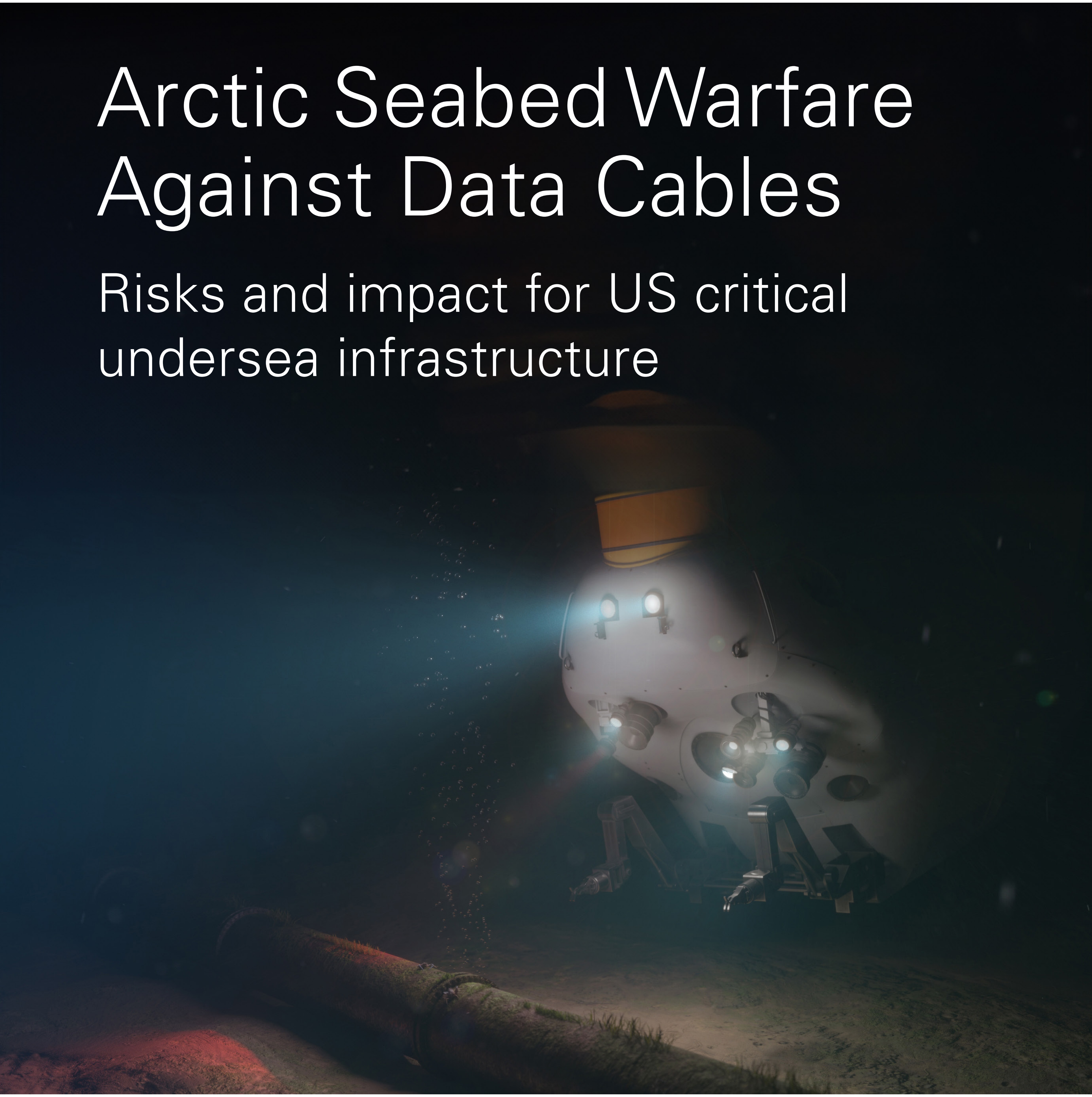
Wilson Center | Polar Institute

Arctic Seabed Warfare Against Data Cables

Risks and impact for US critical undersea infrastructure



Mathieu Boulegue, Global Fellow, Polar Institute | Wilson Center

August 2024

Contents

Executive Summary

- Subsea security and seabed warfare have become a hot-button issue concerning grey zone operations and sub-threshold warfare against critical underwater infrastructure (CUI), notably from Russia and China. For nefarious state actors, CUI disruption represents a low-cost, high-impact capability due to critical dependencies and the potential for cascading impacts.
- Out of the range of CUI, fiber optic data and communication cables are the most vulnerable to disruption. Sabotage against data cables has clear military security repercussions for the United States, NATO, and its allies. Such activities pose significant security risks for the US across the Arctic region but also in and around the North Atlantic, the Barents Sea, the Baltic Sea, and the North Pacific.
- Beyond civilian applications, underwater cables are critical for military-encrypted and diplomatic communication. For the US military, specifically, submarine cables are critical to the protection of the homeland. The vast majority of military communication goes through the transatlantic and transpacific cable network and cables are crucial for remote drone operations in distant theaters.
- Efficient protection of data cables is lacking, and the situation made worse by the inadequacy of current peace- and wartime legal frameworks as well as the insufficient ability of states to attribute attacks and damage done to underwater cables. This is especially true as such disruptions are sub-threshold and multi-domain grey-zone operations.
- There is strong incentive for nefarious states, notably Russia and China, to invest in capabilities able to disrupt and damage underwater cables, especially since such operations have a low entry cost and can reach strategic military and civilian effects against a territory and its population.
- Russia has a strong track record of interest and activities linked to data cables disruption. Cable sabotage is part and parcel of Russia's well-established toolkit of plausibly deniable, sub-threshold activities. Several dedicated units, structures, and subsurface capabilities are devoted to seabed warfare.
- There are two main categories of seabed warfare activities that adversarial actors could conduct against underwater cables: (1) intelligence gathering, mostly the mapping and monitoring of the seabed infrastructure, in preparation for potential acts of sabotage, and (2) the physical destruction of underwater cables. The weaponization of civilian vessels and anchoring 'accidents' represent a key risk associated with cable severing, especially in peacetime. Attacks could also occur against the network of cables landing stations as well as against cable repair and maintenance fleets.
- Data cables present in and around the Arctic region are particularly vulnerable. Due to the geography and presence of natural chokepoints, circumpolar data cables generally display less resilience to disruption and damage, therefore making them prime targets for seabed warfare activities by nefarious state actors.
- The Arctic is a place of low cable resilience, with the presence of several chokepoints across the region: (1) the Svalbard-GIN-GIUK gap, (2) the Canada-Greenland gap across the North-East passage and the Labrador Sea, and (3) around and across the Bering Strait. The absence of genuine cable redundancy in the Arctic region makes them even more critical, especially in the context of US national security under NORTHCOM's supervision.

- These chokepoints feature a mix of shallower waters where Russia in particular could use surface vessels to conduct anchoring and dredging operations as well as deeper Arctic waters where Moscow would require subsurface assets to sabotage cables. The ‘Canada-Greenland gap’ and the seas across the Bering Strait represent critical chokepoints against US regional infrastructure and under the supervision of NORTHCOM.
- Policy attention and action in the global community have not yet sufficiently assessed the ‘critical’ part of ‘critical undersea infrastructure’, the importance of fiber optic cables, and the need to protect them from foreign interference.
- In the United States, the 2023 Implementation Plan for the 2022 National Strategy for the Arctic Region posits that predicting and assessing risk to CUI in the Arctic region is a key component to defending the homeland from external threats. In this context, more research is necessary to understand the nature of the threat against CUI in general, and data cables in particular.
- National policymakers and multilateral stakeholders must find the appropriate balance of response in terms of governance, deterrence, and technology-enabled capabilities. The aim is to make data cables more resilient by design as well as to better mitigate damage to the network while deterring attacks from happening in the first place.
- As cable disruption fundamentally sits across several domains (sea, land, cyberspace) and sectors (cables themselves, landing stations, repair ships, etc.), their protection should be designated ‘critical’ in terms of US national security priority. Another part of the debate is to determine whether CUI should be made a full-fledged operational domain of war.
- Global and effective deterrence against cable disruptions will require consistent Western policy across the myriad aspects of cable protection. The deterrence of cable disruption and damage by nefarious state actors must be streamlined and fully integrated into US and NATO thinking.

Summary of Policy Recommendations

- National policymakers and multilateral, including industrial, stakeholders must find the appropriate balance of response in terms of governance, deterrence, and technology-enabled capabilities. The protection of CUI in general and data cables in particular should be designated ‘critical’ in terms of US national security priority.
- From a military security standpoint, individual nations should conduct cable infrastructure risk assessments to strengthen its resilience. Nations should also aim to develop dedicated seabed warfare strategies to increase preparedness and response to cable disruption. For the US, such an effort could be coordinated as part of the Implementation Plan for the 2022 National Strategy for the Arctic Region (NSAR).
- Nations must determine whether CUI should be made a full-fledged operational domain of war. Doing so would help individual countries and NATO incorporate the protection of data cables into military doctrine as well as craft better deterrence policies.
- NATO should consider updating its Maritime Strategy to incorporate the protection of CUI more prominently. To this end, it could create a dedicated Standing NATO Maritime Group (SNMG) focused on CUI protection, especially in an Arctic and Baltic environment. NATO should also focus on widening the scope of multi-domain exercises aimed at protecting data cables or deterring an attack.
- Information sharing between allies and data fusion within NATO are key to understanding the nature of the threat against CUI as well as anticipating future disruptions against underwater cables. More regular and dedicated contacts on CUI disruption are necessary between nationals and multilateral structures, notably between coast guards of respective nations.
- Nations and multilateral stakeholders should increase the level of cooperation with industrial actors in charge of operating and maintaining the network of fiber optic cables. The aim is to foster more synergies with the private sector regarding information sharing, early warning systems, sensing capabilities, and response to disruptions.
- In the context of the NSAR, the United States government should encourage increased information sharing and data fusion on cables between NORTHCOM and the US Coast Guard (USCG).
- From a national security standpoint, governments should ensure that the private sector does not rely on the technology of foreign companies whose governments are known to engage in cable disruption and espionage, such as China.
- Current legal provisions are insufficient to ensure the protection of underwater cables. National and international legal frameworks must be strengthened to increase the protection of data cables and translate them into policy. ‘Patching’ legal and normative gaps in existing texts would be the first place to start and would help achieve greater clarity over the current legal regime.
- To strengthen international cable protection, the US should consider pioneering discussions around the creation of an international legal treaty defining the ‘rules of the road’ regarding cable disruption during peacetime and wartime.
- The deterrence of cable disruption and damage by nefarious state actors must be streamlined and fully integrated into US and NATO thinking. Deterrence by denial can be ensured through credible presence, notably more naval patrols, and dedicated NATO-led exercises, including in the Arctic.

- The most efficient tool for deterrence by denial is seabed domain awareness around data cables. The development and procurement of seabed-dedicated capabilities and overall Maritime Domain Awareness (MDA) technologies will help monitor, deter, and mitigate potential cable disruption and damage.
- The United States and NATO should encourage and help private cable industry actors to develop and procure seabed-specific capabilities for advanced remote fiber sensing and early warning detection systems. This should be systematically factored into US resource allocation, especially in the context of the NSAR.
- In terms of national resource allocation, the US and its allies must invest in CUI monitoring capabilities such as surveillance sensors, underwater acoustic sensors, coastal radars, next generation Automatic Identification System (AIS) tracking technology, as well as satellite sensors. Technology will ultimately help achieve NATO's objective of 'seabed-to-space situational awareness (S3A)' in terms of multi-domain data fusion.
- Due to existing geographical cable chokepoints and areas where there is little redundancy, the United States should conduct a thorough, updated assessment of the security of all cable landing sites in order to patch existing gaps.
- The United States and its allies should encourage discussions with cable industry leaders to streamline the division of labor for the maintenance and repair of cables in case of intentional damage. In-country resilience starts with defining the interaction between civilian repair capabilities and naval forces.
- In terms of deterrence by punishment, the United States and its allies should systemically make it clear to potential perpetrators that nefarious acts against CUI in peacetime will bring a strong response.
- The United States and its allies should consider increasing the cost of grey zone seabed warfare disruption at peacetime—for instance, by more severely punishing vessels navigating with their AIS or VMS transponders switched off or displaying anomalous trajectories and behavior.

Introduction

Critical undersea infrastructure (CUI) comprises diverse, interdependent types of maritime infrastructure: surface and underwater energy infrastructure (pipelines, power cables, wind farms, etc.), fiber optic data and communication cables, fishing, and shipping infrastructure.[1]

The security and military threat to CUI has raised a lot of policy attention in the wake of recent events in Europe—from the Nord Stream 2 damage in September 2022 to the severing of a data cable close to Svalbard that same year, or the Balticconnector and comms cables incident in the Baltic Sea in October 2023. These events reminded the policy world and the security establishment of NATO countries that CUI, and especially fiber optic data cables, are vulnerable and at risk of disruption by nefarious state actors.

Subsea security and seabed warfare have become a hot-button issue concerning grey zone operations and sub-threshold warfare against CUI, notably from Russia and China. For nefarious state actors, CUI disruption represents a low-cost, high-impact capability due to critical dependencies and the potential for cascading impacts. There is, therefore, a strong incentive for Moscow and Beijing to increase the number of covert activities against seabed infrastructure.

Out of the range of CUI, fiber optic data and communication cables are the most vulnerable to disruption. Sabotage against data cables has clear military security repercussions for the United States, NATO, and their allies. Such activities pose significant security risks for the US across the Arctic region but also in and around the North Atlantic, the North Pacific, and the Baltic Sea.

In the case of escalation, there is a risk that cables would be targeted to degrade the US operating environment and support for allies. Existing risks are compounded by the fact that cable disruption activities are fundamentally multi-domain by nature, as they equally affect land, sea and subsea, as well as the cyberspace.

Data cables present in and around the Arctic region are even more vulnerable than those outside of the region. Due to the geography and presence of natural chokepoints, circumpolar data cables generally display less resilience to disruption and damage, making them prime targets for seabed warfare activities by nefarious state actors. North Atlantic and North Pacific approaches, as well as Nordic and Baltic countries, are vulnerable to disruptions against underwater cables, which would have a tremendous impact on US activities in the region. Recent cases of Arctic reconnaissance and intelligence activities by Russia are a concern for the United States, NATO, and their allies.

The 2023 Implementation Plan for the 2022 National Strategy for the Arctic Region posits that predicting and assessing risk to CUI in the Arctic region is a key component to defending the homeland from external threats.[2] In this context, more research is necessary to understand the nature of the threat against CUI in general, and data cables in particular.

This paper specifically touches upon the threat to data and communications cables, linked to the security of US military communication and surveillance. It looks at the scope, scale, and level of threat of Russian and Chinese seabed warfare activities against data cables, with a focus on the Arctic region. The paper analyses the impact of potential disruption on military security and offers a set of policy recommendations aimed at helping US policymakers better understand existing security risks to the homeland. This will assist key stakeholders in crafting more effective countermeasures and deterrence to protect data cables and increase their overall resilience.

Chapter 1: Understanding the environment around submarine data and communication cables

1.1—Critical interdependencies around data cables

There are over 570 submarine data and communication cables lying at the bottom of the world's seas and oceans. This represents a combined 1.4 million kilometers of cables and over 1,300 landing stations around the world dispatched between over 200 independent cable systems owned by national and international private companies.[3]

Submarine cables are the backbone of trans-oceanic security as well as the central nervous system of the digital age.[4] Advances in glass fiber optic technology since the 1980s-90s have allowed for the interconnection of the entire planet. Today, submarine cables are responsible for the vast majority of the Internet communication traffic (between 97 to 99% of traffic)[5] throughout the world including banking operations, the digital economy, and, more critically, military communication. Cable traffic represents about $10 trillion worth of financial transactions every day.[6]

Cables are, by nature and definition, critical and interdependent infrastructure.[7] Fiber optic cables are essential to digital information traffic: they are much faster, more efficient, and more capable than satellite communication.[8] Driven by the digital economy and the constant need for faster network bandwidth, cable traffic is set to increase exponentially in the coming years.[9]

Data cables are reliable by design. In terms of engineering, they are part of the *'five nines standard'*, meaning they are reliable 99.999% of the time.[10] The submarine cable network is also inherently resilient. Indeed, the network has high redundancy, which means specific data traffic can easily be redirected across several cables in case of damage—provided private restoration agreements are in place between cable providers to allow access to other cable systems. In other words, "*rupturing one cable can cause temporary disruptions but does not cut off service*".[11]

Furthermore, cables are vastly spread out across the ocean floor, meaning bottlenecks are limited to a minimum—even though landing stations are geographically concentrated in specific chokepoints on land and sea approaches to landing sites.[12] In the case of cable rupture, data traffic can be re-routed with limited impact: this essentially means that in highly-resilient parts of the network, an adversary would require a large coordinated effort to reach genuine effects.

This double feature—redundancy and spatial diversity—ensures the organic resilience of the network and brings a high tipping point before reaching a cascading impact on the infrastructure. Contrary to established beliefs, the scenario of a 'doomsday digital blackout' remains highly unlikely.

There are, however, resilience chokepoints in the network, specifically for island nations and archipelagoes[13] which sometimes rely on one or two cables for their access to digital information and economy (for instance the Svalbard archipelago and Taiwan). Specifically, the Arctic is a place of low cable resilience, with the presence of several chokepoints across the region: (1) the Svalbard-GIN-GIUK gap, (2) the Canada-Greenland gap across the North-East passage and the Labrador Sea, and (3) around and across the Bering Strait. The absence of genuine cable redundancy in the Arctic region makes them even more critical, especially in the context of US national security under NORTHCOM's supervision.

1.2—Cable vulnerability, damage, and incidents

While data cables are inherently reliable and resilient, they are, however, fundamentally vulnerable to physical damage. Each year, approximately 200 incidents are reported on the worldwide submarine network.[14]

The vast majority of breaks and damages are related to accidents provoked by human activity (close to 70%)—namely anchoring and trawling activities by fishing vessels and commercial shipping—as well as structural obsolescence (wear and tear, component damage and failure, etc., 6%) and environmental disruptions (geological abrasion, earthquakes, storms, etc., 10%).[15] Anchoring accidents and negligence represent the main cause of cable damage each year, which includes accidental dragging, dropping, and mispositioning.[16] Intentional cable damage by nefarious state and non-state actors is rarely reported as a source of incident—although it recently took place in the Red Sea.[17]

Cable vulnerability is compounded by layout fragilities, not least because data cables are about the size of a garden hose and must remain light and flexible to be operative. In shallow waters, cables are typically armored with steel wire rods and buried between 1-3 meters below the seafloor to mitigate the amount of yearly damage.[18] Most incidents take place within 200 meters of depth, where cables are most reinforced but still hardly stand a chance against a 10-ton anchor.

In deeper waters, beyond the boundaries of the legal continental shelf and Exclusive Economic Zones (EEZ), the cables simply lie on the sea floor and the cable gauge is reduced to combat deep-sea pressure. Consequently, while less prone to anchoring or trawling accidents, these unarmored cables are more susceptible to potential intentional disruptions. At such depths, the main source of damage, however, is seismic or abrasion damage.

The locations of most data cables are public knowledge, which represents another point of vulnerability. Detailed maps with the exact layout of the worldwide cable network are available online[19] as well as widely distributed in the maritime and fishing industry to minimize the number and severity of accidents. As a result, the cables—and particularly the chokepoints of landing stations—are vulnerable to nefarious attacks by state and non-state actors.[20]

A final issue with cable vulnerability relates to repair capabilities. Cable repair and maintenance are not usually performed by governments but by private civilian operators distributed across the world.[21] Repair and maintenance capabilities are generally limited in terms of available surface assets and require skilled workers able to pull up cables from the seafloor. Depending on the amount of damage to a cable, repair can be a complicated and time-consuming endeavor.

1.3—Legal regime and normative provisions governing cable security

The inadequacy of the current peace- and wartime legal framework governing data cables represents another vulnerability.[22] Several international conventions regulate the protection of cables, first and foremost the 1982 United Nations Convention on Law of the Sea (UNCLOS).

Under UNCLOS, the international legal protection for an underwater cable is dependent on where it lays—namely whether in territorial waters up to the 12 nautical miles line, in contiguous waters up to 24 nautical miles, within the boundaries of Exclusive Economic Zones (EEZ) up to 200 nautical miles, or in international waters and high seas outside national jurisdictions.[23]

UNCLOS provisions are notably silent on the EEZ and high seas, where states neither have full responsibility nor freedom of action to efficiently protect cables. In these areas, UNCLOS does not provide sufficient jurisdiction to protect cables on the seabed or to put an end to harmful activities by suspect vessels. Its provisions also only apply during peacetime.

Article 113 of UNCLOS on '*breaking or injury of a submarine cable or pipeline'*[24] requires states to domestically criminalize damage done to an underwater cable by vessels bearing its national flag. However, the article fails to provide for enforcement jurisdiction over harmful activities or the ability for a state to board and arrest suspect vessels in international waters. Another issue is implementation of the minimal existing protections, especially domestic legal implementation of Article 113 of UNCLOS.

Other international texts include the 1958 Geneva Conventions of the Continental Shelf and High Seas as well as the 1884 International Convention for the Protection of Submarine Cables. The 1884 Convention is a fully binding treaty offering a more detailed regime for the protection of cables than UNCLOS during peacetime.

The San Remo Manual on International Law Applicable to Armed Conflicts at Sea[25] also offers some guidance regarding the cable regime, although it is not a binding treaty and only codifies customary international law.

More recently, The Tallinn Manual 2.0 on cyber operations mentions that "*there is no clear norm with respect to either the EEZ or continental shelf, and certainly not for the high seas,*"[26] therefore limiting the scope of cable protection to territorial waters. Meanwhile, the Oslo Manual on the law of armed conflict recognizes a right for states to take *"protective measures with a view of preventing or terminating any harmful interference*" against cables,[27] although this specific statement only applies during peacetime.

Nevertheless, none of these texts or provisions present a compelling body of law to fully protect data cables from interference and harm. The main issue is that the provisions written back in the 19th century, or more recently in the 1950s and 1980s, did not anticipate how critical and therefore how vulnerable the cable infrastructure would become in the context of the digital economy.[28] International and national law are now trailing behind recent developments and policy attention towards CUI.

A key challenge to the current regulatory environment is linked to the ownership structure of cables: data cables themselves as well as maintenance and repair capabilities are mostly owned and operated by private companies—and therefore not linked to specific states. If this feature undoubtedly represents an enabler from a technical and technological perspective, it is a legal impediment.

In the absence of clear regulations with state entities, the private cable industry has organized itself through different bodies, especially around the International Cable Protection Committee (ICPC), the main industry forum addressing legal, regulatory, and technical issues around data cables.

The inadequacy of the current legal regime is compounded by the absence of clear distinction in the protection of underwater cables in times of peace or war. The wartime legal regime is outdated and does not offer a clear answer to the question of what constitutes an armed attack against a cable under international law or how cables should be governed during warfare, especially if they are willfully damaged or destroyed.[29] Quite the opposite: UNCLOS and the 1884 Cable Convention do not apply to armed conflict and are silent on wartime targeting of underwater cables during wartime. Meanwhile, the Tallinn Manual 2.0 implies that the cable infrastructure can be treated as legitimate military targets.[30]

A final legal issue relates to the insufficient ability of states to attribute attacks and damage done to underwater cables. This is because cable disruptions generally take place in the grey zone and are conducted by nefarious states as part of sub-threshold, multi-domain operations. Technical and physical attribution of cable damage relies on persistent monitoring and identifying 'red flags' in the behavior of suspect vessels and submersible crafts (especially civilian surface vessels—fishing and leisure boats—used for such operations).

Unusual patterns of behavior can be detected and monitored remotely through network sensing, satellite tracking, AIS tracking, etc. The most important, however, is the threshold of response: namely, whether there needs to be actual damage done to a cable before it can be stopped and attributed.

Attribution is further complicated by the ownership structure of suspect vessels, as they tend to fly foreign flags and can conceal the identity of the final owner through complex ownership schemes. Attribution is finally compounded by the multi-domain nature of cable sabotage, especially potential cyber operations against landing stations.[31]

As the spectrum of risks and vulnerabilities against cables keeps increasing, there are clear gaps in the legal regime that must be urgently addressed. Overall, with a patchy legal regime and attribution issues, the governance of underwater cables is akin to what the cyber domain was a few decades ago. CUI represent a low-cost, high-impact, and fairly new field that opens the way for renewed interest in subsea security and seabed warfare.

Chapter 2: Subsea security and seabed warfare

2.1—Understanding the seabed threat environment

For adversarial state and non-state actors, cable disruptions represent a low-cost, high-impact scenario compounded by critical interdependencies in the undersea infrastructure and the potential for cascading impacts. Subsea security and seabed warfare are now a major part of the policy conversation about grey zone operations and sub-threshold warfare, with direct military implications for the continuity of communication in a contested environment.

For the past few years, there has been a track record of nefarious activities around underwater data and communication cables. A survey of past incidents and accidents likely attributed to state activities sheds light on what constitutes sub-threshold seabed warfare, especially in and Arctic and Baltic environment.

In 2021, the Norwegian Institute of Maritime Research reported *"extensive damage"* to the fiber optic and electric cables connected to the Lofoten-Vesterålen (LoVe) Ocean Observatory, an underwater facility in northwestern Norway.[32] About 4 km of cable was cut and displaced some 11 km from the facility. The subsequent investigation incriminated, Russian trawlers engaged in suspicious activities at that time, although without making an attribution.[33]

In January 2022, a deep sea Norwegian fiber optic cable connecting Longyearbyen, in the Svalbard archipelago, to Andøya in mainland Norway was damaged underwater.[34] The Svalbard Undersea Cable System is of critical importance for Svalbard, as only two cables connect it to the mainland, and the 100 satellite antennas operated by the Svalbard Satellite Station (SvalSat).[35] The incident was not clearly attributed to a nefarious state actor.

In October 2022, the SHEFA-2 data cable connecting the Shetland Islands was reportedly damaged by a fishing vessel, which created temporary disruptions in Internet access.[36] The event was initially believed to be accidental, and tied to the Russian vessel *Boris Petrov* was flagged in the area at that time.[37] Although the damage was attributed to fishing,[38] the event showed how a state can weaponize civilian vessels, especially a fishing fleet, to conduct plausibly deniable operations against data cables.

More recently, the Balticconnector gas pipeline and fiber optic cables running between Estonia and Finland and Sweden were severely damaged in October 2023.[39] The investigation by Finnish and Estonian authorities called out the Chinese container carrier *NewNew Polar Bear* as likely responsible for the sabotage.[40] It is also suspected to be at the origin of the damage done to a data cable connecting Sweden to Estonia at that time.[41]

The Chinese ship, flagged in Hong Kong, was given permission to transit through the Baltic Sea but was also tied with a Russian-registered company.[42] The investigation further suspected the implication of the Russian vessel *Sevmorput*, owned and operated by Rosatomflot. Both vessels were present within the area of the Balticconnector infrastructure at the time of the incident.[43] Both were also subsequently tracked outside Norwegian waters and further along the Northern Sea Route (NSR) after the *NewNew Polar Bear* was granted sailing permission and escort through the NSR.[44] Repair work on the Balticconnector infrastructure is still underway.

The October 2023 joint incidents in the Baltic Sea, affecting two separate data cables, are unprecedented in scale and policy consequences. Indeed, it evidenced a likely form of collaboration and coordination between Russia and China with the overt aim to disrupt data cables and other CUI connecting NATO countries.[45]

2.2—Threats to military security and risks of seabed warfare against underwater cables

Recent cable incidents in the Arctic and Baltic area, and the subsequent policy interest that it created, are a reminder of the threat cable disruptions represent for military communication and overall military security for the United States, NATO, and its allies.

Beyond civilian applications, underwater cables are critical for military-encrypted and diplomatic communication: most of the military, intelligence, and diplomatic communication traffic goes through the worldwide network of commercial, privately owned cables[46] and the existence of unmapped, classified data cables dedicated to military traffic is limited in practice.[47] Underwater cables are fundamentally part of military Sea Lines of Communication, especially across the Atlantic and the Pacific Oceans.

As discussed above, underwater cables represent 'legitimate' military target during an armed conflict, and their destruction is part of what could constitute a military objective by an adversary—inasmuch as it respects the Law Of Armed Conflict provisions of military necessity, distinction, and proportionality.[48] Damaging underwater cables offers clear strategic and tactical military advantages from disrupting effective military communication in contested environments, limiting the speed of military decisions, hampering freedom of action and operations relying on the cable network (first and foremost drone operations) as well as compromising industrial and military infrastructure.[49]

The situation is compounded by the fact that the network of fiber optic cables itself is dual-use by nature, as it can be used for military applications. Indeed, the use of acoustic remote-sensing capabilities directly inside the fiber optic can be employed for military intelligence gathering and Maritime Domain Awareness (MDA) on the seafloor.[50]

From the US military perspective, submarine cables are critical to the protection of the homeland. The vast majority of military communication goes through the transatlantic and transpacific cable network and cables are crucial for remote drone operations in distant theaters.[51]

There is, therefore, strong incentive for nefarious states like Russia and China to invest in capabilities able to disrupt and damage underwater cables, especially since such operations have a low entry cost and can reach strategic military and civilian effects against a territory and its population. Specifically in high seas, cables become '*easy targets'*[52] due to their remoteness.

As they fundamentally occur in the grey zone, cable disruption operations blur the line between peacetime and wartime and constitute a key element of sub-threshold warfare. Such operations are also multi-domain by nature as they equally affect land, maritime approaches, international waters, as well as the cyberspace.

In peacetime, cable sabotage allows an adversary to disrupt the flow of information, trade, and banking operations; control the information environment in case of escalation; damage the economies of adversaries; as well as potentially reach strategic effects in a low-cost, high-impact logic. However, this situation is caveated by the fact that in the context of the global economy, the potential economic impact from a major disruption against civilian cables would equally hurt Russia and especially China.

At the start of potential military hostilities, cable disruptions are a tactical enabler allowing an adversary to prepare the battlespace, especially at the initial or threatened period of war. Such operations are part of the preparation of the battlespace and represent a ‘first salvo’ in the planning of wider military operations: cable disruption happens in conjunction with other, coordinated activities. Nefarious state actors like Russia and China would likely conduct sabotage operations to disrupt military and civilian communications and therefore hamper the decision-making process and response of an adversary.

There are two main categories of seabed warfare activities that nefarious actors might undertake against underwater cables. The first type of activity pertains to intelligence gathering—specifically the mapping and monitoring of the seabed infrastructure in preparation for potential acts of sabotage as well as overall cable layout awareness. These operations are now regularly carried out by fleets of civilian vessels as well as uncrewed underwater vehicles fitted with remote-sensing and dual-use capabilities.[53]

There is also the physical tapping of cables—with the aim to ‘listen in’ on the fiber optic by cutting the cable sheathe and installing a listening device. This is extremely complicated from a technical point of view. The deeper the cable lays on the seabed, the more such activities would require highly sophisticated hardware and platforms, making them impractical.[54] Furthermore, cable tampering would be quickly picked up by the multiplicity of sensors present in the fiber optic and relayed to cable operators.[55] Cyber and physical intelligence gathering operations are much more likely to take place against landing sites, where cables make landfall at critical chokepoints, instead of directly on the cables at sea.[56]

The second, more problematic type of activity is the physical destruction of underwater cables. Sabotage can happen as an isolated incident against one particular cable or in the form of a coordinated attack against several cables.[57] Sabotage activities vary depending on the platform and capabilities used.

The weaponization of civilian vessels and anchoring ‘accidents’ represent a key risk associated with cable severing, especially in peacetime. States such as Russia and China employ a fleet of ‘ghost ships’ comprised of fishing, transport, research, or leisure surface vessels to conduct repeated anchoring and dredging activities. This represents an unsophisticated, low-cost operation that can be easily concealed as an accident.

Plausible deniability makes direct attribution harder in practice, especially if there is insufficient monitoring, surveillance, and tracking of unusual behavior at sea. During wartime, military surface assets could also be assigned to anchoring and dredging activities in more coordinated and sophisticated operations.

Another form of physical destruction is the use of underwater assets such as submarines and uncrewed remote-controlled submersibles.[58] Russia and China could use such assets to sever cables by either cutting them with the appropriate equipment or using undersea explosives such as torpedoes, mines, or remote-triggered maritime improvised explosive devices (MIEDs).[59]

There is, however, a technological paradox about the destruction of underwater cables. Closer to coastlines and in shallow waters it is much easier for nefarious states to conduct effective, low-tech, and low-cost dual-use surface cable destruction operations, even though there is a greater risk of being caught and face direct attribution. Conversely, the more deniable and harder to detect operations must take place in deeper waters, where cables are less buried and reinforced, but harder to reach even by high-end underwater assets. Furthermore, states like Russia and China must operate a tradeoff in terms of prioritizing the allocation of their limited underwater assets.

A final form of indirect physical sabotage against underwater cables is linked to the targeting of landing stations and the cable repair and maintenance fleet. Not only are cables themselves at risk of destruction, but also the very support and maintenance infrastructure around them. Future scenarios around cable vulnerability must factor in the deliberate targeting of the cable support infrastructure—for instance, the bombing or coastal assault landing operation against a cable landing site, the destruction of a fleet of repair ships, etc.

Chapter 3: Russia and the Arctic threat environment against underwater cables

3.1—Russia and the Arctic seabed threat environment

On top of the aforementioned suspected activities (*see Chapter 1*), there is a track record of Russian interest in disrupting data cables. Reports of suspicious Russian seabed activities date back to at least the early 2010s. In 2013, a joint Nordic investigation flagged Russia's seabed mapping activities in the Baltic and North Seas, which shed light on the Kremlin's willingness to use civilian vessels to potentially sabotage cables.[60]

Observations continued during Russia's first invasion of Ukraine in 2014-2015 and the illegal annexation of Crimea when Russian forces reportedly damaged communication cables on land.[61] US intelligence and NATO started reporting intense seabed activity around the layout of data cables by Russian submarines as early as 2015.[62] A notable example is the Russian naval exercise which took place close to Ireland's EEZ in February 2022, reported to be a demonstration of cable disruption capabilities.[63]

Cable sabotage is part and parcel of Russia's well-established toolkit of plausibly deniable, sub-threshold activities and other forms of grey zone disruptions. For the Kremlin, cable sabotage is an asymmetric enabler, especially in case of escalation or at the initial period of war, potentially giving Moscow greater decision-making speed against an adversary in the early stages of a conflict. The intended objective is to blunt an opponent's ability to respond by limiting or shutting down military and/or civilian communications at the onset of a conflict.[64]

The Kremlin devolves resources to map submarine cables and conduct intelligence gathering operations. In this effort, seabed warfare has an intelligence function in Russia, and not necessarily a naval one.[65] Cable operations represent an important tool in the informational and psychological preparation of the battlespace, with the aim to break Western civilian support in a potential escalation scenario with Russia.[66]

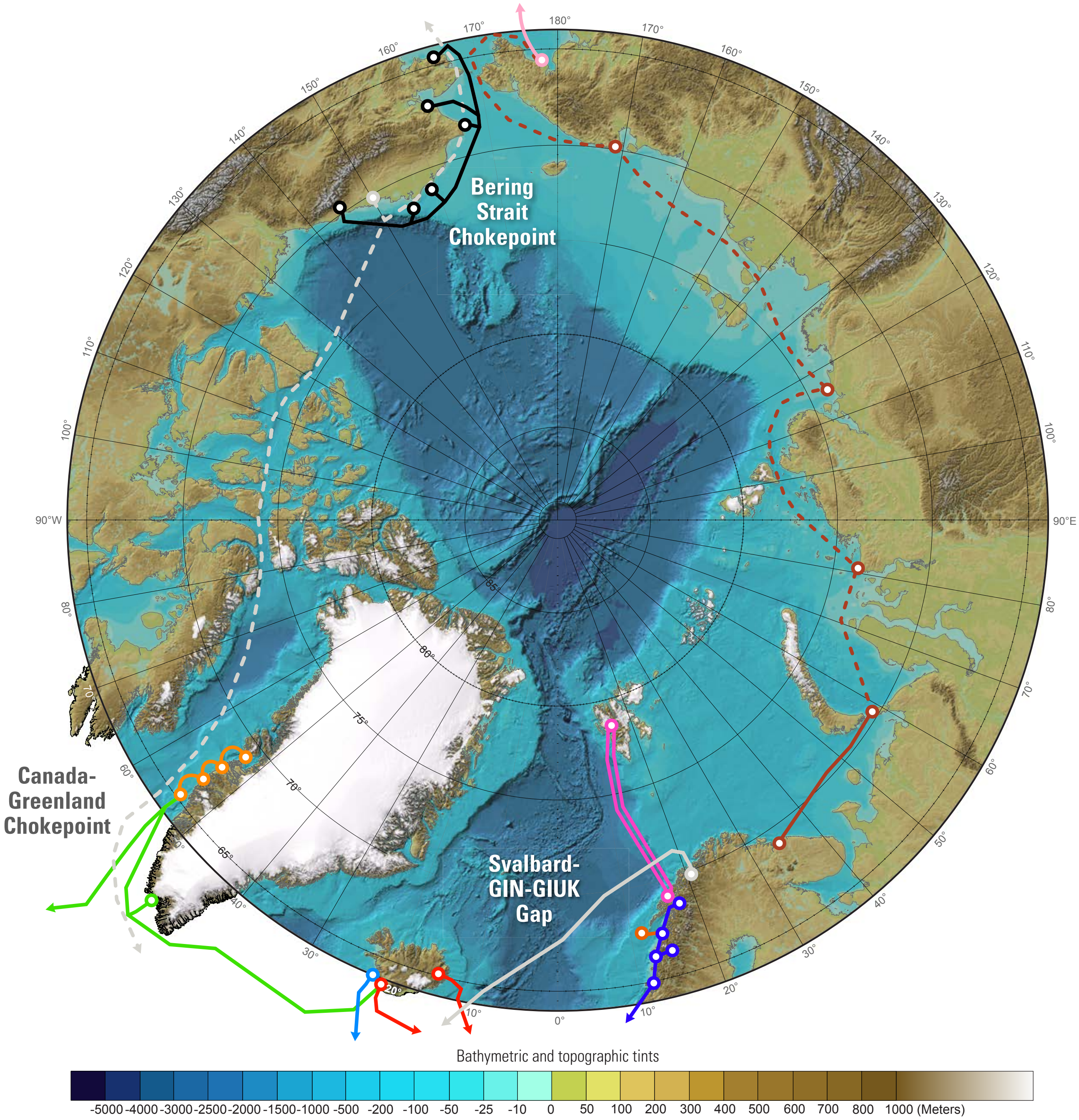
The situation is compounded by the fact that Russia has a strong incentive to probe the seabed in order to test the resolve and response of Western countries and NATO. More provocations and disruptions can therefore be expected in the short and medium terms. In turn, this situation increases the risk of miscalculation, tactical errors, and horizontal escalation.

In an Arctic environment, there are several geographical chokepoints regarding landing stations and the absence of cable redundancy:

1. Around the GIN-GIUK gap and the Svalbard archipelago, where Russia claims to be extending out-of-area interdiction capabilities to hamper access and operation to NATO and its allies,
2. Around the 'Canada-Greenland gap' leading to the North-East passage and by the Labrador Sea, where Russia is also projecting force through strategic bomber overflights and standoff capabilities,
3. Around and across the Bering Strait, between the North Pacific and the Chukchi Sea, where Moscow is projecting interdiction capabilities from the Sea of Okhotsk in the south and between the Chukchi and East Siberian Seas in the north.

These chokepoints feature a mix of shallower waters where Russia could use surface vessels to conduct anchoring and dredging operations as well as deeper Arctic waters where Moscow requires subsurface assets to sabotage cables. The 'Canada-Greenland gap' and the seas across the Bering Strait represent critical chokepoints against US regional infrastructure and under the supervision of NORTHCOM—especially in the context of potential new cable laying in Alaska as well as annual Russian naval exercises off the coast of the Aleutian Islands.[67]

Bathymetric and Submarine Cable Map of the Arctic Ocean


Bering Strait Chokepoint
Canada-Greenland Chokepoint
Svalbard-GIN-GIUK Gap
180°
170°
160°
150°
140°
130°
120°
110°
100°
90°W
90°E
80°
70°
60°
50°
40°
30°
20°
10°
0°
85°
80°
75°
70°
65°
Bathymetric and topographic tints
-5000 -4000 -3000 -2500 -2000 -1500 -1000 -500 -200 -100 -50 -25 -10 0 50 100 200 300 400 500 600 700 800 1000 (Meters)

Source: International Bathymetric Chart of the Arctic Ocean, Submarine Cable Map (Image: Wilson Center)

3.2—Russian structures and units in charge of seabed warfare

The main military intelligence structure in charge of seabed warfare and cable disruption activities is the Main Directorate of Deep-Sea Research (GUGI), also known as Military Unit 40056. Technically independent from the Navy, GUGI is an intelligence and special missions department sitting within the Ministry of Defense.[68] Established in 1965, GUGI is reportedly staffed with personnel from the 29th Separate Submarine Division of the Navy, located with the Northern Fleet naval base at Olenya Guba[69] (north of Murmansk by the Barents Sea).

Among other tasks, GUGI's responsibilities encompass seabed intelligence and operations, and managing the fleet of specialized surface and subsurface assets responsible for seabed operations. [70] GUGI is also charged with maintaining the network of underwater sensors protecting the strategic submarine fleet (*Harmony* surveillance network) as well as naval intelligence operations around Russian naval approaches and beyond.[71]

The multitude of tasks GUGI is mandated to perform may indicate the department is experiencing organizational stretch and, consequently, limited operational tempo for dedicated seabed warfare activities. Because of the overspecialized nature of its missions, GUGI cannot staff easily, therefore limiting the missions it can carry out.[72] The organization must therefore balance between intelligence operations and more aggressive missions against seabed infrastructure requiring specialized assets (especially cable damage operations).

Other Russian structures are also responsible for seabed warfare activities. These include the Intelligence Directorate of the Main Staff of the Russian Navy as well as the Fifth Directorate of the GRU, responsible for military intelligence operations. Since the GRU is more geared towards military operations and GUGI is more suited for naval and seabed-specific tasks, both structures share responsibilities and assets although they assume the similar functions.[73]

In an Arctic context, the Northern Fleet is also in charge, to an extent, of seabed warfare operations—not least because GUGI is staffed with personnel from the 29th Separate Submarine Division (a separate Division of the Northern Fleet). The Division is responsible for special deep-water operations under GUGI's responsibility.[74] Such a situation is undoubtedly creating a complicated distribution of assets and tasks between both structures.[75]

As in the Soviet era,[76] the Northern and the Pacific Fleets are also responsible for operating a fleet of dual-use surface assets in charge of seabed intelligence and sabotage operations—notably fishing and other auxiliary vessels. There is now a track record of such activities by what is described as a fleet of Russian 'ghost ships'.[77] Finally, both Fleets count on special forces units able to conduct seabed sabotage operations.[78]

3.3—Russia’s seabed warfare capabilities

The aforementioned military and intelligence units operate a fleet of specialized assets able to conduct seabed warfare operations and threaten CUI security. Russia can indeed count on both surface and subsurface assets, whether they are manned or autonomous.

GUGI operates the majority of the special purpose subsurface assets. These are adapted to deep-water pressure (notably due to their titanium hulls) and fitted to assume seabed intelligence and warfare functions.[79] Several assets stand out for their capabilities.

The modified Oscar II-class K-329 *Belgorod* nuclear-powered cruise missile submarine (SSGN) is a key asset of GUGI. The *Belgorod* was redesigned in the 2010s from the Oscar II-class with seabed warfare in mind and it can perform a multitude of specialized operations. The *Belgorod* is regularly spotted by Western countries around the Barents Sea and the Kola Peninsula as part of exercises and operations within the Northern Fleet.[80]

The *Belgorod* notably carries the *Poseidon* unmanned underwater vehicle (UUV) armed with a nuclear torpedo. First unveiled in 2015 as the ‘Oceanic Multipurpose System *Status-6*’, the UUV became known in 2018 as *Poseidon* as part of Putin’s ‘super weapons’.[81] The system is mostly designed to increase the scope of Russian sea-based second-strike capabilities as well as mitigate NATO’s missile defense capabilities.

Poseidon UUVs are reportedly propelled by a miniature nuclear reactor, which extends their range considerably.[82] The *Poseidon* is still in development stages[83] and remains far from service entry into the Russian Navy. Both the Northern and Pacific Fleets are expected to receive submarines able to launch *Poseidon* vehicles.

Another key subsurface system is the Project 10831 AS-31 *Losharik* deep-diving nuclear-powered submarine. Under GUGI’s supervision, *Losharik* is launched from the modified Delta IV-class BS-64 *Podmoskovye* SSBN. With an initial design dating date to Soviet times, *Losharik* was built in the 1990s and only launched in 2003. Its unique titanium hull and internal pressure-distribution design allow it to dive and operate at extreme depths.[84]

The special-purpose *Losharik* was specifically designed for seabed warfare; equipped with retractable robotic arms, it can perform seabed infrastructure manipulation operations, including cable cutting. It can also be used for intelligence operations, seabed sensing and surveillance, as well as hydrographic and bathymetric measurements.[85] Furthermore, the *Losharik* was suspected of working on supporting the development of the *Harmony* surveillance system in the Arctic.[86]

The *Losharik* is tragically remembered for the accident in July 2019 that killed 14 crewmembers after an electric failure provoked a fire onboard during docking.[87] Since the accident, the submersible has been undergoing repair work at the Sevmash shipyard,[88] with a planned return to active service by 2025 (although unlikely).

GUGI also manages a fleet of surface vessels, the flagship being the *Yantar* research ship. Disguised as an ‘oceanographic research vessel’, *Yantar* is known to host an array of instruments and sensors likely used for military intelligence and sensing operations, notably around seabed infrastructure[89] and unmapped cables.[90] The ship can host one remotely operated UUV and at least two crewed AS-37 mini-submarines able to reach extreme depths and designed for cable disruption operations.[91] *Yantar* has been deployed around the world since 2015 and a second ‘oceanographic research vessel’, the *Yevgeny Gorigledzhan*, is also in service and conducting surveillance operations.[92]

Beyond GUGI, the Russian Navy is also operating several seabed warfare-specific assets. The *Admiral Vladimirsky* research vessel is suspected of regularly conducting intelligence operations around Arctic waters linked to cable mapping and disruption activities.[93]

Overall, Russia’s cable disruption capabilities appear limited: the Kremlin can only count on a small number of surface and subsurface assets, all of them stretched across a multiplicity of missions and across several intelligence and operations units. Such a situation is therefore naturally limiting the operational tempo and geographical reach of Russian seabed warfare.

Moving forward, it is likely Moscow will focus cable disruptions to more circumscribed operations in known Arctic chokepoints. Peacetime sabotage is more likely to take place in shallower waters or closer to landing stations in order to balance out asset distribution, operational overstretch, and organizational issues between units.[94]

Such operations also require less planning while allowing for cruder capabilities, such as anchoring and dredging. During wartime, the Kremlin would need to distribute seabed warfare assets across a wide range of missions, further increasing the aforementioned risks and making Russian underwater systems less survivable.

Finally, given international sanctions and their impact of the national military industrial base, it is unlikely Russia will be able to deploy a fleet of UUVs anytime soon to conduct designated seabed warfare activities.[95]

China's seabed warfare strategy and capabilities

China is increasingly showing interest in both the development of the underwater cable network and infrastructure as well as in its potential disruption against adversaries. Linked to the Chinese state, HMN Technologies (formerly known as Huawei Marine Networks) is now an industry leader in the deployment and maintenance of submarine cables across the world, with the security implications this poses for the United States and NATO in terms of potential espionage in the fiber optic network.[96]

Through its vast surface and subsurface fleet, China possesses the military capabilities to disrupt and sabotage cables,[97] even though Beijing does not appear to operate many dedicated seabed warfare assets. Considering China's aggressive policy in the South China Sea and the Indo-Pacific region as well as towards Taiwan, Beijing has a strong incentive to increase its presence in the subsea domain and invest in seabed warfare capabilities (notably UUVs for seabed exploration).

Just like Russia, China is also using the pretense of 'maritime scientific research' or 'ocean science' to conduct dual-use activities—including military intelligence gathering around data cables—under the aegis of the Chinese Academy of Sciences and the Ministry of Natural Resources and their fleet of dual-use vessels.[98] The two *Xuelong* icebreakers, managed by the Polar Research Institute of China, for example, might well be employed for dual-use operations, especially seabed surveys and sensing. Finally, China has invested massively in building its network of underwater and seabed sensors, and notably the *Underwater Great Wall* submarine surveillance network.

Considering the low data cable resilience of Taiwan, cable disruption here would represent a low-cost, high-impact operation[99] complementing a blockade of the island—especially at the onset of a potential military operation. Beijing has already been accused in 2023 of conducting anchoring and sand-dredging operations around the Matsu Islands with the clear aim of disrupting data cables in the region.[100]

As regards the Arctic, China had been pushing for the construction of the *Arctic Connect* fiber optic cable, supposed to link Europe and Asia through the Northern Sea Route. The project was halted (if not abandoned) in 2021,[101] but this move revealed Beijing's desire to improve its presence in the regional cable infrastructure, notably for surveillance and intelligence reasons (acoustic sensing, submarine tracking, etc.).[102] The project would. after all. have represented a danger to the integrity of data of Western countries. One thing is obvious: the simple presence of China in the construction and management of Arctic cables would allow Beijing to expand the scope of its cyber disruptions.

The Arctic, however, is not the best region for China to engage in seabed warfare and cable disruption. Indeed, Beijing lacks dedicated capabilities and cold weather technology. Considering China's involvement in the development of the cable infrastructure, the existence of geographical network chokepoints across the region would, in case of disruption, harm Beijing just as much as it hoped to gain from damaging them in the first place. Furthermore, China's vision of Arctic governance is increasingly at odds with Moscow's interpretation of the Northern Sea Route (NSR), as the Kremlin remains the 'gatekeeper' to Beijing's access to Arctic waters through the Pacific.[103]

Chapter 4: Policy impact and recommendations

4.1—Policy impact and Western response

Whether accidental or intentional, disruptions to seabed infrastructure—and specifically the threat to data cables—are not new occurrences. What has changed in the past few years, however, is the sudden policy wake-up call provoked by the Nord Stream gas pipelines explosion in September 2022 as well as subsequent cases of CUI disruption around the North Atlantic and the Baltic Sea (especially the 2023 Balticconnector and cables incident).

It is not certain that Western countries have sufficiently assessed the 'critical' part of 'critical undersea infrastructure', the importance of fiber optic cables, and the need to protect them from foreign interference.[104] If data cables and more widely seabed warfare have now become hot-button issues, policy attention should focus on key priorities to correctly understand the nature of the threat without exaggerating or downplaying it.

National and multilateral responses to recent cable disruptions in an Arctic and Nordic-Baltic environment have so far been relatively robust. The US has been working on the creation of a Cable Security Fleet within the Department of Transportation's Maritime Administration and consisting of US-flagged cable vessels stemming from the private sector.[105] The US Combined Joint Operations from the Sea Centre of Excellence (CJOS CoE) is also reportedly working on the development of a new seabed strategy.

Nordic countries have been strengthening their policies and capabilities for data cable protection.[106] A NATO-EU Task Force on Resilience of Critical Infrastructure was launched in 2023 to address coordination for CUI resilience[107] while the UK-led Joint Expeditionary Force (JEF) will devolve extra resources for the protection of CUI in its area of responsibility.[108]

NATO has been particularly active in the response to cable disruptions. The Alliance set up a new Critical Undersea Infrastructure Coordination Cell (CUICC) in February 2023 as part of NATO HQ in Brussels. The Cell will officially help identify key vulnerabilities as well as "*facilitate engagement with industry and bring key military and civilian stakeholders together*" to mitigate the threat to CUI.[109]

In the wake of the 2023 Vilnius Summit, NATO's Maritime Command (MARCOM) agreed to launch a NATO Maritime Centre for the Security of Critical Undersea Infrastructure.[110] The Centre will be responsible for operational information sharing between NATO members with the objective to develop real-time detection and response capabilities.[111]

Other NATO endeavors include the creation of the Digital Ocean Initiative in 2023, aimed at enhancing the Alliance's Maritime Domain Awareness (MDA) capabilities "*from seabed to space.*"[112] This complements the work done with the private sector through the recently established Defense Innovation Accelerator for the North Atlantic (DIANA) network as well as ongoing discussions taking place with digital industry leaders.

The protection of CUI and data cables in particular is increasingly featured in NATO's operational planning and exercises, as evidenced by the Dynamic Messenger drill that took place in October 2023 off the coast of Portugal. The multi-domain exercise prominently included CUI protection missions, notably through the integration of autonomous underwater vehicles and mine countermeasures.[113]

There is no doubt that the protection of CUI is an integral part of NATO's defense and deterrence posture as well as its endeavor to protect sea lines of communication and defend against grey zone operations.[114] CUI protection now represents a relatively new and dynamic multi-domain process permeating NATO structures. Much remains to be done, however, to achieve a comprehensive picture of the protection of CUI and the deterrence of nefarious attacks.

Moving forward, a key challenge for the Alliance will be to streamline cooperation between the different units and structure in charge of CUI protection (notably between MARCOM and the CUICC), avoid duplication of effort, achieve sufficient information sharing and data fusion, as well as come up with a sound procurement plan in terms of necessary capabilities (notably for MDA).

4.2—Recommendations and policy pathways

Cable disruption activities by nefarious state actors is proverbially uncharted territory. National policymakers and multilateral, including industrial, stakeholders must find the appropriate balance of response in terms of governance, deterrence, and technology-enabled capabilities.[115]

The aim is to make data cables more resilient and better mitigate damage to the network, while deterring attacks from happening in the first place. Global and effective deterrence against cable disruptions will require consistent Western policy across the myriad aspects of cable protection.

Make critical undersea infrastructure genuinely 'critical'

Civilian and military policy responses must factor in the criticality of underwater cables. As cable disruption fundamentally sits across several domains (sea, land, cyberspace) and sectors (cables themselves, landing stations, repair ships, etc.), their protection should be designated 'critical' in terms of US national security priority.[116]

From a military security standpoint, individual nations must conduct cable infrastructure risk assessments to strengthen its resilience.[117] Nations should also aim to develop dedicated seabed warfare strategies, taking after France[118] and the United Kingdom,[119] to increase preparedness and response to cable disruption. For the US, such an effort could be coordinated as part of the Implementation Plan for the 2022 National Strategy for the Arctic Region (NSAR).

Another part of the debate is to determine whether CUI should be made a full-fledged operational domain of war. Doing so would help individual countries and NATO incorporate the protection of data cables into military doctrine as well as craft better deterrence policies. The drawback is the risk of militarizing the response to cable disruption and potentially change the nature of the legal and normative conversation around cable governance.

NATO should consider updating its Maritime Strategy, already dating back to 2011,[120] to incorporate the protection of CUI more prominently. To this end, the Alliance could create a dedicated Standing NATO Maritime Group (SNMG) focused on CUI protection, especially in an Arctic and Baltic environment.[121] NATO should also focus on widening the scope of multi-domain exercises aimed at protecting data cables or deterring an attack.

Increase cooperation and information sharing between allies

Information sharing between allies and data fusion within NATO are key to understanding the nature of the threat against CUI as well as anticipating future disruptions against underwater cables. Existing endeavors require more depth and coordination to achieve intended effects and avoid duplication of efforts. More regular and dedicated contacts on CUI disruption are necessary between nationals and multilateral structures, notably between coast guards of respective nations.

Nations and multilateral stakeholders should increase the level of cooperation with industrial actors in charge of operating and maintaining the network of fiber optic cables. The aim is to create more synergies with the private sector regarding information sharing, early warning systems, sensing capabilities, and response to disruptions. Government-industry data fusion and cooperation are paramount to the resilience of data cables. The situation is compounded by the fact that neither can achieve full resilience on their own: while nations protect and deter, the industry detects, maintains, and repairs.

From a national security standpoint, governments should also ensure that the private sector does not rely on the technology of foreign companies whose governments are known to engage in cable disruption and espionage. This situation particularly applies to China, with the *Arctic Connect* example in mind.

In the context of the US NSAR, there remains a lot to be done across the United States government to increase data sharing between agencies. A potential place to start would be to increase the level of information sharing and data fusion on cables between NORTHCOM and the US Coast Guard (USCG).

Create a comprehensive legal regime around data cables

Current legal provisions are insufficient to ensure the protection of underwater cables. National and international legal frameworks must be strengthened to increase the protection of data cables and translate them into policy. 'Patching' legal and normative gaps in existing texts would be the first place to start and would help achieve greater clarity over the current legal regime. For instance, there is potential to expand UNCLOS with an additional protocol for the domestic criminalization of intentional cable damage.

To strengthen international cable protection, the US should consider pioneering discussions around the creation of an international legal treaty defining the 'rules of the road' regarding cable disruption during peacetime and wartime. Such a body of law would also have to address critical questions left unanswered to this day—such as the potential prohibition of cable damage, the neutrality of cables (notably to avoid adverse effects against countries not party to a conflict), etc.

Those discussions would greatly benefit from the learning curve of legal and normative provisions existing in cyberwarfare and space—such as responsible state behavior, easier attribution, etc. Conversely, the cyberwarfare regime would also benefit from systematically including the protection of data cables, as they have been generally overlooked in cyberwarfare discussions.

Craft dedicated cable disruption deterrence policies

The deterrence against cable disruption and damage by nefarious state actors must be streamlined and fully integrated into US and NATO thinking.[122] Deterrence by denial can be ensured through credible presence, notably more naval patrols, and dedicated NATO-led exercises, including in the Arctic.

However, the most efficient tool for deterrence by denial is seabed domain awareness around data cables. The development and procurement of seabed-dedicated capabilities and overall Maritime Domain Awareness (MDA) technologies will help monitor, deter, and mitigate potential cable disruption and damage. Obtaining a comprehensive seabed and maritime picture further helps understand the nature of the threat and the capabilities needed to respond.

In terms of capabilities, the deployment of surface and subsurface assets (notably UUVs) alone is not sufficient to achieve full seabed awareness.[123] The United States and NATO should encourage and help private cable industry actors to develop and procure seabed-specific capabilities for advanced remote fiber sensing and early warning detection systems. US resource allocation should systematically factor this in, especially in the context of the NSAR.

The aim is to achieve real-time detection capabilities that, together with streamlined government-private data fusion, will provide quicker response and data traffic management. The advent of big data analytics, AI-enabled tools, and machine learning also help maritime anomaly detection around data cables and early warning.[124]

In terms of national resource allocation, the US and its allies must invest in CUI monitoring capabilities such as surveillance sensors, underwater acoustic sensors, coastal radars, next generation Automatic Identification System (AIS) tracking technology, satellite sensors, etc. Technology will ultimately help achieve NATO's objective of seabed-to-space situational awareness (S3A) in terms of multi-domain data fusion.[125]

Better overall awareness also means easier attribution in case of an attack (*see below*). This is particularly relevant in and around Arctic waters, considering the presence of geographical chokepoints, potential gaps in radar and sensor coverage, and the low resilience of data cables.

Deterrence by denial should also rest on strengthening the resilience of the underwater cable network. Better resilience can be achieved by first acknowledging the existence and then protecting known geographical cable chokepoints and areas where there is little redundancy—this is paramount in the context of Arctic-related cables.

As these capabilities are vulnerable, resilience can be increased by protecting landing stations onshore and in the cyberspace.[126] Of particular importance, the United States should conduct a thorough, updated assessment of the security of all cable landing sites in order to patch existing gaps.

Resilience will only be achieved if the private fleets of maintenance and repair ships are strong, efficient, and protected. The United States and its allies should encourage discussions with cable industry leaders to streamline the division of labor for the maintenance and repair of cables in case of intentional damage.

In-country resilience starts with defining the interaction between civilian repair capabilities and naval forces—for instance, military escorts for repair ships, operating modular vessels for joint emergency operations,[127] embarking repair specialists on military surface assets, or training military specialists and deck officers to cable repair work, etc.

Finally, deterrence against cable disruption requires improved deterrence by punishment, with the objective of raising the cost of a potential attacks by ensuring a strong and swift response. Credibly messaging deterrence is paramount: the United States and its allies should systemically make it clear to potential perpetrators that nefarious acts against CUI in peacetime will bring a strong response.

Furthermore, the United States and its allies should consider increasing the cost of grey zone seabed warfare disruption during peacetime—for instance, by more severely punishing vessels navigating with their AIS or VMS transponders switched off or displaying anomalous trajectories and behavior.

Thanks to modern technology, the active tracking of anomalous AIS and VMS behavior should lead to more proactive attribution. The United States and its allies should more proactively detect unusual behaviors from surface assets, especially if they take place around known data cable layouts.

Unusual patterns of behavior (especially if transponders are off and/or if known 'risk ships' are present) are generally indicative of a willingness to engage in cable disruption activities. Such situations should automatically lead either to a 'prebuttal' (before any disruption occurs) through the use of declassified intelligence or be immediately attributed, should damage occur.

A strong, coordinated, and proactive attribution against such anomalous behavior will help maintain credibility around the protection of data cables, especially at NATO level, and help deter future attacks,[128] as long as it is followed by unequivocal policy repercussions for the perpetrators.

Endnotes

1 Christian Bueger and Tobias Liebetrau (2023), Critical maritime infrastructure protection: What's the trouble?, *Marine Policy*, Issue 155, September 2023.

2 White House (2023), Implementation Plan For The 2022 National Strategy For The Arctic Region, October 18, 2023.

3 More information on data cables is available in TeleGeography, '*Submarine Cable Frequently Asked Questions'* and in Dennis E. Harbin III (2021), Targeting Submarine Cables: New Approaches To The Law Of Armed Conflict In Modern Warfare.

4 Douglas R. Burnett *et al.*, eds. (2014), Submarine Cables: The Handbook of Law and Policy.

5 TeleGeography, '*Submarine Cable Frequently Asked Questions'*

6 Nadia Schadlow and Brayden Helwig (2020), Protecting undersea cables must be made a national security priority, *Defense News*, 1 July 2020.

7 Giovanni Soldi *et al.* (2023), Monitoring of Underwater Critical Infrastructures: the Nord Stream and Other Recent Case Studies, *Aerospace and Electronic Systems Magazine*, 38:10, October 2023.

8 Most undersea fiber-optic cables can reach average speeds of up to 200-250 Tbps (Terabit/second) while the Starlink satellite system, for instance, reaches download speeds of about 25-220 Mbps (Megabit/second). See https://www.starlink.com/legal/documents/DOC-1400-28829-70

9 Colin Wall and Pierre Morcos (2021), Invisible and Vital: Undersea Cables and Transatlantic Security, Commentary, *CSIS*, 11 June 2021.

10 Rishi Sunak (2017), Undersea Cables: Indispensable, insecure, *Policy Exchange*.

11 Garrett Hinck (2018), Evaluating the Russian Threat to Undersea Cables, *Lawfare Media*, 5 March 2018.

12 Camino Kavanagh (2023), Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour, *UNIDIR*; Olga Wasiuta (2023), Russian Threats To The Submarine Internet Cable Infrastructure, *Zeszyty Naukowe Sgsp*, September 2023.

13 Bueger and Liebetrau (2023), *op. cit.*

14 Jonathan E. Hillman (2021), Securing the Subsea Network A Primer for Policymakers, *CSIS*.

15 Sunak (2017), *op. cit.*; International Cable Protection Committee (2021), Submarine Cable Protection and the Environment, Issue #2, March 2021.

16 Soldi *et al.* (2023), *op. cit.;* Dimitrios Eleftherakis and Raul Vicen-Bueno (2020), Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors, *Sensors*, 20, 737.

17 AP News, *3 Red Sea data cables cut as Houthis launch more attacks in the vital waterway*, 4 March 2024.

18 Sophie Ryan (2023), Submarine Communication Cables and Belligerent Rights in Armed Conflict, *SSRN*, April 2023.

19 For instance, a comprehensive map of cables is available here: https://www.submarinecablemap.com/

20 Sunak (2017), *op. cit.*

21 EU Parliament (2022), Security threats to undersea communications cables and infrastructure – consequences for the EU, April 2022.

22 Burnett *et al.*, eds. (2014), *op. cit.*

23 Soldi *et al.* (2023), *op. cit.*; EU Parliament (2022), *op. cit.*

24 United Nations Convention on the Law of the Sea (UNCLOS), Article 113.

25 For more information, see Kavanagh (2023), *op. cit.*

26 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017), Cambridge University Press.

27 Oslo Manual on Select Topics of the Law of Armed Conflict : Rules and Commentary (2020), *Springer Nature.*

28 Sunak (2017), *op. cit.*

29 Ryan (2023), *op. cit.*; Kavanagh (2023), *op. cit.*

30 Sarah Kuszynski (2022), The Geopolitics of Undersea Cables: Underappreciated and Under Threat, *London Politica*, December 2022; Kavanagh (2023), *op. cit.*

31 NATO Parliamentary Assembly (2023), Protecting Critical Maritime Infrastructure – The Role Of Technology, General Report, Njall Trausti Fridbertsson (Iceland), General Rapporteur.

32 The War Zone, *Norwegian Undersea Surveillance Network Had Its Cables Mysteriously Cut*, 11 November 2021.

33 Runar Spansvoll (2023) Studying Moscow's Coercive Campaign Against Norway, *The RUSI Journal*, 168:3, 74-85.

34 The Barents Observer, *Disruption at one of two undersea cables to Svalbard*, 9 January 2022.

35 Niels Nagelhus Schia, Lars Gjesvik and Ida Rødningen (2023), The subsea cable cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed?, *NUPI Policy Brief*, 1/2023.

36 BBC, *Damaged cable leaves Shetland cut off from mainland*, 20 October 2022.

37 Kuszynski (2022), *op. cit.*

38 Shetland News, *Governments knew what caused October communication outage but never told the public*, 19 January 2023.

39 The Barents Observer, *Russian, Chinese ships spotlighted by Finnish police after pipeline damage, are now pairing up outside northern Norway*, 18 October 2023.

40 Police of Finland, *National Bureau of Investigation has clarified technically the cause of gas pipeline damage*, 24 October 2023.

41 Government Offices of Sweden, *Damaged telecommunications cable between Sweden and Estonia*, 19 October 2023.

[42] RFE/RL, *Hunt For Answers Continues Over Chinese Ship's Suspected Role In Damaging Baltic Pipeline,* 2 November 2023.

[43] Kristina Spohr with Laurel Baker (2023), Sanctions, Shipping, and Sabotage: China and Russia Enter the 'Gray Zone' in the Baltic Sea, *Wilson Center*, Polar Perspective no. 14, November 2023.

[44] Rosatom, Information on the movement of vessels on the approaches to the water area and in the water area of the Northern Sea Route, https://nsr.rosatom.ru/operativnaya-informatsiya/informatsiya-o-dvizhenii-sudov-na-podkhodakh-k-akvatorii-i-v-akvatorii-severnogo-morskogo-puti-sosto/?arrFilter_ff%5BNAME%5D=&arrFilter_DATE_ACTIVE_FROM_1=03.11.2023&arrFilter_DATE_ACTIVE_FROM_2=&set_filter=Y ; The Barents Observer, *Newnew Polar Bear sails towards Bering Strait*, 6 November 2023.

[45] Spohr (2023), *op. cit.*

[46] Michael Sechrist (2010), Cyberspace In Deep Water: Protecting Undersea Communication Cables By Creating an International Public-Private Partnership, *Harvard Kennedy School*, March 2010.

[47] Wall and Morcos (2021), *op. cit.*

[48] International Law Studies (2023), *Newport Manual on the Law of Naval Warfare.*

[49] French Ministry of Defense (2022), *Seabed warfare strategy*, February 2022.

[50] Frank Jüris (2020), Handing over infrastructure for China's strategic objectives: 'Arctic Connect' and the Digital Silk Road in the Arctic, *Sinopsis*, March 2020.

[51] Harbin (2021), *op. cit.*

[52] Sunak (2017), *op. cit.*

[53] Katarina Kertysova and Gabriella Gricius (2023), Countering Russia's Hybrid Threats in the Arctic, *European Leadership Network*, August 2023; NATO Parliamentary Assembly (2023), *op. cit.*

[54] House of Lords International Relations and Defence Committee (2023), Corrected oral evidence: The Arctic, Testimony by Dr. Sidharth Kaushal and Dr. Lee Willett, Wednesday 5 July 2023.

[55] EU Parliament (2022), *op. cit.*

[56] Wall and Morcos (2021), *op. cit.*

[57] Morten Soendergaard Larsen (2023), Russian 'Ghost Ships' Are Turning the Seabed Into a Future Battlefield, *Foreign Policy*, May 2023.

[58] NATO Parliamentary Assembly (2023), *op. cit.*

[59] EU Parliament (2022), *op. cit.*

[60] Kertysova and Gricius (2023), *op. cit.*

[61] Justin Sherman (2022), Cord-cutting, Russian style: Could the Kremlin sever global internet cables?, New Atlanticist, *Atlantic Council,* 31 January 2022; Reuters, *Ukraine says communications hit, MPs phones blocked,* March 2014.

[62] The New York Times (2015), *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*, 25 October 2015; BBC, *Russia a 'risk' to undersea cables, defence chief warns,* 15 December 2017.

[63] Soldi *et al.* (2023), *op. cit.*

[64] EU Parliament (2022), *op. cit.*; Wall and Morcos (2021), *op. cit.*

[65] Sidharth Kaushal (2023), Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure, RUSI, May 2023.

[66] *Ibid.*

[67] High North News, *Military Vessels From Russia and China Recently Operated Near Alaska*, 7 August 2023.

[68] Michael Kofman (2019), Fire aboard AS-31 Losharik: Brief Overview, *Russia Military Analysis,* 3 July 2019.

[69] Kaushal (2023), *op. cit.*

[70] French Ministry of Defense (2022), *op. cit.*

[71] Kaushal (2023), *op. cit.*; House of Lords International Relations and Defence Committee (2023), *op. cit.*

[72] House of Lords International Relations and Defence Committee (2023), *op. cit.*

[73] Kaushal (2023), *op. cit.*

[74] Army Recognition, *Russian Northern Fleet Creates Submarine Division for Deep-Water Operations*, 27 April 2018.

[75] Hotaka Nakamura (2023), The Enemy Below: Fighting against Russia's Hybrid Underwater Warfare, *Center for Maritime Strategy*, 29 June 2023; House of Lords International Relations and Defence Committee (2023), *op. cit.*

[76] Byung Ki Kim (1988), Moscow's South Pacific Fishing Fleet Is Much More Than It Seems, *Heritage Foundation,* September 1988.

[77] Larsen (2023), *op. cit.*; *Skyggekrigen* documentary, https://www.drsales.dk/programmes/putin-s-shadow-war/

[78] Mathieu Boulègue (2019), Russia's Military Posture in the Arctic: Managing Hard Power in a 'Low Tension' Environment, *Chatham House - Royal Institute of International Affairs*; Kaushal (2023), *op. cit.*

[79] A detailed list of assets is available in Kofman (2019), *op. cit.*

[80] US Naval Institute News, *Russian Doomsday Sub Belgorod Spotted in the Arctic*, 5 October 2022.

[81] Richard Connolly (2021), Putin's 'super weapons', in Chatham House, Advanced Military Technology in Russia, *Chatham House - Royal Institute of International Affairs.*

[82] Izvestiya, *'«Poseydon» v lodke: submarinu gotovyat k ispytaniyam yadernykh robotov.'*, 11 February, 2021, https://iz.ru/1123160/anton-lavrov-aleksei-ramm/poseidon-v-lodke-submarinu-gotoviat-k-ispytaniiam-iadernykh-robotov

[83] Reuters, *Russia produces first set of Poseidon super torpedoes - TASS,* 16 January 2023.

[84] Kofman (2019), *op. cit.*; Kaushal (2023), *op. cit.*

[85] Wasiuta (2023), *op. cit.*

[86] Jüris (2020), *op. cit.*

[87] Fontanka, *'Ogon, batapeiya'*, 9 July 2010, https://www.fontanka.ru/2019/07/08/098/?utm_source=yxnews&utm_medium=desktop

[88] The War Zone (2019), *Russia's Fire-Damaged "Losharik" Spy Submarine Heads For Repairs As New Details Emerge*, 16 August 2019.

[89] Nakamura (2023), *op. cit.*

[90] The New York Times, *Russian Ships Near Data Cables Are Too Close for U.S.*, 25 October 2015.

[91] Hinck (2018), *op. cit.*; Harbin (2021), *op. cit.*

[92] NL Times, *Russian ship suspected of espionage spotted off Dutch coast,* 20 October 2023.

[93] Larsen (2023), *op. cit.*

[94] House of Lords International Relations and Defence Committee (2023), *op. cit.*

[95] French Ministry of Defense (2022), *op. cit.*

[96] Kuszynski (2022), *op. cit.*

[97] EU Parliament (2022), *op. cit.*

[98] French Ministry of Defense (2022), *op. cit.*

[99] PBS, *Taiwan blames Chinese ships for cut internet cables*, 8 March 2023.

[100] Wen Lii (2023), After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience, *The Diplomat*, 15 April 2023.

[101] Alexandra Middleton and Bjørn Rønning (2022), Geopolitics of Subsea Cables in the Arctic, *The Arctic Institute*, 2 August 2022.

[102] Jüris (2020), *op. cit.*

[103] Mathieu Boulègue (2022), The militarization of Russian polar politics, *Chatham House - Royal Institute of International Affairs*, June 2022.

[104] Kertysova and Gricius (2023), *op. cit.*

[105] Office of the Law Revision Counsel of the United States House of Representatives, Chapter 532—Cable Security Fleet, https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title46-chapter532&edition=prelim

[106] Larsen (2023), *op. cit.*

[107] European Commission, *EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure*, Press release, 29 June 2023.

[108] Ministry of National Defense of Lithuania, *JEF Response Option activated to address regional critical infrastructure security*, 28 November 2023.

[109] NATO, *NATO stands up undersea infrastructure coordination cell,* 15 February 2023.

[110] NATO MARCOM, *NATO focus is on Critical Undersea Infrastructure during series of multi-domain exercises with latest autonomous vehicles in Portugal,* 4 October 2023.

[111] NATO Parliamentary Assembly (2023), *op. cit.*

[112] NATO, *NATO Defence Ministers launch initiative to enhance maritime surveillance capabilities,* 12 October 2023.

[113] NATO MARCOM, *NATO focus is on Critical Undersea Infrastructure during series of multi-domain exercises with latest autonomous vehicles in Portugal,* 4 October 2023.

[114] Monaghan *et al.* (2023), *op. cit.*

[115] Bueger and Liebetrau (2023), *op cit.*

[116] International Cables Protection Committee, *Best Practices For Protecting And Promoting Resilience Of Submarine Telecommunications Cables*, Version 1.2.

[117] Wall and Morcos (2021), *op. cit.*

[118] French Ministry of Defense (2022), *op. cit.*

[119] UK Centre for Seabed Mapping, https://www.admiralty.co.uk/uk-centre-for-seabed-mapping

[120] NATO, *Alliance Maritime Strategy*, March 2011.

[121] Monaghan *et al.* (2023), *op. cit.*

[122] *Ibid.*

[123] Eleftherakis and Vicen-Bueno (2020), *op. cit.*

[124] Soldi *et al.* (2023), *op. cit.*

[125] Paolo Braca (2023), Multi Domain Situational Awareness Seabed to Space Situational Awareness (S3A), *NATO Science and Technology Organization, Center for Maritime Research and Experimentation*, March 2023.

[126] Wall and Morcos (2021), *op. cit.*

[127] Bueger and Liebetrau (2023), *op cit.*

[128] Spohr (2023), *op. cit.*

This publication was sponsored by the Homeland Defense Institute. The views expressed in this publication do not necessarily represent the views of the United States Air Force Academy, North American Aerospace Defense Command and United States Northern Command, the Department of Defense, or the United States Government.

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004–3027

Wilson Center

🌐 wilsoncenter.org
f woodrowwilsoncenter
𝕏 @TheWilsonCenter
📷 @thewilsoncenter
in The Wilson Center

Polar Institute

🌐 wilsoncenter.orgpolar-institute
✉ polar@wilsoncenter.org
f facebook.com/ThePolarInstitute
𝕏 @polarinstitute
📳 202.691.4320