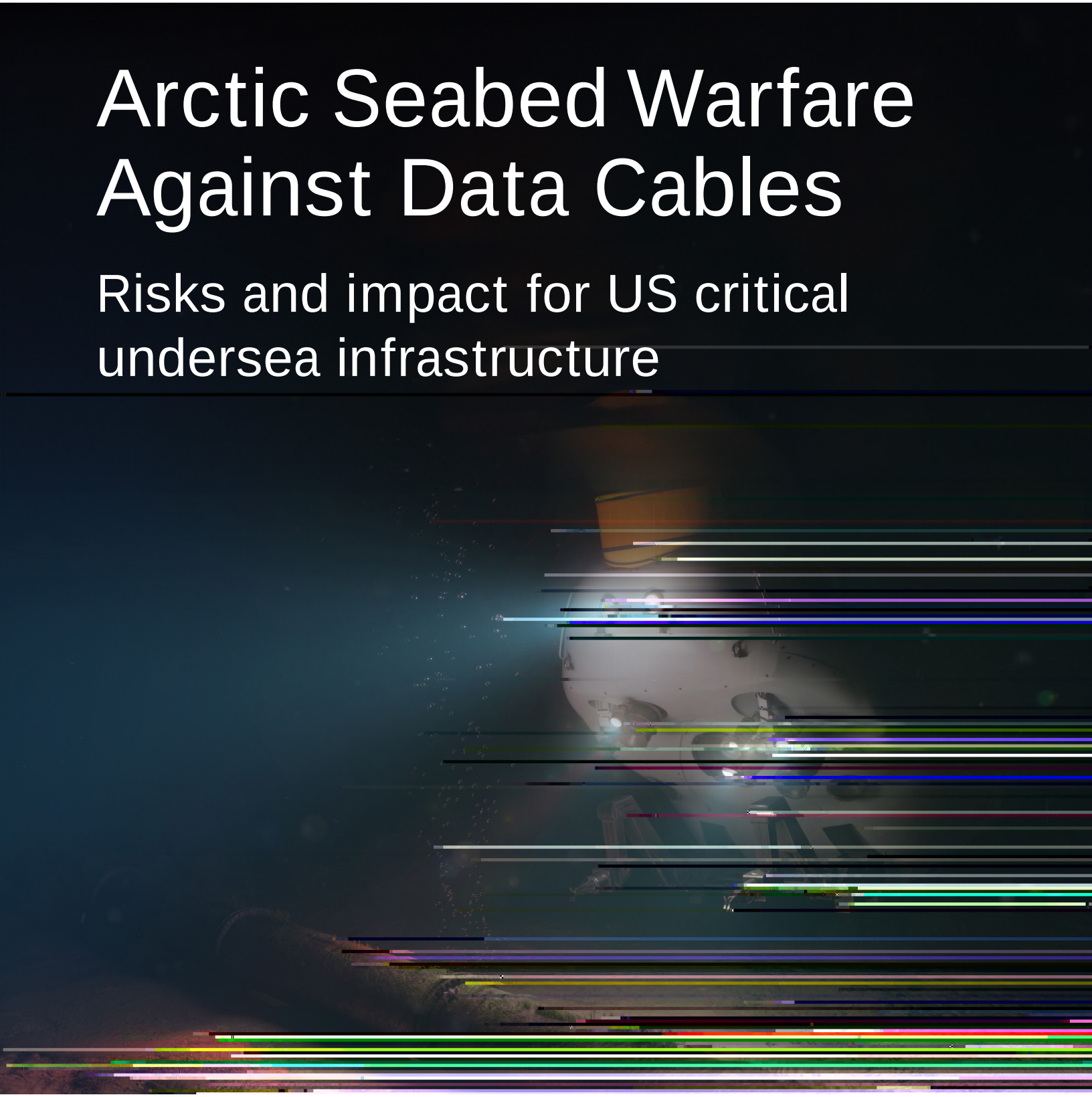
Wilson Center

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.
- E□cient 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 insu□cient 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 e□ects 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 nat

- These chokepoints feature a mix of shallower waters where Russia in particular could use surface vessels

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 NArdep gs/T1 (he security and mil)/Mthm1 ()soc/I43/10 0 BDC BCID 2407e

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 tra□c (between 97 to 99% of tra□c)[5] throughout the world including banking operations, the digital economy, and, more critically, military communication. Cable tra□c 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 tra□c: they are much faster, more e□cient, and more capable than satellite communication.[8] Driven by the digital economy and the constant need for faster network bandwidth, cable tra□c 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'*

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

The October 2023 joint incidents in the Baltic Sea, a□ecting 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

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 e□ective, 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 tradeo□ 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.

These chokepoints feature a mix of shallower waters where Russia could use surface vessels to conduct an1rr

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

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 su□ciently 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

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 e□ects and avoid duplication of e□orts. 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

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 o□cers 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 o□ 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 o□ 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

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_%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 NetwIText missing*

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 O□ce 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 P□63upC□Span□actualText□EEFF□BDC □F□□(.)TjEM□□Td6jEMn5er□.*