undersea cable between Svalbard and a mainland site using an entirely different route were already under discussion before the incident. The current cables, installed in 2003 and funded partially by US National Oceanic and Atmospheric Administration (NOAA), NASA, and Kongsberg Satellite Services (KSSAT), have an expected life expectancy until at least 2028, when the new cables should be in place. While the old cables remain intact, the new ones offer additional redundancy.

After the sabotage of the Nord Stream pipelines in October 2022 (discussed below), Svalbard's governor indicated that the Svalbardfiberen incident was reassessed but "no connection between the damage to the gas pipelines and the Svalbard fiber has been proven."[16]

1.2. 2022 Nord Stream Sabotage Case

On September 26, 2022, a series of underwater explosions damaged the Nord Stream 1 and Nord Stream 2 natural gas pipelines built to transport natural gas from Russia to Germany via the Baltic Sea. At the time of the incidents, Russia had stopped selling to Europe through the pipeline, but it remained filled with gas.[17] Russia's majority state-owned gas company, Gazprom, is the majority shareholder of both projects. German energy companies hold the second-largest stakes. Over the course of four days, four leaks were identified in the pipelines at a depth of approximately 80 meters (260 feet) on the Baltic Sea floor within Denmark's and Sweden's Exclusive Economic Zone (EEZ).

Investigation

Denmark and Sweden launched police investigations into the incidents in their respective EEZs. Since the leaks were located outside both countries' territorial waters, however, the incidents were not deemed attacks against either country. The incidents also did not occur within Germany's EEZ, but that country's authorities launched their own investigation. The leaks affected German infrastructure previously deemed critical to the national energy supply.

Although Germany originally proposed a joint investigation team with Denmark and Sweden,[18] all three countries ultimately acted on their own. According to media reports, Swedish and Danish concerns about information sharing featured into the decision. Differences among the organizational structures of the three countries' police forces may have complicated coordination. Denmark, Germany, and Sweden rebuffed Russian demands to join their respective investigations.

The Swedish effort was led by the Swedish Security Service, with assistance from several other agencies, including the Swedish coast guard, the Swedish armed forces, and the Swedish Police Authority.[19] The Danish investigation was led by the Danish National Police in cooperation with the Danish intelligence services. In Germany, the Federal Criminal Police Office and the Federal Police were tasked with the investigation. The German navy assisted with the process.[20]

On November 18, 2022, the Swedish Security Service informed the public that the "investigation shows that the pipelines have been subject to gross sabotage" and that "the extensive damage to the gas pipelines [resulted] from detonations [that were] thoroughly documented."[21]

In January 2023, German investigators searched a rental sailboat suspected of ties to the incident and found traces of explosives.[22] An investigation into the crew, who were allegedly carrying fake Ukrainian passports, has led authorities to follow inconclusive leads indicating the potential involvement of Ukrainian nationals.[23] One month before the incidents, Dutch intelligence warned of a pro-Ukrainian sabotage plot against the pipeline.[24] Many experts and officials have questioned if the explosives could have been successfully deployed from the vessel in question and have discussed the possibility of a false-flag operation.

In late April 2023, a Danish newspaper reported that the Danish military had photographed a Russian submarine rescue ship, the SS-750, which carries a mini-submarine, in the Baltic Sea off Bornholm four days before the attack on the pipelines.[25]

Unlike the Svalbardfiberen incident, the Nord Stream leaks were clearly caused by human interference. The use of explosives means that the incidents were a result of deliberate sabotage. Nonetheless, Sweden and Denmark closed their investigations in February 2024 without naming a perpetrator. The German investigation remains ongoing.

Significance of the Nord Stream pipeline projects

Both Nord Stream pipeline projects were highly controversial and criticized, especially by central and eastern European countries. Some objected because the pipelines circumvented their territories and deprived them of transit fees. The United States and non-transit countries such as the Baltic States opposed the pipelines for strategic reasons: The pipelines solidified Germany's bilateral ties to Russia and increased Germany's dependence on Russia for natural gas, strengthening Moscow's political leverage over Europe's largest country.

Russia proposed Nord Stream 2, and German politicians backed the project despite US and European concerns after the Kremlin invaded Crimea in 2014 and despite the Kremlin's willingness to halt gas flows to pressure Ukraine. The pipeline was finished, but its certification process was suspended in February 2022 following Russia's full-scale invasion of Ukraine. In September of that year, Russia indefinitely stopped gas supplies to Europe through the Nord Stream 1 pipeline. It cited equipment issues due to Western sanctions as the reason. Nord Stream 2 subsequently became a symbol of Germany's failed energy and Russia policies.

Broader Policy Response

Beyond demonstrating the risks of energy dependence on Russia, the Nord Stream incidents served as a wake-up call to many European governments since they highlighted the vulnerability of CUI and the need to enhance national and multinational efforts to protect undersea assets, including energy infrastructure.

In the immediate aftermath, NATO's European allies provided naval support to protect the sites of the incident and other critical undersea assets. The allies have since "stepped up air and naval patrols and increased presence in the Baltic and North Seas".[26]

Given Europe's reliance on Norway's natural gas following Russia's 2022 invasion, protecting that country's energy infrastructure also became a priority. Oslo deployed the Norwegian Home Guard, a rapid mobilization force, to protect energy infrastructure.[27] And Norway's state-owned GASSCO AC, which oversees all gas flows to Europe and operates 99% of the pipelines connected to the country, updated, exercised, and operationalized its emergency preparedness plans, and intensified civil-military cooperation, especially with the country's navy and with relevant domestic and European agencies and administrations. The aim was to enhance surveillance, optimize monitoring and response processes, and clarify responsibilities.

The incidents also led other countries to reassess and enhance national emergency preparedness, delineate civil and military roles and responsibilities for critical energy and communications infrastructure protection (including against kinetic threats), and clarify investigation processes. In addition, the events gave new momentum to bilateral, minilateral, and multilateral efforts that enhance critical infrastructure resilience and protection.

1.3. 2023 Damage of the Balticconnector Pipeline and Communication Cables

In the early morning hours of Sunday, October 8, 2023, the Balticconnector offshore gas pipeline connecting Finland and Estonia, and operated by Gasgrid Finland and Estonian Elering, was damaged. Finnish state-owned company Balticconnector and Estonian Eesti Gaas, the largest private energy company in the Finnish-Baltic region, hold equal shares in the project. Two telecommunications cables were also damaged in the incident—one cable between Sweden and Estonia in the afternoon of October 7, and one between Finland and Estonia on October 8. The privately owned data cables supported only civilian systems and were not of military or strategic importance. The gas pipeline damage occurred in the Finnish EEZ, and the data cable incidents in the Swedish and Estonian EEZs. Two vessels were in the vicinity of the pipeline and cables when the damage occurred: a Chinese container ship, the Newnew Polar Bear, flying the flag of Hong Kong, and a Russian-flagged nuclear-powered cargo vessel, the Sevmorput. In international media coverage, Hamas' attack on Israel on October 7 overshadowed the incidents.

Investigation

Balticconnector operators Gasgrid Finland and Elering observed an unusual drop in pressure in the pipeline in the early morning hours of October 8, 2023, and took the pipeline offline. It was later confirmed that damage occurred at two locations in Finland's EEZ.

The drop in pressure sparked an immediate investigation. Since the damage occurred in its EEZ, Finland led the investigation, in close coordination with Estonia. Finland's National Bureau of Investigation (KRP), operating under the direction of the Ministry of the Interior, was put in charge of investigating the incident. KRP was supported by the Finnish Border Guard, the Finnish Defence Forces, and other authorities. Due to the two countries' close relations and established communication channels, cooperation on the investigation was smooth.

Estonia and Sweden, working closely with the private-sector operators, took the lead in coordinating the government responses to the cable incidents in their respective EEZs. In Estonia, prosecutors from the internal police and the security police oversaw the investigation. The country's Ministry of Climate, supporting Finnish authorities, was responsible for the pipeline investigation, and the Ministry of Economic Affairs and Communications was responsible for the cable investigation. Coordination between Finland's and Estonia's navies also started immediately after the incidents, and the governments of both countries used a variety of channels to alert NATO allies. Some of those partners sent surveillance ships and patrol aircraft. However, questions about legal authority, given the vessel's location in international waters and the connection of the Newnew Polar Bear to the incident, stopped officials in Estonia, Finland, and Sweden from boarding the vessel.

While establishing attribution for the incidents was challenging due to their ambiguous nature, technical identification of the causes was possible several days later. Finnish authorities confirmed on October 11 that an

anchor found next to the pipeline belonged to the Newnew Polar Bear. KRP then announced on October 19 that it had completed its on-site investigation into the pipeline damage and that it had been caused by an external mechanical force. On October 25, KRP confirmed that Newnew Polar Bear was suspected of damaging the pipeline and cables by dragging an anchor along the seabed.

In November 2023, Finland and Estonia requested the PRC's cooperation in the investigation. Both European countries have confirmed that Beijing has indicated its willingness to cooperate with the investigation. In February 2014, Finnish Foreign Minister Elina Valtonen said that the investigation has moved forward, but she declined to disclose details. Repairs on the Balticconnector gas pipeline were completed in April 2024, and the gas pipeline is again functional.

Symbolic Implications of the Incidents

The Balticconnector pipeline commenced its operations in 2020 with the aim of ending Finland's gas isolation. The pipeline connected the country to the rest of Europe, thereby enhancing regional security by increasing gas supplies. It has been Finland's only natural gas conduit since Russian imports were stopped in May 2022. Nonetheless, the pipeline damage did not severely impact Finland since little gas is used for household energy consumption. In Finland, industry is the main gas consumer.

At the time of the damage to the pipeline and cables, the Newnew Polar Bear was completing its maiden journey across the Northern Sea Route (NSR) from Qingdao to St. Petersburg and back. According to the NSR General Administration, Torgmoll, a Russian-registered company with offices in the PRC, granted the vessel permission to transit the NSR. At the time of the incident, the Sevmorput, the Russian-flagged nuclear-powered cargo vessel, accompanied the Newnew Polar Bear. Although both ships were investigated due to their proximity to the damage sites, the PRC vessel entered the spotlight after its anchor was recovered. Many experts believe the distance and speed at which the Newnew Polar Bear dragged its anchor, coupled with its lack of communication with authorities in the area, make it extremely unlikely that this was an accident. Speculation about possible PRC-Russia collusion has arisen.

Broader Policy Response

By October 2023, NATO allies had learned important lessons, especially from the Nord Stream incidents. They also improved information sharing and civil-military coordination processes, which enabled quick bilateral (Finland-Estonia and Estonia-Sweden) and NATO responses in the Balticconnector case. After the incidents, a Norwegian navy vessel shadowed the Newnew Polar Bear for approximately 15 hours as it passed the western Coast of Norway on its voyage back toward the NSR.[28] For its part, NATO increased patrols in the Baltic Sea by conducting "additional surveillance and reconnaissance flights, including with maritime patrol aircraft, NATO AWACS planes, and drones" and dispatched a "fleet of four NATO minehunters".[29]

Moreover, Finland and Estonia drew on their historically high levels of military and societal readiness and on their comprehensive approach to security. This enabled a quick national response across the civil-military sector.

Finland, Estonia, and NATO also closely coordinated on strategic communication after the incident, an especially important development given that attribution (technical and political) plays an important role in defining countermeasures and as a tool of deterrence. In the case of the Balticconnector, Finnish authorities carefully avoided blaming a specific actor or country. As the investigation progressed, identifying the cause of the damage still did not lead to any political attribution. But by identifying the cause, Finnish authorities could control the narrative around the incident. They were able to provide factual information, and hamper alternative, dis- and misinformation campaigns, by communicating investigation findings to the public through press conferences and government press releases.

In Estonia, the incident resulted in initiatives to strengthen oversight of critical, private-sector infrastructure to ensure that the government had clear information about the location, function, and operational structure of assets. Clear protocol and reporting structures were also established. Lastly, the incidents led Estonia and other US allies in the region to assess repair capabilities in the Baltic Sea, which are limited, and to plan for incidents affecting several cables that could impact regional communication functionality. The EU and NATO also conducted meetings to assess the implications of the incidents and devise clearer information sharing processes, including those regarding civilian infrastructure deemed critical to NATO.

2. The Actors Involved

The Newnew Polar Bear and Nord Stream cases highlighted the complicated nature of undersea infrastructure incidents, which often affect several private entities and nation-states. Investigations and responses, therefore, also require close collaboration with multiple states' authorities and commercial entities.

The green transition, which relies in large part on offshore energy production, expands the number of targets for adversaries. This has led to growing efforts to enhance collaboration and planning across NATO allies' public-private and civil-military sectors on a national, bilateral, and minilateral level.

2.1. The Role of Nation-States, and Bilateral and Minilateral Efforts

In response to recent incidents, NATO countries have intensified their focus on undersea infrastructure protection. Individual allies are expanding their ability to monitor and protect CUI through new national policies, initiatives, and capability investments. According to a Center for Strategic and International Studies (CSIS) report, France, for instance, "announced a new seabed warfare strategy and investments in ocean floor defense, and the UK has set up a Centre for Seabed Mapping and earmarked two new Multi-Role Ocean Surveillance (MROS) vessels to serve primarily as subsea protection ships".[30]

Moreover, bilateral and minilateral formats are gaining traction. In April 2024, six countries bordering the North Sea—Belgium, Denmark, Germany, the Netherlands, Norway, and the United Kingdom—signed an agreement to protect CUI in that body of water from foreign sabotage and attack, and to share information and best practices. The pact is of critical importance as the North Sea increasingly turns into "a hub for critical infrastructure", connecting European countries through power cables, gas pipes and telecommunications links, thus increasing "cross-border interdependence" and heightening "risk of sabotage and unwanted attention from hostile actors", as Denmark's Ministry of Climate, Energy and Utilities has emphasized.[31]

In addition, the UK-led Joint Expeditionary Force (JEF) announced in 2023 that it would "accelerate cooperation … to detect, deter and respond to threats against … critical undersea and offshore infrastructure, reassure Allies and demonstrate collective commitment to the security and stability of Northern Europe; all in full alignment with NATO".[32] The United Kingdom and Norway have also enhanced their bilateral cooperation though a strategic partnership on undersea threats. They launched in May 2023 an effort[33] "to collaborate on protecting critical energy infrastructure, anti-submarine warfare and subsea protection" and to "enhance North Atlantic Security".[34]

2.2. The Role of Multilateral Organizations

NATO plays a critical role in protecting CUI and, per alliance policy, attacks on undersea assets of an ally may result in an Article 5 response, triggering members' collective defense commitment. Even short of any decision by the North Atlantic Council (NAC), NATO's Supreme Allied Commander Europe (SACEUR) has the power to activate forces to respond quickly and enhance the alliance's presence in case of a crisis or suspected attack on critical infrastructure. The NATO Response Force (NRF) can be activated within 10 days, and some elements of its "spearhead force", the Very High Readiness Joint Task Force (VJTF), which includes a multinational land brigade,

"are ready to move within two to three days". The NRF includes land, air, maritime, and Special Operations Forces (SOF). The standing NATO Maritime Groups (SNMGs) and the Standing NATO Mine Countermeasures Groups (SNMCMGs) constitute the maritime element.[35]

Following recent incidents, NATO has enhanced its coordinating role on critical infrastructure protection. In addition to leveraging the work of existing institutions, including the NATO Energy Security Center of Excellence founded in 2012, the alliance has established several new centers focusing on threats to CUI. The Critical Undersea Infrastructure Coordination Cell at NATO's headquarters in Brussels was formed in February 2023. The center facilitates "engagement with industry and brings key military and civilian stakeholders together, shares best practices, leverages [innovative] technologies and boosts the security of Allied undersea infrastructure", as Secretary General Jens Stoltenberg has emphasized.[36]

Following NATO's Vilnius summit in July 2023, member states established the Maritime Centre for the Security of Critical Underwater Infrastructure within NATO's Allied Maritime Command (MARCOM) in the United Kingdom. In October 2023, NATO conducted Exercise Dynamic Messenger 23 off the coast of Sesimbra and Tróia, Portugal, which included NATO allies, then-partner Sweden, and industry partners. Together, they tested "the ability of the Alliance to integrate autonomous vehicles into its operations".[37] According to NATO, the results of this exercise, which was the first with a specific focus on CUI, "will inform the incorporation of new technologies into the development of future NATO doctrine, tactics and procedures".[38] The exercise tested autonomous intelligence, surveillance, and reconnaissance (ISR) capabilities, addressed the "complex legal, political and technical environments surrounding the overall protection of CUI", and "provided the starting point for refining the operational command and control processes needed to carry out such tasks".[39]

NATO also launched its Digital Ocean Initiative in 2023 to enhance maritime situational awareness to protect CUI through "persistent maritime surveillance and innovative anti-submarine warfare capabilities".[40] In April 2024, the Digital Ocean Industry Symposium brought together more than 200 industry representatives and officials to assess industry's role in developing relevant capabilities, including undersea and space-based sensors, and avenues for quick and effective data processing and sharing across the alliance.[41]

NATO is now primarily focused on coordinating and synergizing allied responses to CUI incidents. Its ambition is the "creation of a global scale network of sensors, from seabed to space, to better predict, identify, classify and combat threats. It envisages maritime domain awareness, subsea sensors, unmanned surface vessels, drones and satellites, and exploits AI, big data, and autonomous systems, alongside conventional assets".[42] This will help allies to identify responsible parties and to reduce plausible deniability and thereby disincentivize future large-scale attacks.

The EU, in coordination with NATO, has also played an important role in preparing its member states to protect CUI. In March 2023, the EU-NATO Task Force on Resilience of Critical Infrastructure was launched. A European Commission report released in June 2023, ahead of the Vilnius summit, distinguishes "four key sectors of cross-cutting importance: energy, transport, digital infrastructure and space".[43] It also recommends "[s]trengthening the Structured Dialogue on Resilience and the Structured Dialogue on Military Mobility" especially "between NATO's International Military Staff and the EU Military Staff".

Even before the establishment of the EU-NATO task force, the EU's Directive on the Resilience of Critical Entities, which aims to protect such entities against "a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage, as well as public health emergencies", came into effect.[44] EU member states are consequently required to conduct regular risk assessments "to identify entities that are considered critical or vital for society and the economy" and support those entities by enhancing their resilience against threats.[45] The directive gives EU members states until October 17, 2024 to adopt the necessary national legislation. NATO should conduct its own complementary effort to develop a comprehensive list of CUI that is critical to alliance operations and security, and incentivize measures that enhance the resilience of these assets.

3. Lessons for the US and North American Arctic

NATO efforts have implications for the Arctic as seven of the eight Arctic Council states are now alliance members. Initiatives on CUI protection will yield important lessons for the region, especially regarding implementing processes to enhance situational awareness and information sharing. They will also help shape coordination of best practices and the establishment of better communication channels across the alliance to work more closely with civil entities and the private sector. But given the Arctic's unique operating environment, these measures will often be challenging to implement.

Still, initiatives strengthening defense and deterrence against hybrid threats will be critical. The race for Arctic resources and access is taking strategic competition in the region to a new level, with Russia and the PRC increasingly emboldened to aggressively pursue their national interests. The growing strategic alliance between Moscow and Beijing is allowing the latter to establish a greater Arctic presence. The two countries have stepped up their economic, scientific, technological, and civil-military cooperation. They have conducted joint naval maneuvers and, in 2023, signed a memorandum of understanding (MoU) for joint maritime law enforcement along the NSR. A growing commercial and military presence in the Arctic could threaten NATO allies' CUI, especially given Moscow's and Beijing's focus on hydrographic mapping and the development of undersea assets. Existing and planned Arctic CUI projects are currently limited, but as melting sea ice makes the Arctic Ocean more accessible, opportunities for hydrocarbon exploration and for expanded communication infrastructure are growing. According to US geological assessments, the Arctic continental shelves "may constitute the geographically largest unexplored prospective area for petroleum remaining on Earth",[46] which raises the potential for oil and gas extraction despite the associated environmental risks and high cost. The focus on critical seabed minerals, which are vital for defense and industrial supply chains, including those needed for the green transition, is also growing. In January 2024, Norway's parliament voted to allow commercial deep-sea mining in the country's continental shelf.[47] The PRC is using its leverage in the International Seabed Authority (ISA) to shape international law and position itself to gain mining rights for commercial deep-seabed mining in international waters.[48]

At the same time, there will be greater demand to establish data networks among Europe, North America, and Asia. Undersea communication cables routed through the Arctic can significantly shorten distances and accelerate data traffic.[49] Growing reliance on the Internet of Things and artificial intelligence (AI) demand greater data throughput and speed. However, seabed mining might pose a threat to CUI and will likely impact where cables may be laid. Several undersea cable projects to transit the Arctic Ocean are in the planning stage. Alaskan Far North Digital LLC is partnering with Finland's Cinia Ltd. and Japan's Arteria Networks Corp. to build a long-haul submarine fiber cable from Japan to Norway, Finland, and Ireland that would then link to Alaska and the Canadian Arctic. It is projected to be operational by the end of 2026. Quintillion Subsea Operations LLC, which already operates a 1,180-mile subsea cable along the Alaskan coast, is also planning separate cables connecting the US state to Asia and Canada to Europe.[50]

The harsh weather and environmental conditions in the North American Arctic, which is colder than its European counterpart, complicate access and infrastructure development. More infrastructure and connectivity are urgently needed to enhance civilian living conditions in remote Arctic communities and to support military operations. Situational awareness is lacking due to limited satellite coverage. Moreover, high-latitude challenges, higher levels

of charged particles, and electromagnetic disruptions complicate remote sensing and pose challenges to positioning and navigation. This also impacts situational awareness.

Far North Digital advertises the Far North Fiber Route project, arguing that the "Arctic route avoids critical global choke points and political risks". The company highlights "lower volume of ship traffic versus conventional routes within or crossing vessel lanes".[51] While this is currently true, the relative lack of situational awareness could make the cables more vulnerable to deliberate attacks from Russia and the PRC. Moreover, shifting ice plates and other geological events can damage cables. Challenges in access to the North American Arctic can be a boon because undersea infrastructure is more insulated from commercial traffic and harder to reach by adversaries. But the location also makes it difficult to repair damaged cables.

This makes it even more important for Arctic CUI assets to be built with resilience and redundancy in mind. Moreover, protection of cables and energy infrastructure in the region will require specific Arctic-capable assets to support situational awareness from space, in the air, and in the undersea domain, and to defend CUIs against threats. These assets are not readily available across NATO, and it will likely fall to individual North American and Nordic allies to field them. Unlike in the Baltic Sea or the North Sea, European NATO allies will not be able to quickly send naval reinforcements to the North American Arctic. This means that the responsibility of protecting CUI in the region will primarily fall to North American countries, with each focusing on its own territorial waters. This increases CUI vulnerabilities in international waters.

In addition to fielding capabilities to enhance situational awareness, defense, and deterrence, the United States, Canada, and the Nordic allies must ensure that they have access to vessels that can make difficult repairs. Currently, only four companies operate and maintain submarine cables internationally: US SubCom, Japan's NEC Corporation, France's Alcatel Submarine Networks, and the PRC's HMN Tech.[52] Alcatel Submarine Networks operates a cable fleet of seven vessels.[53] SubCom operates six cable-laying ships.[54] The US Navy has one vessel to fill this function, the USNS Zeus. None of these vessels is specifically developed for Arctic operations, and their use will be seasonally dependent. In 2023, repairs to Quintillion's submarine cable along the Alaskan coast took two months in the summer (the cable was cut in mid-June and repaired on September 19).[55] Access will be more difficult for cables further offshore.

3.1. Streamlining US Civil-Military Cooperation to Protect CUI

As additional critical infrastructure in the Arctic is developed, its vulnerability will grow. More assets means more resources are needed to defend, maintain and repair them. This will require a greater role and more coordinated operations across US federal, state, and local agencies, the Joint Force, and the private sector to adequately defend, deter, and respond to potential incidents.

National, bilateral, and multilateral responses to incidents of CUI damage in the Baltic Sea and High North have demonstrated the importance of having maximum clarity on roles, responsibilities, and a streamlined command structure across the civil-military-private spectrum to ensure CUI resilience and to deter and defend against malign hybrid and kinetic activities. Clear structures and open communication channels are critical within national governments and with international partners and institutions.

The United States is making important strides to reach that goal, especially on prevention and risk management. The National Security Memorandum (NSM) on Critical Infrastructure Security and Resilience, published in April 2024, "[e]mpowers the Department of Homeland Security to lead a whole-of-government effort to secure U.S. critical infrastructure, with [the Cybersecurity and Infrastructure Security Agency (CISA)] acting as the National Coordinator for the Security and Resilience of U.S. Critical Infrastructure".[56] The NSM replaces Presidential Policy Directive 21 (PPD-21), issued in 2013, which sought to clarify "the critical infrastructure-related functions, roles, and responsibilities across the Federal Government". PPD-21 attempted to enhance "overall coordination and collaboration" with the Secretary of Homeland Security providing "strategic guidance" and other departments—led by the Department of Defense (DoD), the Department of Justice, the Department of Interior, the Department of Commerce, and the intelligence community (IC)—providing the most important support functions.[57]

The NSM builds on this and emphasizes "[c]lose and continuous coordination among the Department of Homeland Security (DHS), [Sector Risk Management Agencies (SRMAs)], and other relevant Federal departments and agencies, to include law enforcement and the IC" and "collaboration with owners and operators; State, local, Tribal, and territorial governments; international partners; and other entities". The document highlights that "most of the Nation's critical infrastructure is owned and operated by non-Federal entities, which are primarily responsible for individual assets' security and resilience."[58]

The NSM allocates responsibility to coordinate and deconflict responsibilities across the federal government to the Federal Senior Leadership Council (FSLC), which is co-chaired by the CISA director, "and will be informed by engagement with the National Security Council". It places the lead in engaging with foreign governments, international organizations, and partners with the Department of State and has the DoD "lead the evaluation of the risk to and prioritization of mitigations for sector-specific [Defense Critical Infrastructure], in coordination with the National Coordinator, the IC, and relevant SRMAs".[59]

It also allocates "authority to assess security risks to the Marine Transportation System and other modes of transportation, develop security measures and regulations, and seek or ensure compliance with those measures and regulations" to the Transportation Security Administration administrator and the United States Coast Guard commandant.[60] Beyond this, the NSM specifically mentions the role of international partners and allies to help "[s]trengthen the security and resilience of critical infrastructure" and "to build situational awareness and capacity, facilitate operational collaboration, promote effective infrastructure risk management globally, and develop and promote international security and resilience recommendations."[61]

The document also emphasizes that, "[a]s part of its national defense mission, DoD supports defense of critical infrastructure".[62] But from open-source literature, it is unclear when and how the transition of responsibilities in the case of a crisis would be initiated or what entities within the DoD would take the lead, and which would serve supporting functions to field forces and assets. This question poses a particular challenge in the North American Arctic and Alaska, given gaps in resourcing and the doctrine to streamline the command structure in this theater. DHS cooperation with infrastructure owners and operators, and with other agencies, will be critical for CUI protection and to advance situational awareness in the North American Arctic. In the case of a crisis or CUI incident involving a potential foreign threat, the state of Alaska, USNORTHCOM, the US Navy, and special operation forces would likely play an important role, with support from the US Coast Guard and local state agencies.

4. The Path Forward for the United States and its Allies in the Arctic

Recent incidents involving undersea infrastructure in the Baltic Sea and High North have focused NATO's and individual member states' attention on this evolving challenge. This has led to important initiatives. But more needs to be done on a multilateral level, and within individual member states, to protect and defend CUI in the Arctic, and respond adequately to and deter against malign activities. Developing and procuring necessary capabilities is required, as is clarifying laws, processes, responsibilities, and roles, and enhancing efforts that support situational awareness and presence. Most importantly, NATO allies must determine how they can address the challenge of attribution to hold malign actors accountable and respond adequately to provocations.

4.1. "Hard" Solutions: A Focus on Capabilities

To start, the United States must address gaps in situational awareness by deploying and upgrading its assets and systems. Without the necessary hardware and software to detect, deter, and defend against threats to CUI, the United States is not adequately positioned to meet and deny security challenges, hybrid or conventional, in the North American Arctic. The United States and Canada must work together to ensure the smooth implementation of NORAD modernization. They must cooperate, as part of the NORAD modernization plan, on upgrading of the Arctic Over the Horizon Radar (A-OTHR), which is expected to reach initial operating capability in 2028 and full operational capacity in 2031, and the Polar Over the Horizon Radar (P-OTHR), scheduled for initial operational capability in 2023 and full operational capability by 2033. In addition, the Arctic Satellite Broadband Mission (ASBM), which is led by Space Norway's subsidiary Heosat, will host two "Northrop Grumman-built satellites" with "civilian and military payloads, including two Viasat Ka-band payloads that will extend the company's satellite-based communications network across the Arctic region". The ASBM will play a critical role in closing connectivity gaps and supporting US and NATO military command and control in the region.[63]

The United States needs to make a concerted effort to upgrade its Arctic maritime and undersea assets (including icebreakers, unmanned underwater vehicles (UUVs), and underwater sensors). The United States should match, if not outpace, strategic rivals that could use such assets to challenge its sovereignty and security. In light of budgetary constraints, the United States should leverage defense innovation and develop cost-effective solutions, including autonomous systems to enhance situational awareness in space, from the air, and in the undersea domain. To achieve this, it should work closely with the private sector to assess the viability of commercial options. More strategic involvement of the defense industry and the commercial sector is critical to developing Arctic-specific or -adapted capabilities, and to fostering more research and development in this field.

Pooling and Sharing of Resources with Other Allies

Cooperation with Canada (and the Kingdom of Denmark) will be critical to keep the North American Arctic secure. The bilateral cooperation should go beyond NORAD modernization and also focus on joint efforts in the maritime and undersea domains. The United States should build on its collaboration with Norway and deepen joint efforts with other NATO Arctic allies to develop, advance, and procure specific Arctic capabilities, especially unmanned systems in the air and undersea domains. This effort should be pursued with the highest priority to

enhance situational awareness, filling gaps while NORAD modernization and updates to the Over the Horizon Radar are implemented.

The United States and its NATO Arctic allies should apply lessons from the alliance's Digital Oceans initiative to leverage the role of the private sector and AI in developing new Arctic-capable assets and integrating AI solutions into existing and future monitoring and data-processing technologies. NATO should also consider an alliance-wide approach to incentivizing the private sector to enhance CUI resilience and fortification. The alliance could consider a funding structure for private entities that develop or operate infrastructure deemed critical to NATO. This could include a fund for this purpose that would help member states finance the fortification of critical infrastructure.

4.2. "Soft" Solutions: Interagency, Civil-Military, Public-Private Cooperation

While steps taken to clarify roles, functions, and responsibilities across the US government for protecting CUI go in the right direction, a special focus should be placed on streamlining response processes. In a crisis scenario, clear processes and command structures outlining the responsibilities of different US government agencies, the DoD, and the relevant combatant command will be critical for swift and decisive responses. An optimized response process will contribute to greater resilience and strengthen deterrence against threats.

The nature of hybrid threats and the potential involvement of civil and commercial actors requires deeper civil-military and public-private collaboration. To adequately respond to potential challenges from Russia and the PRC, whose civil and military sectors are more deeply intertwined, US federal agencies must devise clear roles and responsibilities across civil-military domains and response processes across a much broader spectrum of conflict. Greater depth and operationalization of collaborative efforts with local law enforcement and private-sector stakeholders will be key. The United States and other allies should consider emulating elements of Norway's model of state oversight over privately owned energy infrastructure and its government's close collaboration with the navy to protect CUI. Given national differences, including in legislation and governmental structures, this model would have to be adapted to each nation's unique circumstances.

Since most US critical infrastructure is privately owned, the US government needs to take additional steps to incentivize and work with the private sector to develop best practices and technical solutions that enhance CUI resilience by reinforcing cables through protective armor, integrating monitoring capabilities, and ensuring that relevant commercial entities are adequately equipped to tackle management and repair work in a timely manner. Beyond working with the private sector on risk assessments, it will be important to coordinate and navigate complex legal questions across the public-private spectrum, and prepare operators for potential incidents.

Bilateral and Multilateral Soft Solutions

In addition to investing in joint air, space, and undersea capabilities, the United States must work with other allies, most importantly Canada and Norway (and partners in Asia), to implement processes to ensure early detection of potential naval, submarine, and UUV movements from Russia and the PRC and to optimize information sharing.

Deployments of additional assets to defend infrastructure and advance situational awareness during and after Russian and Chinese naval maneuvers in the region are of particular importance.

The US federal government, the US armed forces, and state and local law enforcement should work together closely to ensure that information sharing and operational cooperation processes are optimized across borders, especially that with Canada. Bilateral cooperation between the United States and Canada would be welcomed by the latter's public and private sectors. Proposed future Arctic infrastructure, such as cables or extractive industry outposts and infrastructure, would likely pass through or near US-Canadian border regions and would be vulnerable to attack due to increased traffic and shallower waters. A bilateral approach, following the NORAD model but focused on protecting undersea infrastructure, would therefore, be useful, especially if it entailed a significant public-private partnership component. Such a bilateral approach to cooperation would also allow intelligence to remain within Five Eyes, which can ease friction and improve speed. Canada has emphasized its "renewed focus on the surveillance and control of the Canadian Arctic", which it indicates will be "complemented by close collaboration with select Arctic partners, including the United States, Norway and Denmark, to increase surveillance and monitoring of the broader Arctic region".[64]

Even outside these bilateral or minilateral formats, the United States should ensure that it can seamlessly work with other NATO Arctic allies, that intelligence can be quickly processed, and that counterparts in different ministries are clearly identified. Given the critical role of commercial actors, the private sector must be closely integrated into this multilateral process. This effort should go beyond outlining roles on paper. NATO and its Arctic member states should consider additional exercises and simulations involving the private sector to practice within these decision-making environments. Regular public-private table-top exercises sponsored by NATO or Arctic countries would help operationalize response processes and strategic communication approaches.

As the Balticconnector case has demonstrated, control over information sharing and strategic communication is important during ongoing investigations to minimize the potential for disinformation. The United States and its allies should build on these experiences. Strategic communication and signaling to adversaries will also play a key role in attribution, where possible, and in deterring CUI challenges.

Beyond clarifying and operationalizing processes, NATO allies should work together to conduct and continuously update threat assessments for CUI, including, as applicable, in the Arctic. To do so, the United States and its allies must also continue to look to lessons learned from the war in Ukraine. As recommended in a previous GMF publication, USNAVEUR and the Second Fleet should continuously assess the use of UUV in light of Ukrainian and Russian tactics and evaluate implications for the North Atlantic.[65] These threat assessments should inform decision-making for capability development and procurement to ensure allies develop and field the necessary capabilities to protect their CUI assets. As the United States and NATO assess vulnerabilities, patterns surrounding past incidents may be useful in identifying priority areas.

5. Assessing Vulnerability: The Grayest of Gray Areas

Cases in the Baltic Sea and High North reveal factors that could make undersea infrastructure particularly vulnerable to deliberate attacks, depending on location or strategic and symbolic value.

Strategic and High-Value Targets

Undersea infrastructure that is critical to enable military operations or to civil supply will need to be monitored and protected especially closely to prevent data breaches and damage that puts national supply and operations at risk. Where possible, governments should steer the private sector to incorporate redundancies and monitoring capabilities.

Assets with High Symbolic Value

Assets with high symbolic value could be exposed to additional risk. This includes projects that have political importance, compete with Russian and PRC economic interests, or can be weaponized as a tool for political pressure or punishment. NATO allies should take special precautions to monitor Western CUI systems that excluded Russian and PRC investment despite interest from these countries. The allies should also monitor undersea infrastructure that was built after prior projects involving Russia and the PRC were paused or cancelled due to concerns about dual-use capability or due to impaired diplomatic relations.

Complicated Ownership Structure

As outlined above, the ownership structure of undersea infrastructure connecting countries is often complicated, with civil and private entities from many nations involved in its financing, development, and operation. This complicates any delineation of responsibilities and potential response options. It also increases the importance of information sharing and of coordination processes between the public and private sectors.

Gray Areas in International Law

While analysts criticize the patchwork of clear international legal frameworks and mechanisms to address CUI threats, international law offers avenues to address threats to undersea cables in international waters. The International Convention for the Protection of Submarine Telegraph Cables (Paris Convention) of 1884, which has been ratified by 36 states, applies to all "legally established submarine cables" outside territorial waters "landed on the territories, colonies, or possessions of one or more of the High Contracting Parties". Article 2 holds that "break[ing] or injur[ing] a submarine cable, willfully or by culpable negligence, in such a manner as might interrupt or obstruct telegraphic communication, either wholly or partially" is a punishable offense. Article 10 allows "officers of a warship or a ship specifically designated by a Party to the Paris Convention" to board a vessel if its crew "has committed an infraction of the measures provided for by the Convention". While the agreement applies in international waters, national laws concern territorial waters. But to apply these laws, NATO allies must have the civil and military presence, response mechanisms, and structural processes to do so.

NATO allies should develop scenarios and prepare response options for incidents that affect territorial waters, EEZs, and the high seas. While attacks in territorial waters are less likely due to limited access, EEZs will be vulnerable given increased traffic. Allies should, therefore, consider updating applicable national laws and, more importantly, collaborate with the international community to clarify and enforce legal frameworks and norms by building on existing laws, including the cable convention, and informal formats, such as the International Cable Protection Committee. It will be important to include countries from the "Global South" in this process, in part to counter Russian and PRC ambitions to develop alternative governance approaches.

Conclusion

NATO, the EU, their member states, and the private sector are developing important national, bilateral, minilateral, and multilateral initiatives to increase the resilience of CUI and protect assets. These initiatives include upgrading capabilities, sharing information, streamlining processes, and holding joint naval and air maneuvers. But more needs to be done. NATO and individual allies also need to develop their capacity to respond to and attribute incidents, and enhance deterrence against hybrid threats, including those in the undersea domain.

Continuing incidents, backed by Russia and the PRC, that undermine alliance deterrence and implicitly move the goal posts of acceptable behavior also demonstrate that past responses have been insufficient. NATO policy holds that an attack against critical infrastructure may result in an Article 5 response. Reactions to incidents that fall short of this may be deemed as weak by adversaries testing the boundaries of tacitly accepted behavior, thereby undermining deterrence. With this in mind, NATO must enhance its ability to attribute and condemn attacks. Alliance members should also consider expanding NATO response options and enhance SACEUR's authority to quickly respond to threats against CUI. This could include a stronger and better resourced maritime readiness force following the model of the VJTF. NATO should also help its members coordinate announcements on actions allies may take in response to incidents in their EEZs. Such actions include the right to board a vessel suspected of damaging undersea cables.

In the Arctic, where NATO allies' posture and capabilities are more limited, more concerted efforts to enhance situational awareness will be of utmost importance and will serve as the basis for detecting and denying threats, and for holding potential aggressors accountable. NATO's Arctic allies should closely monitor undersea infrastructure that is especially vulnerable due to its location, its strategic value, its complicated ownership structure, and its political and symbolic value. Russian and PRC naval maneuvers should trigger an increased NATO presence to protect and defend nearby assets during and after exercises.

Allies should also focus on assessing the legal implications of incidents based on their locations—in territorial waters, in countries' EEZs, or outside them—and share the results broadly with civil, military, and private stakeholders across the alliance to allow for quick decision-making. In addition, efforts to advance and enforce national and international legal frameworks and norms with support from the "Global South" should be considered.

Given competing security priorities and limited resources of the United States and its allies, governments and the military will be forced to think creatively about capability developments and pursue cost-effective solutions. The Ukraine war has demonstrated the utility of commercial unmanned aerial vehicles and UUVs. At the same time, the conflict has highlighted Russia's focus on EW and satellite jamming. Lessons learned from these developments will be important as NATO allies deploy future capabilities, including in the Arctic, to ensure redundancies and avoid single points of system failure.

The Arctic environment creates unique challenges. Specific capability requirements, limited assets, long distances, and difficult operational conditions complicate joint operations. As a result, NATO's Arctic allies will have to think differently about the alliance's role in this theater and place an even greater focus on homeland defense and the protection of their own EEZs. This will require, in Alaska's case, maximum US doctrinal clarity on

responsibilities and streamlined processes across the civil-military-private sectors, with clear guidance on the transfer of responsibilities across the spectrum of conflict.

Together, NATO's Arctic allies should build on the alliance's initiatives that support joint approaches to capability development, procurement, and information sharing and processing. Regular consultations to assess threats, and to clarify command and control and response processes to account for an evolving security landscape, will be useful. Lastly, NATO and its Arctic allies should conduct joint exercises and simulations to operationalize decision-making processes across the dynamic civil-military-private spectrum.

Endnotes

[1] Malte Humpert, "Nord Stream Pipeline Sabotage Mirrors Svalbard Cable Incident", High North News, September 29, 2022. https://www.highnorthnews.com/en/nord-stream-pipeline-sabotage-mirrors-svalbard-cable-incident

[2] Niels Nagelhus Schia, Lars Gjesvik, and Ida Rødningen, The subsea cable cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed?, Norwegian Institute of International Affairs, January 2023, p. 1. https://www.nupi.no/en/publications/cristin-pub/the-subsea-cable-cut-at-svalbard-january-2022-what-happened-what-were-the-consequences-and-how-were-they-managed

[3] Malte Humpert, "Nord Stream Pipeline Sabotage Mirrors Svalbard Cable Incident", High North News, September 29, 2022. https://www.highnorthnews.com/en/nord-stream-pipeline-sabotage-mirrors-svalbard-cable-incident

[4] Atle Staalesen, "'Human activity' behind Svalbard cable disruption", The Barents Observer, February 11, 2022. https://thebarentsobserver.com/en/security/2022/02/unknown-human-activity-behind-svalbard-cable-disruption

[5] Niels Nagelhus Schia, Lars Gjesvik and Ida Rødningen, The subsea cable cut at Svalbard, p. 2.

[6] Atle Staalesen, "'Human activity' behind Svalbard cable disruption".

[7] Niels Nagelhus Schia, Lars Gjesvik and Ida Rødningen, The subsea cable cut at Svalbard, p. 2.

[8] Ibid.

[9] Ibid, p. 3.

[10] High North News, "4.3 Kilometers of Subsea Cable Vanished Off North Norwegian Coast" November 10, 2021. https://www.highnorthnews.com/en/43-kilometers-subsea-cable-vanished-north-norwegian-coast

[11] The Svalbard Treaty, February 9, 1920. https://www.jus.uio.no/english/services/library/treaties/01/1-11/svalbard-treaty.html

[12] Andrew Yerkes, WHOSE FISH? LOOKING AT SVALBARD'S FISHERIES PROTECTION ZONE, The Polar Connection, December 4, 2016. https://polarconnection.org/svalbard-fisheries-protection-zone/

[13] Andreas Østhagen, Otto Svendsen, and Max Bergmann, Arctic Geopolitics: The Svalbard Archipelago, Center of Strategic and International Studies, September 14, 2023. https://www.csis.org/analysis/arctic-geopolitics-svalbard-archipelago

[14] Niels Nagelhus Schia, Lars Gjesvik, and Ida Rødningen, The subsea cable cut at Svalbard, p. 2.

[15] Ibid, p.3.

[16] Ibid, p.2.

[17] Uliana Pavlova and Anna Cooban, "Russia cuts off gas exports to Europe via Nord Stream indefinitely", CNN Business, September 5, 2022. https://www.cnn.com/2022/09/02/energy/nord-stream-1-pipeline-turned-off/index.html

[18] RND, "Faeser kündigt Ermittlungsgruppe zu Nord-Stream-Pipelines an" ["Faeser Announces Investigation Group for Nord Stream Pipelines"], October 2, 2022. https://www.rnd.de/politik/nord-stream-pipelines-nancy-faeser-kuendigt-ermittlungsgruppe-an-FRK77FWJF2ZACDVYEEEVSCJAII.html

[19] Swedish Security Service, "Confirmed sabotage of the Nord Stream gas pipelines", November 18, 2022. https://sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/press-room/news/news/2022-11-18-confirmed-sabotage-of-the-nord-stream-gas-pipelines.html

[20] Zeit Online, "Bundespolizei und Marine starten Aufklärungsmission an Pipeline-Lecks" ["Federal Police and Navy begin Reconnaissance Mission"], October 9, 2022. https://www.zeit.de/politik/deutschland/2022-10/nordstream-mission-bundespolizei-marine-aufklaerung

[21] Ibid.

[22] Tagesschau, "Denying All Involvement", September 26, 2023. https://www.tagesschau.de/investigativ/nord-stream-anschlaege-102.html

[23] Ibid.

[24] Shane Harris and Isabelle Khurshudyan, "Ukrainian military officer coordinated Nord Stream pipeline attack", The Washington Post, November 11, 2023. https://www.washingtonpost.com/national-security/2023/11/11/nord-stream-bombing-ukraine-chervinsky/

[25] The Guardian, "Russian navy ship photographed near Nord Stream pipelines before blasts", April 28, 2023. https://www.theguardian.com/world/2023/apr/28/russian-navy-vessel-seen-near-nord-stream-pipelines-days-before-blasts

[26] NATO Secretary General Jens Stoltenberg said that "the sabotage of the Nord Stream pipelines last year and the recent damage to the Balticconnector pipeline and cables show that infrastructure is vulnerable, and that threats are real and developing. Since these incidents, NATO has stepped up air and naval patrols and increased presence in the Baltic and North Seas." NATO, "NATO Secretary General addresses protection of critical undersea infrastructure, support to Ukraine with EU Defence Ministers", November 14, 2023. https://www.nato.int/cps/en/natohq/news_220058.htm

[27] RFE/RL, "Norway Deploys Soldiers At Oil, Gas Plants In Wake Of Nord Stream Leaks", October 3, 2022.https://www.rferl.org/a/norway-deplys-soldiers-oil-gas-plants-nord-stream-leaks/32063134.html

[28] Nerijus Adomaitis and Anne Kauranen, "Norwegian Navy shadows Chinese vessel probed over Baltic pipe damage", Reuters, October 18, 2023. https://www.reuters.com/world/europe/norwegian-navy-shadows-chinese-vessel-probed-over-baltic-pipe-damage-2023-10-18/

[29] NATO, "NATO steps up Baltic Sea patrols after subsea infrastructure damage", October 19, 2023. https://www.nato.int/cps/en/natohq/news_219500.htm

[30] Sean Monaghan, Otto Svendsen, Michael Darrah, et al., NATO's Role in Protecting Critical Undersea Infrastructure, CSIS, December 19, 2023.

[31] Claudia Chiappa, "6 countries move to protect the North Sea from Russians", Politico, April 9, 2024. https://www.politico.eu/article/6-european-countries-sign-pact-protect-critical-energy-infrastructure-north-sea-from-russia/

[32] Ministry of Defence, Joint statement by Joint Expeditionary Force ministers, June 2023", June 13, 2023. https://www.gov.uk/government/news/joint-statement-by-joint-expeditionary-force-ministers-june-2023

[33] Ministry of Defence, "UK and Norway to increase cooperation on undersea capabilities", May 18, 2023. https://www.gov.uk/government/news/uk-and-norway-to-increase-cooperation-on-undersea-capabilities

[34] Ibid.

[35] NATO, NATO Response Force. https://www.nato.int/cps/en/natolive/topics_49755.htm

[36] NATO, "NATO stands up undersea infrastructure coordination cell", February 15, 2023. https://www.nato.int/cps/en/natohq/news_211919.htm

[37] NATO, "NATO focus is on Critical Undersea Infrastructure during series of multi-domain exercises with latest autonomous vehicles in Portugal", October 4, 2023. https://mc.nato.int/media-centre/news/2023/nato-focus-is-on-critical-undersea-infrastructure-during-series-of-multidomain-exercises-with-latest-autonomous-vehicles-in-portugal

[38] Ibid.

[39] Ibid.

[40] NATO, "NATO and industry work together to strengthen maritime surveillance", April 16, 2024. https://www.nato.int/cps/en/natohq/news_224798.htm?selectedLocale=en

[41] Ibid.

[42] NATO, "Maritime Unmanned Systems Innovation Advisory Board discuss NATO innovation in the maritime domain", November 9, 2021. https://www.nato.int/cps/en/natohq/news_188548.htm?selectedLocale=en

[43] European Commission, EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure, June 29, 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564

[44] European Commission, Critical infrastructure resilience, March 21, 2024. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en

[45] Ibid.

[46] U.S. Geological Survey, Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle, 2008. https://pubs.usgs.gov/fs/2008/3049/fs2008-3049.pdf

[47] European Parliament Research Service, Norway to mine part of the Arctic seabed, January 2024. https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757616/EPRS_ATA(2024)757616_EN.pdf

[48] Isaac B. Kardon and Sarah Camacho, Why China, Not the United States, Is Making the Rules for Deep-Sea Mining, Carnegie Endowment for International Peace, December 19, 2023. https://carnegieendowment.org/research/2023/12/why-china-not-the-united-states-is-making-the-rules-for-deep-sea-mining?lang=en

[49] Isabelle Bousquette, "A Warming Arctic Emerges as a Route for Subsea Cables", The Wall Street Journal, June 15, 2022. https://www.wsj.com/articles/a-warming-arctic-emerges-as-a-route-for-subsea-cables-11655323903

[50] Ibid.

[51] Far North Digital, LLC, Demand for secure, fast and expansive international data transmission capacity continues to grow. https://www.fn-digital.com/project

[52] Joe Brock, "Inside the subsea cable firm secretly helping America take on China", Reuters, July 6, 2023. https://www.reuters.com/investigates/special-report/us-china-tech-subcom/#:~:text=SubCom%20operates%20six%20cable%2Dlaying,sheaves%20of%20fiber%2Doptic%20cable

[53] Alcatel Submarine Networks, ASN Fleet. https://www.asn.com/our-fleet/#pop-up-menu-anchor

[54] Joe Brock, "Inside the subsea cable firm secretly helping America take on China".

[55] Quintillion, "Quintillion Subsea Fiber Cable Repair Complete", September 19, 2023. https://www.quintillionglobal.com/quintillion-subsea-fiber-cable-repair-complete/

[56] The White House, National Security Memorandum on Critical Infrastructure Security and Resilience, April 30, 2024. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

[57] Other actors outlined by the 2013 document are the General Services Administration, the Nuclear Regulatory Commission (NRC), and the Federal Communications Commission. The White House, Presidential Policy Directive -- Critical Infrastructure Security and Resilience, February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[58] The White House, National Security Memorandum on Critical Infrastructure Security and Resilience, April 30, 2024. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

[59] Ibid.

[60] Ibid.

[61] Ibid.

[62] Ibid.

[63] Sandra Erwin, "Arctic broadband satellites complete key tests ahead of mid-2024 launch", SpaceNews, November 29, 2023. https://spacenews.com/arctic-broadband-satellites-complete-key-tests-ahead-of-mid-2024-launch/

[64] Government of Canada, Global Defense Engagement, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy/global-defence-engagement.html

[65] Heather A. Conley, Mathieu Boulègue, Sophie Arts, et al, Defending America's Northern Border and Its Arctic Approaches Through Cooperation With Allies and Partners, GMF Insights, August 2023.