10.6326/NDJ.202506_40(2).0001

關鍵海底基礎設施保護：北約的利益與企圖

NATO and Critical Undersea Infrastructure Protection: What Interest and Ambition?

布魯克．史密斯—溫莎 (Brooke Smith-Windsor)

歐洲蘭德公司前資深防衛、安全與基礎設施首席研究員

摘 要

作爲當代最具影響力且歷史最悠久的集體防衛同盟，北約(NATO)常被視爲多國軍事應對威脅的典範。本文聚焦其最新的安全議題：因應近期歐洲多起能源管線與通信電纜異常中斷事件，所引發的對關鍵海底基礎設施遭破壞與間諜活動的關切。本文從2023年維爾紐斯峰會(Vilnius Summit)的關鍵決策出發，結合北約的地緣特性、職權範圍與三大核心任務（威懾與防衛、合作安全，以及危機預防與管理）探討該同盟及其32個成員國在全球海底空間防護角色的演變。總之，本文闡明了北約作爲一個致力於維護海底規則型國際秩序的全球軍事聯盟，如何展現其決心與作爲，無論是對盟友還是潛在對手而言，皆具有深遠意義。

關鍵詞：北約、海底基礎設施、能源管線、通信電纜、維爾紐斯峰會

Abstract

Contemporary history's most enduring collective defence alliance, the North Atlantic Treaty Organization (NATO), often is referred to as the "gold standard" for multinational military response to threats to international order. This paper explains the latest addition to its inventory of security concerns: sabotage and espionage of critical undersea infrastructure (CUI) following a spate of suspicious disruptions to energy pipelines and communication cables in the European theatre. Proceeding from the seminal decisions of the 2023 Vilnius Summit, the paper considers NATO's geography, jurisdiction, and three core tasks (deterrence and defence, cooperative security, and crisis prevention and management) to explore the evolving role of the alliance and its 32 member states in the protection of the world's undersea domain. In sum, it sheds light on what friends and challengers alike may expect from this global military actor prepared to uphold the rules-based international order on the ocean floor.

Keywords: NATO, Undersea Infrastructure, Energy Pipeline, Communication Cable, Vilnius Summit

Introduction

The North Atlantic Treaty Organization (NATO) released its maritime strategy in 2011. Heralding an era of cooperative "interdependence between states," the strategy paid scant attention to possible interstate contestation, never mind warfare on the world's seabed. A passing reference to trans-oceanic telecommunications cables, pipelines and valuable resources lying in, on or beneath the ocean floor was joined by one espousing the general importance of maintaining critical infrastructure.[1] Fast forward to 2023 and NATO's Vilnius Summit elevates the protection of "critical undersea infrastructure" (CUI) to a strategic priority.[2] The pronouncement followed NATO's Strategic Concept released the previous year that proclaimed a return to global strategic competition wherein "malign actors seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities." Henceforth, NATO and its member states resolved "to deter, defend, contest and deny across all domains and directions."[3]

NATO's Vilnius Summit elevates the protection of critical undersea infrastructure to a strategic priority.

Why the change? The return of full-scale war in Europe (Ukraine) and a threatening Russian Federation is the overarching context. The specific one is the rise in suspected deliberate ruptures to undersea gas pipelines and telecommunication cables in the North Atlantic Area, possibly with Russian involvement. 2022 witnessed suspicious damage to the Space Norway subsea fiberoptic cable and the well-publicized Nord Stream gas pipelines explosions. Other incidents in NATO member states' Exclusive Economic Zones (EEZs) followed—Balticonnector and EE-S1 in 2023 and more recently C-Lion-1 and ESTLINK2 in 2024.[4] With 99 percent of the world's internet communications passing through undersea cables since the fiberoptic revolution of the 1980s,[5]

1 NATO, *Alliance Maritime Strategy*, 11 March 2011, para. 4, 5, https://www.nato.int/cps/ua/natohq/official_texts_75615.htm

2 NATO, *Vilnius Summit Communique*, 11 July 2023, para. 65, https://www.nato.int/cps/ge/natohq/official_texts_217320.htm

3 NATO, 2022 *Strategic Concept*, 29 June 2022, para. 15, 20, https://www.nato.int/strategic-concept/

4 Illia Kabachynskyi, "As Energy and Communications Cables Are Cut All Over the Baltic Sea, Hybrid Warfare Takes Hold," *UNITED24 Media*, 15 January 2025, https://united24media.com/war-in-ukraine/as-energy-and-communications-cables-are-cut-all-over-the-baltic-sea-hybrid-warfare-takes-hold-5111;
Laura Gozzi, "Nato launches new mission to protect crucial undersea cables," *BBC News*, 14 January 2025, https://www.bbc.com/news/articles/c4gx74d06ywo;
Shaun Walker, "Nato to boost Baltic Sea presence after suspected sabotage of underwater cable," *The Guardian*, 27 December 2024, https://www.theguardian.com/world/2024/dec/27/estonia-begins-naval-patrols-to-protect-cable-after-suspected-sabotage-finland;

it is no surprise that CUI is a newfound strategic concern. As the deputy commander of NATO's Allied Maritime Command (MARCOM) has remarked: "We know the Russians have developed a lot of hybrid warfare under the sea to disrupt the European economy, through cables, internet cables, pipelines…All our links between the US, Canada and Europe are transmitting under the sea, so there are a lot of vulnerabilities." [6] Those susceptibilities extend to offshore windfarms and oil rigs needed for energy security, as well as seabed mining infrastructure. NATO's fresh preoccupation with the undersea environment is intensified by what its Parliamentary Assembly and others have observed as a proliferation of transformative undersea technology (e.g. autonomous systems) capable of defensive as well as hostile operations.[7] The CUI seascape is further complicated by the fact that the majority of CUI is in private sector hands, multiple jurisdictions are at play (territorial sea, EEZs, contiguous zones, continental shelf, "The Area" of the deep seabed), and detailed knowledge of the globe's seabed remains largely unknown (80 percent of the world's ocean floor is unmapped).[8] To address the challenges, in 2024 NATO Headquarters inaugurated the CUI "Network" of public and private stakeholders under the auspices of the Assistant Secretary General for Innovation, Hybrid and Cyber.[9] Operationally, MARCOM in the same year launched the NATO Maritime Center for CUI.[10] What is more, in 2025, it initiated a dedicated operation, Baltic Sentry, to surveil and deter further disruption to

---

Cynthia Mehboob, "NATO's best-laid subsea security plans," *The Interpreter*, 20 November 2024, https://www.lowyinstitute.org/the-interpreter/nato-s-best-laid-subsea-cable-security-plans;
Helga Kalm, "NATO's Path to Securing Undersea Infrastructure in the Baltic Sea," *Emissary*, 29 May 2024, https://carnegieendowment.org/research/2024/05/nato-baltic-sea-security-nord-stream-balticconnector?lang=en

5 Robert Martinage, "Under the Sea: The Vulnerability of the Commons," *Foreign Affairs* 94 no. 1 (2015), 118-119.

6 Miranda Bryant, "Undersea "hybrid warfare" threatens security of 1bn, Nato commander warns," *The Guardian*, 16 April 2024, https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns

7 Njall Trausti Fridbertsson, *2023–General Report–Protecting Critical Maritime Infrastructure–The Role of Technology*, 032 STC 23 E rev.2 fin (Brussels: Science and Technology Committee, 2023), 7-8, https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc; Elio Calcagno, "The Underwater Environment and Europe's Defence and Security. The Underwater Domain," *Documenti IAI* 23 no. 13 (2023), 9-10.

8 Nippon Foundation, *The Nippon Foundation GEBCO Seabed 2030 Mission Statement*, 2018, https://www.gebco.net/documents/seabed2030_brochure.pdf

9 Anna Ribeiro, "NATO conducts initial meeting for undersea infrastructure network to boost security against rising threats," *Industrial Cyber*, 28 May 2024, https://industrialcyber.co/threats-attacks/nato-conducts-initial-meeting-for-undersea-infrastructure-network-to-boost-security-against-rising-threats/

10 NATO, Allied Maritime Command, Media Centre, "NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure," *News*, 28 May 2024, https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui

CUI in the Baltic Sea.[11]

This paper explores key factors shaping NATO's engagement in CUI protection. It unpacks the Vilnius Summit's pledge of a "collective commitment" to safeguarding CUI.[12] Following an appreciation of the threats, the paper considers NATO's prospective role in addressing them from three perspectives: geography ("North Atlantic Area" and beyond); jurisdiction (member states' territorial seas/EEZs, and "The Area"); core tasks (deterrence and defence, cooperative security, and crisis prevention and management). The purpose is to clarify and inform NATO's interest and level of ambition in this evolving maritime domain.

Threats to Critical Undersea Infrastructure

As a defensive military alliance of 32 European and North American states, NATO's role in CUI protection and security necessarily begins with an appreciation of the threats to inform whether armed forces are an appropriate tool to address them. As far as global CUI is concerned, threats or challenges generally fall within five categories: natural; technical; accidental; criminal; geopolitical.

First, physical damage to CUI, often occurring in depths greater than 1000m, is most often attributed to natural phenomena such as earthquakes.[13] In 2006, for instance, one severed

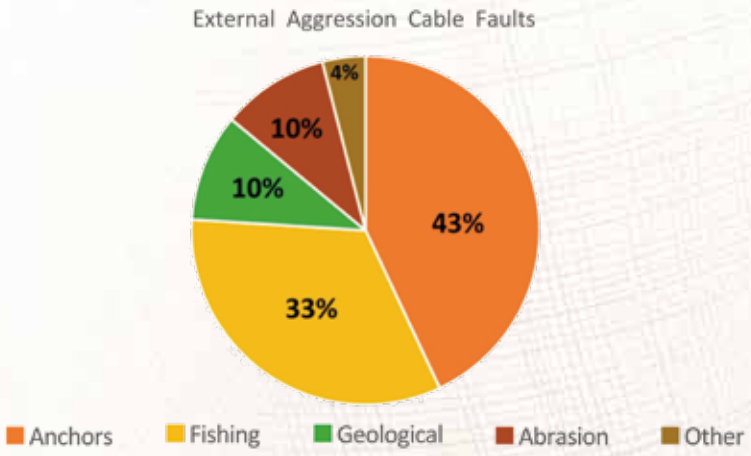

Figure 1. Underwater cable threats by category (2007 to 2018)

Source: Dimitrios Eleftherakis and Raul Vicen-Bueno, "Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors," *Sensors Review* 20 no. 737 (Basel: MDPI, 2020), 5, https://mdpi-res.com/d_attachment/sensors/sensors-20-00737/article_deploy/sensors-20-00737-v4.pdf?version=1581329530

11 NATO, Newsroom, "NATO launches "Baltic Sentry" to increase critical infrastructure security," *News*, 14 January 2025, https://www.nato.int/cps/en/natohq/news_232122.htm; Gozzi, "NATO launches new mission."

12 NATO, *Vilnius Summit Communique*, para. 65.

13 Charles Bukowski, "Do Nothing: An Alternative Opinion on Critical National Infrastructure and Seabed Warfare," *WavellRoom*, 15 February 2024, https://wavellroom.com/2024/02/15/alternative-opinion-on-critical-national-infrastructure-and-seabed-warfare/

nine cables off Taiwan disrupting regional trade and financial markets.[14] Second, technical disruptions occasionally stem from component failure. Of the remaining three threats involving human activities, accidental damage is the most common occurrence.[15] The International Cable Protection Committee (ICPC), for example, places disruption to undersea cables caused by commercial fishing vessels' anchoring, trawling and related activities such as mooring lines of fish aggregating devices (FADs) as accounting for 70 percent of damage worldwide.[16] **Figure 1.** As for the fourth, criminal actions have been most common in South-East Asia. Two highly publicized incidents occurred in 2007 and 2013 with the suspected culprits apprehended by law enforcement.[17]

Accidental damage is the most common occurrence.

Concerning the fifth source of CUI impairment, deliberate action with geopolitical motive refers to sabotage or espionage. Examples include the use of mines targeting CUI, the cutting of cables to disrupt an adversary's communications, or intercepting the data (including classified sources) transiting them. Western armed forces practiced CUI sabotage and espionage in World Wars I and II.[18] During the Cold War, the US Sound Surveillance System (now the Integrated Undersea Sound System) was designed to prevent Soviet submarines from doing the same.[19] With respect to the more recent CUI disruptions catalogued in the Introduction, state (Russian) sabotage or sponsorship of malicious anchoring or trawling by Russian, Chinese-flagged or other research and fishing vessels has been suspected. The latter falls into the category of "hybrid tactics"—actions aimed to harm but "below the threshold of detection, attribution and response."[20] In this context, potential cyber attacks on CUI, alongside physical attacks

Aside from the risk of a state, hybrid or terrorist debilitating attack on CUI, there exist potential vulnerabilities from the national affiliation of companies building, operating and maintaining it.

14 Martinage, "Under the Sea," 119.

15 Diren Dogan and Deniz Cetikli, *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment* (Istanbul: Maritime Security Centre of Excellence, 2023), 26.

16 International Cable Protection Committee, *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables*, Version 1.2, 24 November 2024, 1-2, https://www.iscpc.org/publications/icpc-best-practices/

17 "Vietnam's submarine cable "lost" and "found", *LIRNEasia*, 2 June 2007," https://lirneasia.net/2007/06/vietnams-submarine-cable-lost-and-found/; Bukowski, "Do Nothing."

18 Fridbertsson. *2023–General Report*, 1; Martinage, "Under the Sea," 123-124.

19 France, Ministry of Armed Forces, *Seabed Warfare Strategy. Report by the Working Group* (Paris: Ministry of Armed Forces, 2022), 18.

20 Sean Monaghan et al., "NATO's Role in Protecting Critical Undersea Infrastructure," *CSIS Briefs*, December 2023, 2, https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure

may be included. Hybrid tactics by state or non-state actors received special mention in the Vilnius Summit's passage on CUI followed by the statement: "Cyberspace is contested at all times as threat actors increasingly seek to destabilize the Alliance by employing malicious cyber activities …"[21] Lastly, while uncommon, terrorist groups also may be included in deliberate manmade attacks on CUI. The most recent example is a possible Houthi assault on fiber-optic cables transiting the Red Sea close to Yemen. The incident temporarily disrupted 25 percent of communications traffic between Europe and Asia.[22]

Aside from the risk of a state, hybrid or terrorist debilitating attack on CUI, a recent CSIS report also draws attention to potential vulnerabilities stemming from the national affiliation of companies building, operating and maintaining it.[23] The undersea cable market is singled out. National security concerns about ownership turn on government directed stoppage in times of conflict, not to mention opportunities for cyber espionage. While three of the four principal cable laying firms currently are from NATO or closely aligned countries (United States' SubCom, France's Alcatel, Japan's Nippon Electric Company), China's HMN Technologies (formerly Huawei Marine Networks) is an emergent player that aims to capture 60 percent of global market share. Whereas Russia favours a strategy of gathering intelligence from or cutting existing cable infrastructure to achieve its foreign policy aims, China privileges one of manufacture and maintenance control to engage in espionage or coerce other states.[24] Consequently, HMN has been blocked from US CUI projects. The same CSIS report goes on to advocate for similar vigilance as regards high risk cable maintainers and repairers.

While seabed cables carry their peculiar risks, pipelines do as well. Compromised energy security and societal disorder notwithstanding, environmental damage resulting from overt or hybrid kinetic attacks on subsea energy pipelines is a going concern. Oil spills readily come to mind, but natural gas leaks present their own hazards. The Nord Stream explosions, for example, accounted for the largest single source of global-warming methane gas in recent history.[25]

Of the preceding threats and challenges to CUI involving human activities, the majority have

21 NATO, *Vilnius Summit Communique*, para. 66.

22 "Cutting of 4 Submarine Fiber Optic Cables in the Red Sea", *ZMSCable News*, 7 March 2024, https://m.zmscable.com/new/Cutting-of-4-Submarine-Fiber-Optic-Cables-in-the-Red-Sea-Affects-25-of-Data-Traffic-between-Asia-and-Europe; Hanna Ziady, "Red Sea cables have been damaged, disrupting internet traffic," *CNN*, 4 March 2024, https://edition.cnn.com/2024/03/04/business/red-sea-cables-cut-internet/index.html

23 Daniel Runde, Erin Murphy and Thomas Bryja, *Safeguarding Subsea Cables. Protecting Cyber Infrastructure amid Great Power Competition* (Washington DC: Center for Strategic and International Studies, 2024), 2-5.

24 Dogan and Cetikli, *Maritime Critical Infrastructure Protection*, 28-29.

25 Kostas Poursanidis, Jumana Sharanik and Constantinos Hadjistassou, "World's largest natural gas leak from nord stream pipeline estimated at 478,000 tonnes," *iScience*, 1-5, https://www.cell.com/iscience/pdf/S2589-0042(23)02849-3.pdf

occurred on or in proximity to the continental shelf. Nevertheless, by virtue of new technologies, the equation may soon evolve to increasingly implicate CUI deep below the high seas as well. Alongside the exposure of cables and pipelines at even greater depths, potential mining of heretofore unreachable prized manganese, cobalt, copper, nickel and other rare earth elements lying in the international seabed (polymetallic nodules, polymetallic sulphides, ferromanganese crusts) may present an additional arena of competition or contestation on the ocean floor. For example, 80 percent of cobalt production, essential for clean energy applications, is currently controlled by China. Yet deep seabed sources may equal or surpass current terrestrial supply.[26] In 2023, US Congress members twice petitioned the President and Secretary of Defence to counter Chinese investment and control in deep-sea mining technology.[27] The aim? To "keep all options, including deep-sea opportunities, on the table in assessing polymetallic nodules as a viable resource to secure critical minerals and close national security vulnerabilities."[28] The alert is understandable. The International Seabed Authority (China and Russia are members, but not the US) is close to finalizing regulations for exploitation of mineral resources in the deep seabed beyond national jurisdiction in accordance with the United Nations Law of the Sea (UNCLOS).[29]

Faced with renewed great power competition, countering politically motivated threats to allied CUI—whether overt or hybrid, contemporary or on the horizon—would appear the logical preoccupation of a US-led defensive alliance like NATO. It is here that the current trajectory proclaimed at Vilnius aligns. Yet expenditure of costly military and political capital in this direction need also be tempered with a reminder that, as mentioned earlier, the most prevalent causes of CUI disruption are unintentional. In this regard, a supporting rather than lead role for the alliance must figure in its strategic calculus regarding CUI protection. Before exploring the shape of the Atlantic Alliance's principal and ancillary functions in CUI protection, the geographic and jurisdictional boundaries of alliance action warrant clarification. Since its foundation, where NATO may act, in large measures drives how it acts.

---

26 Caitlin Keating-Bitonti, *Seabed Mining in Areas Beyond National Jurisdiction: Issues for Congress*, R47324 (Washington DC: Congressional Research Service, 2022), 4, 13.

27 Robert J. Wittman et al. to Secretary Lloyd J Austin III, 7 December 2023, https://wittman.house.gov/uploadedfiles/20231207-wittmanstefanik-national_security_impacts_of_seabed_mining-signed.pdf

28 Robert J. Wittman et al. to President Joseph R. Biden and Secretary Lloyd J. Austin III, 25 July 2023, https://metals.co/wp-content/uploads/2023/07/Letter-to-POTUS-AND-SecDef-on-Seabed-Mining.pdf

29 Caitlin Keating-Bitonti, "US Interest in Seabed Mining in Areas Beyond National Jurisdiction: Brief Background and Recent Developments," *In Focus*, 26 November 2024, https://crsreports.congress.gov/product/pdf/IF/IF12608; International Seabed Authority, Council, *Statement of the President on the work of the Council of the International Seabed Authority during the first part of the twenty-ninth session*, ISBA 29/C/9, 22 April 2024, part VII, https://www.isa.org.jm/wp-content/uploads/2024/04/ISBA_29_C_9.pdf

NATO's Geography

Delineating the geographic scope of NATO member states' "collective commitment" to CUI protection necessarily begins with the alliance's founding Washington Treaty of 1949. Its reference to the "North Atlantic Area" circumscribes the alliance's principal function of collective self defence, including the use of armed forces to restore and maintain the security of the territory of North America and Europe north of the Tropic of Cancer.[30] In this context, the 2022 Strategic Concept reaffirms the member states' commitment "to defend every inch of Allied territory,"[31] which now stretches from Turkey to northern reaches of Finland and Sweden. In this regard, even before Operation Baltic Sentry was inaugurated, the NATO Parliamentary Assembly issued a resolution on "Enhancing the Protection of Allied Critical Maritime Infrastructure." It welcomed the decision to increase the number of ships patrolling the North, Baltic and Mediterranean Seas.[32] To these maritime regions of importance must be added the Black Sea and the North Atlantic. The subsea cables traversing the latter represent the highest concentration in the world.[33] They are the physical manifestation of the "transatlantic link" between Europe and North America. **Figure 2.** Most come ashore within tens of miles of each other close to New York and New Jersey.[34] Not surprisingly, on America's East Coast, the alliance's Joint Force Command-Norfolk describes its role as a multinational, operational level headquarters that "projects stability, deters aggression and stands ready to defend NATO territory from Florida to Finnmark, the Tropic of Cancer to the North pole and from Seabed to Space." [35]

Unlike the European Union (EU) that encompasses "Outermost Regions' in the Indian Ocean and "Overseas Countries and Territories' in the Pacific,[36] NATO territory does not extend

30 NATO, *The North Atlantic Treaty*, 4 April 1949, art. 6, https://www.nato.int/cps/ua/natohq/official_texts_17120.htm

31 NATO, 2022 *Strategic Concept*, para. 20.

32 NATO, Parliamentary Assembly, *Enhancing the Protection of Allied Critical Maritime Infrastructure*, Resolution 488, 9 October 2023, para. 5, https://www.nato-pa.int/document/resolution-488-enhancing-protection-allied-critical-maritime-infrastructure

33 Fridbertsson. *2023–General Report*, 2.

34 Martinage, "Under the Sea," 120.

35 NATO, Joint Force Command Norfolk, *Vision*, https://jfcnorfolk.nato.int/about-us

36 European Union, European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council on the update of the EU Maritime Security Strategy and its Action Plan "An enhanced EU Maritime Security Strategy for evolving maritime threats,"* JOIN(2023) 8 final, 10 March 2023, 2, https://oceans-and-fisheries.ec.europa.eu/publications/joint-communication-update-eu-maritime-security-strategy-and-its-action-plan-enhanced-eu-maritime_en

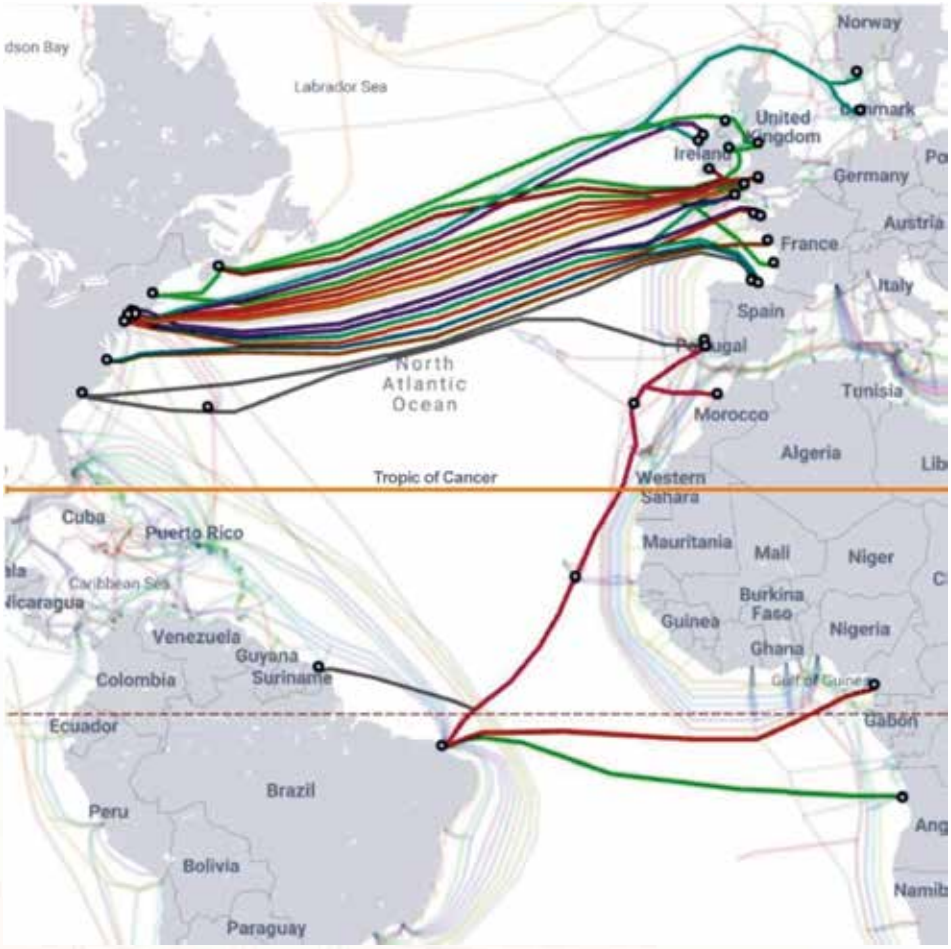

Figure 2. Transatlantic Undersea Communication Cables

Source: IEEE Spectrum, https://spectrum.ieee.org/undersea-internet-cables-nato

to the Indo-Pacific beyond the West Coast of North America. The US and Canada historically have addressed the latter's defence bilaterally. There is no reason to expect otherwise regarding CUI. Be that as it may, the global interconnectedness of CUI means that the Atlantic Alliance cannot afford to ignore threats to it wherever they arise. Hence, the frequent references to a "360 degree" approach to defence, a NATO commitment to protecting the "global commons" as well as enhancing alliance resilience through partnerships ("cooperative security") with states and organizations in "our broader neighborhood and across the globe." [37] Moreover, while the 2024 Washington Summit heralded the most consequential efforts in a generation to collectively defend allied territory, out-of-area "crisis prevention and management" remains within NATO's official repertoire to which CUI cannot be excluded as discussed further below.[38]

37 NATO, *Vilnius Summit Communique*, para. 1, 72.

38 NATO, *Washington Summit Declaration*, 10 July 2024, para. 1, 7, https://www.nato.int/cps/cn/natohq/official_texts_227678.htm

NATO's Jurisdiction

With respect to NATO's primary, although not exclusive, concern with CUI located in the North Atlantic Area, it is important to recall that alliance actions there remain at the consensual discretion of its 32 members. The 2023 Vilnius communique was careful to qualify that while NATO as an entity stands ready to support allies in CUI protection, it will do so only "if and when requested:" "the protection of critical undersea infrastructure on Allies' territory remains a national responsibility as well as a collective commitment."[39] Thus, before considering what alliance action might look like, the question arises: what does "Allies' territory" mean in context? And in an associated question: what international laws and norms govern activities by NATO and its member states related to the seabed lying beyond national jurisdiction beneath the high seas?

The protection of critical undersea infrastructure on Allies' territory remains a national responsibility as well as a collective commitment.

NATO member state France's 2023 Seabed Warfare Strategy is instructive in addressing such questions. It clarifies that under UNCLOS, the sovereign rights and prerogatives of coastal states governing seabed activities principally relate to the "territorial sea" (up to 12 nm) and the EEZ (up to 200 nm and sometimes extended depending on the morphology of the continental shelf).[40] **Figure 3.** Notwithstanding the right of innocent passage for foreign vessels, within 12nm the coastal state may adopt laws and regulations related to the laying of cables and pipelines, hydrography and marine scientific research. Within the EEZ, all states may lay and maintain submarine cables and pipelines subject to the coastal state's right to take "reasonable measures" for its exclusive exploration and exploitation of the continental shelf.[41] Beyond the EEZ, the seabed and subsoil of the high seas is known as "The Area."[42] UNCLOS refers to it as the "common heritage of mankind" (Article 140).[43] Since 1994, the International Seabed Authority (ISA) has issued exploration licenses for UNCLOS states parties.[44] As for laying seabed cables and pipelines in The Area, all states may do so. Additionally, if a vessel on the

39 NATO, *Vilnius Summit Communique*, para. 65.

40 France, Ministry of Armed Forces, *Seabed Warfare Strategy*, 14.

41 United States, US Department of Commerce, *Submarine Cables–International Framework* (Washington DC: National Oceanic and Atmospheric Administration, n.d.), https://www.noaa.gov/general-counsel/gc-international-section/submarine-cables-international-framework

42 International Cable Protection Committee, *Government Best Practices*, 11.

43 United Nations, *United Nations Convention on the Law of the Sea*, 1982 (entry into force 1994), art. 140, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

44 Keating-Bitonti, "US Interest in Seabed Mining."

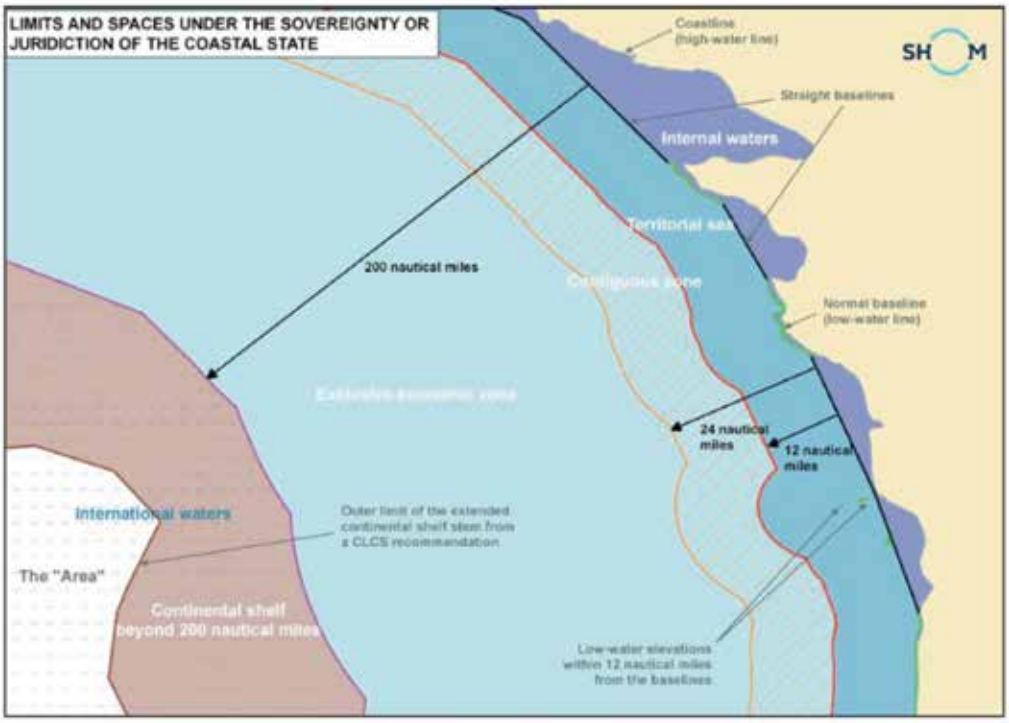

Figure 3. Segmentation of the Maritime Space

Source: France, Ministry of Armed Forces, *Seabed Warfare Strategy. Report by the Working Group* (Paris: Ministry of Armed Forces, 2022), 14.

high seas willfully or unintentionally damages them, the domestic law of the ship's flag state should apply (UNCLOS Articles 112 and 113).[45] Since 1958, the non-profit International Cable Protection Committee (ICPC) promotes best practices for respecting such provisions by private as well as public stakeholders.[46]

Why are these and other UNCLOS provisions significant to NATO? Six reasons stand out. First, because 30 of its 32 members are parties to the Convention, they may choose to request (illustrated by Baltic Sentry) relevant alliance assistance in exercising control of seabed activities within their maritime approaches and jurisdiction under the Law of the Sea.

Second, the European Union of which 23 NATO allies are members is also a contracting party to UNCLOS within areas of exclusive and mixed competence.[47] "Since both the EU and its member states participate in the Convention, it is of paramount importance that they act in a uniform manner maintaining the unity of the European Union."[48] This means that NATO's evolving approach to CUI protection necessarily must take into account the Union's as well

45 United Nations, *United Nations Convention on the Law of the Sea*, art. 112, 113.

46 https://www.iscpc.org/

47 Esa Paasivirta, "The European Union and the United Nations Convention on the Law of the Sea," *Fordham international Law Journal* 38, no. 4 (2015), 1046-7.

48 Paasivirta, "The European Union," 1050-51.

as national positions under UNCLOS. A case in point is the September 2024 "Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World" (the so-called "New York Principles") endorsed by the European Union, EU-NATO members Finland, France, the Netherlands and Portugal as well as NATO allies Canada, UK and USA (later Norway).[49]

30 of NATO's 32 member states are parties to UNCLOS apart from the United States and Türkiye.

Third, as members of ISA, the 30 UNCLOS allies can work to safeguard future access to potential sources of rare earth elements needed for economic and national security which lie in The Area's polymetallic nodules and sulphides.[50] This already has been advocated for by members of the US Congress and is discussed further below.[51]

That being said, and in a fourth consideration for NATO's 30 UNCLOS adherents, they are obliged to ensure that The Area is used for peaceful purposes (Article 141).[52] This necessarily should restrain their militarization of the international seabed whether nationally, through NATO, the EU or otherwise, and aid in their holding to account others for the same. In this regard, UNCLOS makes clear that the general conduct of states in relation to The Area shall be in "accordance the principles embodied in the Charter of the United Nations and other rules of international law in the interests of maintaining peace and security and promoting international cooperation and mutual understanding" (Article 138).[53]

Fifth, while possible pirate attacks against CUI are conceivably addressed under Article 101(a)(ii), UNCLOS is silent on hostile acts of terrorism against CUI occurring outside territorial waters. Regarding the latter, the 30 UNCLOS allies therefore may proactively work to fill the gap as called for by legal scholars, and operationalize the former (Article 101) should piracy become a significant concern.[54]

---

49 Winston Qiu, "US and its Allies Issue Joint Statement on the Security and Resilience of Undersea Cables," *Insights*, 7 October 2024, https://www.submarinenetworks.com/en/nv/insights/us-and-its-allies-issue-joint-statement-on-the-security-and-resilience-of-undersea-cables; European Union, European Commission, *The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World*, 26 September 2024, https://digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world;

50 The United States and Turkye are ISA Observers.

51 Keating-Bitonti, "US Interest in Seabed Mining;" Robert J. Wittman et al. to Secretary Lloyd J Austin III.

52 United Nations, *United Nations Convention on the Law of the Sea*, art. 141.

53 United Nations, *United Nations Convention on the Law of the Sea*, art. 138.

54 Douglas R. Burnett, "The 1884 International Convention for Protection of Submarine Cables Provisions Not in UNCLOS Deserve Attention Now," *Squire, Sanders Legal Counsel Worldwide*, April 2011, 11-12, https://cil.nus.edu.sg/wp-content/uploads/2011/04/Douglas-Burnett_1884_International_Convention_for_Protection_of_Submarine_Cables_Provisions_Not_in_UNCLOS_De1.pdf

Sixth, and finally, concerning the two NATO members that have not ratified UNCLOS—the United States and Türkiye—the Convention is now widely recognized as constituting customary international law. Thus, it should broadly align them with those provisions implicating NATO discussed herein.

In addition to UNCLOS, another international treaty with jurisdictional implications for NATO and CUI is the 1888 International Convention for Protection of Submarine Telegraph Cables ("Paris Convention"). Article 10 is of particular interest. Its provisions did not migrate to UNCLOS, but nevertheless apply to the 36 states parties, which include the United States, and several European NATO members as well as Russia. Under this Article, their "officers commanding ships of war" may board non-military vessels on the high seas suspected of damaging undersea cables "willfully or through culpable negligence" for the purpose of obtaining evidence for penalties to be administered in civil and criminal courts. A Cold War precedent stems from 1959. Then officers of the USS Roy O. Hale boarded a Soviet trawler under suspicion of cutting transatlantic communication cables.[55] As discussed further below, in an era of renewed great power competition, the judicious operationalization of this Convention alongside relevant UNCLOS provisions merit consideration when advancing NATO's Vilnius CUI pledge.

In addition to UNCLOS, another international treaty with jurisdictional implications for NATO and CUI is the 1888 International Convention for Protection of Submarine Telegraph Cables ("Paris Convention").

NATO's Core Tasks and Critical Undersea Infrastructure

The emphasis on judicious operationalization applies broadly to NATO's core tasks of deterrence and defence, cooperative security, and crisis prevention and management as they relate to CUI. All three need to be circumscribed by considerations of threat, geography and jurisdiction as outlined above. In this regard, some general observations set the stage for treating each core task in kind.

Where the primary causes of CUI disruption are concerned, their unintentional or natural character cautions against excessive involvement of an alliance established principally to counter military threats. In the much rarer cases where malicious human agency may be involved, addressing CUI threats in the geographically delimited North Atlantic Area needs to be NATO's primary concern driven by considerations of CUI density: the North Atlantic including the North Sea, the Baltic and Mediterranean Seas. Even here, however, a degree of moderation

55 United States, US Department of Commerce, *Submarine Cables*; Burnett, "The 1884 International Convention", 8-10.

is in order. As one senior MARCOM official remarked, "Maritime and air assets cannot guard every inch of maritime CUI space, nor should they, as the other deterrence and defense requirements are still with us." [56] Jurisdictionally, collective action by maritime forces under NATO command likewise faces inherent limitations. It is important to recall that a member state must first consent to NATO involvement in CUI protection within its territorial waters where freedom of navigation and overflight may be most restricted, and in its EEZ where privileged seabed resource rights are to be upheld. Therefore, the maritime approaches to allies' coasts are the segment of the ocean space where NATO may be expected to be most visible in CUI protection, but only when consensually agreed at 32. "Risks of interference with undersea infrastructure increase in shallower waters proximate to coastlines." [57] Beyond those waters, concern with CUI should, as previously observed, be more restrained in accordance with UNCLOS' peaceable aspirations and the 30 member states' Convention obligations regarding The Area. Nevertheless, malevolent actions against CUI there, at ever greater depths courtesy of emergent technologies, could elicit a NATO response. This would be particularly so if its member states' national interests or allied maritime forces freedom of maneuver in deployment areas were compromised as a result.

The maritime approaches to allies' coasts are the segment of the ocean space where NATO may be expected to be most visible in CUI protection.

Deterrence and Defence

Since 1949, NATO's collective defence clause—Article 5—has been the linchpin of the alliance. Responding to an overt "armed attack" by a state or non-state actor against CUI would follow the letter of the Washington Treaty. Doing so in the face of cyber and hybrid attacks would also apply since the momentous decisions of the North Atlantic Council (NATO's highest decision-making body) in 2014 and 2016 respectively. Given the rarity of terrorist CUI actions, state-motivated attacks of any of the three genres (armed, cyber, hybrid) would seem more likely with Russia atop the countries of concern. Since 2022 and Russia's military operation in Ukraine, the alliance's strategic paradigm has definitively shifted from non-state to state threats.[58] That being said, the invocation of Article 5 is a rarity (only once after 911). Why? Because the risk of escalation and full-scale war (possibly with nuclear powers) weighs heavily

56 James Henry Bergeron, "Maritime NATO After the Russian Invasion of Ukraine," *Atlantisch Perspectief* 47 no. 4 (2023), 38.

57 Eoin Micheal McNamara, "Reinforcing resilience: NATO's role in enhanced security for critical undersea infrastructure," *NATO Review*, 28 August 2024, https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html

58 Bergeron, "Maritime NATO," 36.

in the political calculus of member state capitals. Crossing that collective defence Rubicon is not taken lightly—which prompts the question: what would it take for Article 5 to be activated in the face of CUI disruption? The response to 911 is informative. As this author has observed elsewhere, establishing with sufficient confidence the "external direction" or foreign source of the attack (Afghanistan) as well as the magnitude of harm inflicted on allied territory (significant physical destruction and human casualties) were key determinants in 2001.[59] Using this episode as a guide, the invocation of Article 5 in the face of a CUI attack would turn on attribution and consequences.

Yet attribution in recent cases of CUI disruption such as Nordstream has proven extremely challenging.[60] As MARCOM's deputy commander, Vice Admiral Didier Maleterre, has observed particularly as regards the identity of a suspected actor behind hybrid operations: "If the Russians are using very high-handed capabilities—and I cannot go into details but we are talking about submarines and nuclear submarines—that's very, very tough; very difficult." [61] Even in cases where far less sophisticated fishing trawlers have been linked to CUI disruption (e.g. Balticonnector) proving malicious intent for geopolitical gain as opposed to common accidents is equally problematic. Without a clearly established foreign chain of command behind recent CUI ruptures in the North Atlantic Area, the result has been reluctance by the NAC to formally "name and shame" suspected perpetrators.[62] Nonetheless, should the "proof beyond reasonable doubt" threshold for apportioning responsibility be met, and once more using 911 as the bellwether, the question of an attack's scale also would likely figure in any Article 5 equation. While significant human casualties are unlikely, the gravity of societal disruption due to a CUI attack on the "lifeline sector" of communication or energy,[63] or the coordinated physical destruction of numerous CUI nodes, are prospective key variables. As others have noted, in this regard, "Russia is aware of the calculations and will likely keep the severity of attacks just below the point that seems like an all-out war." [64] The

The "proof beyond reasonable doubt" threshold for apportioning responsibility and an attack's scale would likely figure in any Article 5 equation.

59 Brooke A. Smith-Windsor, "From "Armed Attack" to "Cyber Attack": The Evolution of Collective Self-Defense in NATO," *Defense Strategy and Assessment Journal* 9 no. 1 (2019), 70, https://indsr.org.tw/en/respubcationmenus?uid=14&resid=1870

60 Kalm, "NATO's Path to Securing Undersea Infrastructure."

61 Bryant, "Undersea "hybrid warfare" threatens security of 1bn."

62 Anchal Vohra, "NATO to revise strategy on how to tackle hybrid threats," *DW*, 12 May 2024, https://www.dw.com/en/nato-to-revise-strategy-on-how-to-tackle-hybrid-warfare/a-70959822

63 Dogan and Cetikli, *Maritime Critical Infrastructure Protection*, 8.

64 Vohra, "NATO to revise strategy."

same could be said of any other future state challenger to NATO and its member states in the CUI domain.

Given the high bar for Article 5 activation, the implication is that member states, when requesting NATO help in CUI protection, are more likely to do so in the context of deterrence. Simply signaling, as NATO allies have already done, the possibility of invoking article 5 in the case of direct, hybrid, or cyber CUI attacks would fall in the realm of deterrence by punishment.[65] Deterrence by denial—"to deter an action by making it infeasible or unlikely to succeed, thus denying a potential aggressor confidence in attaining its objectives" [66] —emerges as a second body of activity in the seas within NATO's geographic scope. Both types are underpinned by the "Concept for Deterrence and Defence of the Euro-Atlantic Area" agreed by allies in 2020. One of its notable features is the Supreme Commander Allied Powers Europe's (SACEUR) "strategic Directive," which emphasizes peacetime deterrence and preparedness through more "vigilance activity" (e.g. joint exercises, increased intelligence, surveillance, and reconnaissance).[67]

In a maritime context, NATO's four Standing Maritime Groups or Standing Naval Forces (under MARCOM command and force generated on a rotational basis supported by air assets), conduct this mission on a routine or, if required, contingency basis as illustrated by Baltic Sentry, and in the Mediterranean by Sea Guardian. What is more, the task aligns with the Alliance Maritime Strategy's reinforcing one of "maritime security." It stresses conducting surveillance and patrolling, and sharing support with law enforcement in the course of scheduled or NAC-approved activities and deployments in the North Atlantic Area. These activities are to be conducted "in accordance with international law (including any applicable treaties and customary law)."[68] Therefore, notwithstanding UNCLOS, here it is worthwhile to recall the 1888 Paris Convention. SNF force rotations may leverage the particular boarding rights (Article 10) afforded warships of the member states which are party to it. Beyond operations at sea, it is important to remark that in 2024 NATO also launched a USD 2.5 million project (under the Hybrid Space/Submarine Architecture Ensuring Infosec of Telecommunication [HEIST] consortium) to redirect communications to space should subsea cables be cut intentionally or inadvertently.[69] The initiative aligns with NATO member states' overarching commitment to

65 Michael J. Mazarr, "Understanding Deterrence," *Perspectives*, 19 April 2018, 2-3, https://www.rand.org/pubs/perspectives/PE295.html; Vohra, "NATO to revise strategy."

66 Mazarr, "Understanding Deterrence," 2.

67 Monaghan et al., "NATO's Role," 3, 8.

68 NATO, *Alliance Maritime Strategy*, para. 4.

69 Peter Felstead, "NATO project aims to reroute internet into space in case undersea cables are compromised," *European Security and Defence*, 7 August 2024, https://euro-sd.com/2024/08/major-news/39771/nato-plans-to-save-internet/; NATO, Newsroom, "NATO-funded project to reroute internet to space in case of disruption to critical infrastructure," *News*, 31 July 2024, https://www.nato.int/cps/en/natohq/news_228257.htm

the resilience of critical infrastructure in accordance with Article 3 of NATO's founding treaty, and is identified as a cornerstone of credible deterrence.[70]

Whether in a CUI deterrence or defence function, however, investing in and deploying expensive military assets must be commensurate with the level of malicious threat (still extremely low compared to accidental fishing and anchoring disruptions), political and operational expectations (the NATO Secretary General also has acknowledged achieving 100 percent coverage of subsea cables is unrealistic),[71] and the availability of other options providing for the protection and integrity of CUI. The latter include natural barriers to deliberate interference such as the oceans' depths (the Atlantic's average is over 3 km), and harsh operating environments, particularly in the more northern extremes of NATO's treaty area. To these may be added barriers to entry, especially for non-state actors, to the emergent technologies and sophisticated operational requirements for seabed operations at depth.[72] Moreover, cable armouring and cable burial already is common industry practice,[73] and cable operators themselves, who own over 90 percent of the subsea architecture, routinely build in redundancy to current networks to minimize the impact of the 2 to 4 breaks that on average occur globally every week without significant consequences.[74] As for-profit enterprises, it is in their interest to do so, just as is the timely repair of any damage (also a chiefly industry affair), which often trumps attribution investigations for in their case possible financial compensation under UNCLOS.[75] In this context, just as it made little strategic sense to keep NATO warships on station indefinitely to deter and defend against piracy in the Red Sea and Indian Ocean in the previous decade, rather than empower industry to take the lead (in this case eventually with armed guards afloat alongside reinforced best practices),[76] the same logic should apply to CUI protection. In the democratic states that comprise the Atlantic Alliance, the military is always the force of last resort. Safeguarding CUI is no exception, which is why post-Vilnius, NATO's additional core

The NATO Secretary General has acknowledged achieving 100 percent coverage of subsea cables is unrealistic.

70 NATO, Public Diplomacy Division, "Resilience, civil preparedness and Article 3," *NATO from A to Z*, 13 November 2024, https://www.nato.int/cps/uk/natohq/topics_132722.htm?selectedLocale=en

71 "NATO creates new centre, focuses on underwater assets," *ANI*, 17 June 2023, https://www.aninews.in/news/world/europe/nato-creates-new-centre-focuses-on-underwater-assets20230617223607/

72 Bukowski, "Do Nothing."

73 International Cable Protection Committee, *Government Best Practices*, 2.

74 Lane Burdette, "What to know about submarine cable breaks," *Telegeography*, 21 November 2024, https://blog.telegeography.com/what-to-know-about-submarine-cable-breaks

75 Bukowski, "Do Nothing."

76 International Maritime Organization, "Private Armed Security," *Maritime Security and Piracy*, n.d., https://www.imo.org/en/OurWork/Security/Pages/Private-Armed-Security.aspx

task of cooperative security with other stakeholders is ascendent.

Cooperative Security

The 2022 Strategic Concept emphasizes partnerships through dialogue and practical cooperation as contributors to security within the North Atlantic Area and abroad. "Partnerships are crucial to protect the global commons, enhance our resilience and uphold the rules-based international order." [77] The Alliance Maritime Strategy similarly refers to a maritime "comprehensive approach" to leveraging the competencies, capabilities and cultures of other maritime actors.[78] In a CUI context, this is likely to manifest in Allied governments' adroit management of two cooperative security trajectories. On the one hand, prioritized partnerships with like-minded actors (state and non-state, public and private) to shore up deterrence and defence, and seabed warfare capabilities especially within the North Atlantic Area. On the other hand, remaining open to confidence-building and aspirational initiatives for global or "universal" cooperation in managing the world's seabed. The latter includes fora outside NATO and the "West" where the alliance's current principal declared challengers, Russia and China, are participants. The full range of current and potential cooperative security CUI initiatives is beyond the scope of this paper. A survey of some key ones, however, sheds light on the possibilities for the 32 member state governments, whether working through NATO, or acting on a national basis in allied interests elsewhere. Those intended to engage likeminded actors to secure the seabed of the North Atlantic Area are considered first.

"*Like-minded*" approaches

In its paper on "Government Best Practices," the ICPC recommends the establishment of a single point of contact for cross-sectoral consultation on issues arising from submarine cable installation, repair, and protection, including national security considerations. This encompasses "to understand industry technology and operating parameters and share data regarding risks.[79] As mentioned previously, at Vilnius NATO allies elevated this advice to the international level and expanded it by establishing the Network at NATO Headquarters to address all CUI: a "convening authority" to build

Prioritized partnerships with like-minded actors (state and non-state, public and private) to shore up deterrence and defence, and seabed warfare capabilities especially within the North Atlantic Area.

77 NATO, 2022 *Strategic Concept*, para. 42.

78 NATO, *Alliance Maritime Strategy*, para. 6.

79 International Cable Protection Committee, *Government Best Practices*, 1, 6, 11.

"communities of trust."[80] Early work has focused on information-sharing and situational awareness. One aim is to leverage NATO's traditional military intelligence, signals and sensor data with information from friendly civilian partners to identify CUI anomalies and possible interference. MARCOM's Center for CUI is similarly engaged at the operational level to "deny deniability" to any potential aggressor.[81]

The ICPC Best Practices abound in additional areas for Network consultation and coordination to safeguard CUI. Notable among them are augmenting military deterrence with "legal deterrence." This by encouraging member state governments to update and enforce legislation for fishing and anchoring offenses related to cable damage in accordance with the Paris Convention and UNCLOS (Article 113).[82] An additional initiative would be advocacy for increased geographic diversity of undersea cable routes and landings in Europe and North America to reduce the risk of damage from a single natural or manmade incident. According to ICPC, this would be preferable to high density "cable protection zones" patrolled by military or coast guard assets.[83] Other best practices include requiring even the smallest of fishing vessels to employ automated identification systems to monitor activity in proximity to member state-dependent CUI. Another is to establish a FAD registry to ensure their safe distance from planned or installed CUI. NATO member states could also heed ICPC's call to adopt and enforce the recommended spatial separation distances between cable laying, maintenance and repair ships and other vessels in their territorial waters or EEZs.[84]

Turning to The Area, as introduced previously, courtesy of new technologies the ISA is on the cusp of issuing licenses for the exploitation of polymetallic nodules and sulphides. The Network warrants consideration for NATO member states' discussion of a coordinated response to the long-term implications for their national security. While initial mining activity is expected in the Pacific and Indian Ocean,[85] already exploration licenses have been issued to NATO-ISA member states France and Poland, as well as Russia, in the Mid-Atlantic Ridge. **Figure 4.** Ensuring that Russia does not dominate control of the deep-sea resources there could be achieved through coordinated allied approaches in ISA by the 30 UNCLOS-NATO allies (e.g. via the ISA Assembly, and their elected representatives on the Council and the Legal and

80 Lee Willett, "NATO steps up response to "clear and present" undersea infrastructure risk," *NavalNews*, 16 May 2023, https://www.navalnews.com/naval-news/2023/05/nato-steps-up-response-to-clear-and-present-undersea-infrastructure-risk/

81 NATO, Allied Maritime Command, Media Centre, "NATO officially launches new Maritime Centre."

82 International Cable Protection Committee, *Government Best Practices*, 5.

83 Ibid, 3,7, 8, 10.

84 Ibid, 2, 3, 4.

85 Ibid, 11.

Technical Commission).[86] Additionally, just as the US House Armed Services Committee has urged the US Department of Defence to study the refinement of polymetallic nodules for defence applications and to be vigilant of competitors doing the same,[87] so too could NATO allies within the Network. The Network similarly could facilitate discussion of a coordinated allied approach to the interpretation and implementation of the "due regard" and "reasonable regard" obligations under UNCLOS. Here the objective would be to ensure any prospective deep sea mining and biodiversity initiatives do not unduly interfere with the laying and operation of submarine cables vital for transatlantic communication or essential military activities.[88] Canada, France (Ifremer), Germany and Portugal have been active participants in the related consultations on the ISA

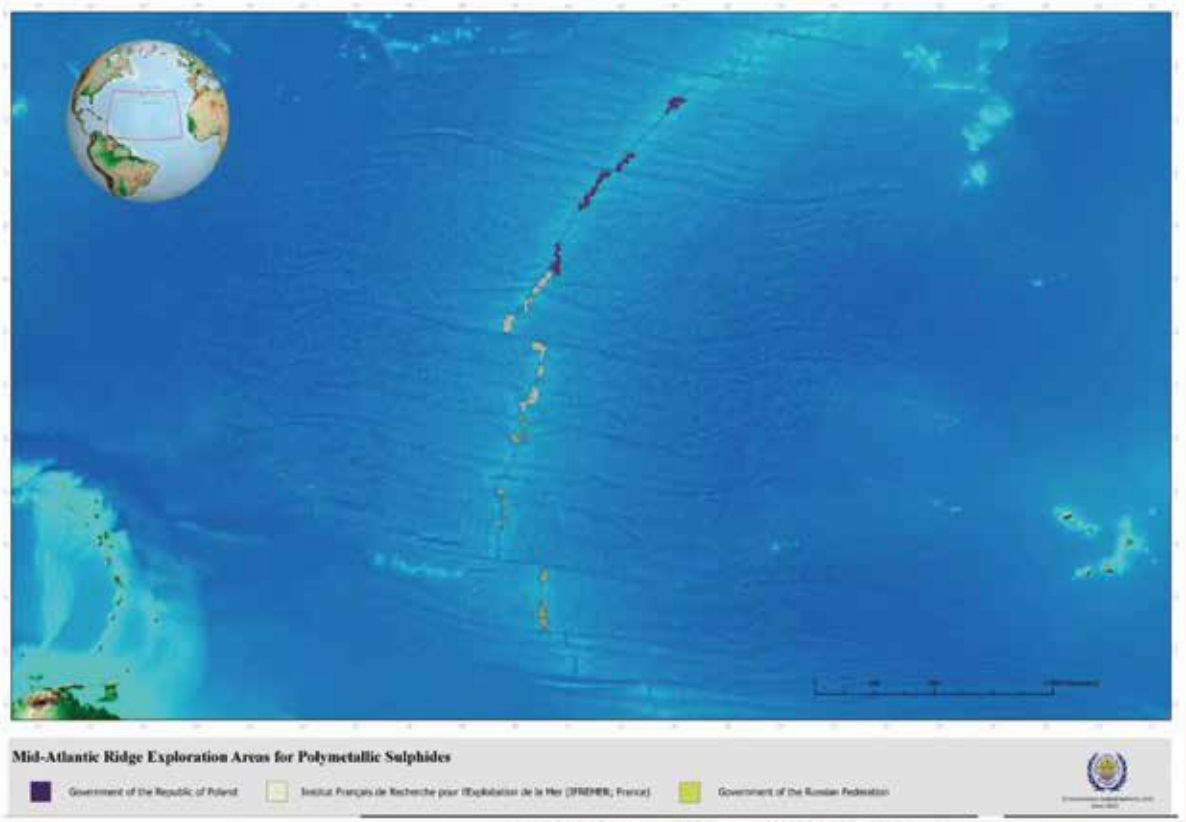

Figure 4. Mid-Atlantic Ridge Seabed Exploration Areas

Source: International Seabed Authority, "Mid-Atlantic Ridge. Exploration Area," https://www.isa.org.jm/maps/mid-atlantic-ridge/

86 International Seabed Authority, "Organs of the International Seabed Authority," *About the Authority*, n.d., https://www.isa.org.jm/organs/

87 Keating-Bitonti, "US Interest in Seabed Mining."

88 International Cable Protection Committee, Government Best Practices, 11; International Seabed Authority, *Deep Seabed Mining and Submarine Cables: Developing Practical Options for the Implementation of the "Due Regard" and "Reasonable Regard" Obligations under UNCLOS. Report on the Second Workshop* (Bangkok: ISA Technical Study No. 24, 2018), 79.

Strategic Plan 2024-2028.[89] Any one of them could take up the mantle within the Network, or in more restricted NATO fora if required. Similarly, in terms of a coordinated approach to operationalizing germane UNCLOS provisions, allies could leverage the Network to discuss ways to fill the void with regard to acts of terrorism and piracy vis-à-vis CUI, as mentioned previously.

Beyond the Network and MARCOM's Center for CUI, other opportunities exist for NATO engagement with likeminded governments, industry and academic partners. The "Digital Oceans Initiative" presented at the 2021 NATO Conference of National Armaments Directors is illustrative. It aims to leverage new and emerging technologies, such as AI and autonomy, "to improve Allies' capacity to 'see our oceans' through the creation of a global scale network of sensors, from seabed to space, to better predict, identify, classify and combat threats." [90] In April 2024, NATO Headquarters convened the Digital Ocean Industry Symposium attracting over 200 delegates.[91] Within six months, a tangible outgrowth was "REMPUS24" (Robotic Experimentation and Prototyping with Maritime Unmanned Systems) to test autonomous systems in antisubmarine warfare, naval mine warfare and the protection of CUI.[92] Going forward, NATO-industry collaboration could consider securing capabilities for rapid CUI repair in the event of a member state emergency or war. The Cable Security Fleet initiative launched by the United States in 2021 with Pentagon involvement is one national-level exemplar.[93]

The "Digital Oceans Initiative" was presented at the 2021 NATO Conference of National Armaments Directors.

As far as international organizations are concerned, the European Union is necessarily

89 International Seabed Authority, *Strategic Plan of the International Seabed Authority for the period 2024-2028 Draft 1*, 2023, https://www.isa.org.jm/strategic-plan-2024-2028/; International Seabed Authority, *Strategic Plan of the International Seabed Authority for the period 2024-2028 Draft 1 - Submissions*, 2023, https://www.isa.org.jm/strategic-plan-2024-2028/

90 NATO, Newsroom, "NATO Defence Ministers launch initiative to enhance maritime surveillance capabilities," *News*, 12 October 2023, https://www.nato.int/cps/ra/natohq/news_219441.htm; NATO, Newsroom, "Maritime Unmanned Systems Innovation Advisory Board discuss NATO innovation in the maritime domain," *News*, 9 November 2021, https://www.nato.int/cps/ru/natohq/news_188548.htm?selectedLocale=en

91 NATO, Newsroom, "NATO and industry work together to strengthen maritime surveillance," *News*, 16-17 April 2024, https://www.nato.int/cps/en/natohq/news_224798.htm?selectedLocale=en#:~:text=NATO%20and%20industry%20work%20together%20to%20strengthen%20maritime%20surveillance&text=On%2016%20-%2017%20April%202024,challenges%20in%20the%20maritime%20domain.

92 NATO, Newsroom, "REMPUS 2024: NATO's Digital Ocean Initiative gets a boost in Portugal," *News*, 24 September 2024, https://www.nato.int/cps/en/natohq/news_228959.htm?selectedLocale=en#:~:text=NATO%20Allies%20gathered%20for%20the,threats%20in%20the%20maritime%20environment.

93 Runde, Murphy and Bryja, *Safeguarding Subsea Cables*, 7.

atop NATO's CUI partnership list given the considerable overlap in their members' maritime neighborhoods. The Irish Sea is indicative. While neutral Ireland is not a NATO member, vital transatlantic undersea communications cables transverse its EEZ. Already in 2023 suspicious activities in those waters by Russian cable cutting-capable commercial and repair vessels were reported.[94] The undersea risks have not been lost on concerned analysts from neighbouring non-EU member, United Kingdom, who have described the Irish Sea as one of the country's weakest points in maritime defence.[95] With this backdrop, it is understandable that the March 2023 declared "update" to the EU Maritime Security Strategy and its Action Plan to address evolving maritime security threats such as CUI emphasized the need for intensified staff-to-staff cooperation with NATO. In accordance with the two organizations' 2023 Joint Declaration, the "EU-NATO structured dialogue on resilience" and the "task force on resilience of critical infrastructure" were singled out.[96] Furthermore, the update outlines a number of EU initiatives to address CUI where it is easy to envision complementarity with NATO efforts. For example, EU regional cooperation plans to ensure surveillance of underwater and offshore infrastructure, screening of foreign direct investments in maritime critical infrastructure, R&D investment in military capabilities for enhanced domain awareness and underwater control including interoperable unmanned systems, as well leveraging Helsinki's European Centre of Excellence for Countering Hybrid Threats.[97] The latter two initiatives, for instance, respectively dovetail with the work of NATO's Maritime Unmanned Systems High Visibility Project [98] and the NATO Maritime Center of Excellence work on maritime critical infrastructure protection.[99] To buttress collaboration with EU-wide efforts, NATO in turn may work bilaterally with EU member states not represented

The European Union is necessarily atop NATO's CUI partnership list given the considerable overlap in their members' maritime neighborhoods.

94 McNamara, "Reinforcing resilience;" Mehboob, "NATO's best-laid subsea security plans."

95 Mark Solarz Hendriks and Harry Halem, *From space to seabed. Protecting the UK's undersea cables from hostile actors* (London: Policy Exchange, 2024), 10.

96 European Union, European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication*, 7,8, 11, Annex 8; European Union and NATO, *Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization*, 10 January 2023, www.nato.int/nato_static_fl2014/assets/pdf/2023/1/pdf/230110-eu-nato-joint-declaration.pdf, para. 12.

97 European Union, European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication*, 12-14.

98 NATO, Public Diplomacy Division, "Maritime Unmanned Systems," *FactSheet*, February 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/2/pdf/2102-factsheet-mus.pdf

99 Dogan and Cetikli, *Maritime Critical Infrastructure Protection*.

in the Atlantic Alliance. In February 2024, for example, Ireland and NATO agreed to bolster CUI protection under the country's Individual Tailored Partnership Program.[100]

Considering the updates to its maritime strategy, and reinforcing initiatives such as the "Recommendation on the Security and Resilience of Submarine Cable Infrastructure," [101] the EU undoubtedly will remain NATO's focal point for partnership with likeminded international actors with overlapping memberships. Awareness and coordination of approaches with others, however, will also be essential. The Group of 7 (G7), comprised of 6 NATO allies and Japan (a longstanding official NATO partner), is one of them. In March 2024, G7 Industry, Tech & Digital Ministers issued a joint statement prioritizing the security and resilience of cable communications among member countries in terms of routing, maintenance, repair, and vendors.[102] Marrying up this initiative with NATO's prioritized CUI role launched at its headquarters in the same year will necessarily default to the rotating G7 presidency, in 2025 held by Canada.

"*Universal*" *approaches*

While often a necessity, exclusivity in international affairs risks resentment. China and Russia have been relatively muted on NATO initiatives like the Network and MARCOM's Center for CUI (although Baltic Sentry did elicit Moscow's attention).[103] This perhaps is explained by the December 2024 UN General Assembly Resolution on the "Oceans and law of the sea" endorsed by them and another 150 states. The resolution acknowledged a role for "relevant regional organizations' concerning "dialogue and cooperation" on the protection of undersea cables and pipelines.[104] That said, the previously cited New York Principles endorsed by an informal grouping of 8 NATO member states, its four official Asia-Pacific Partners (Australia, Japan, New Zealand, South Korea), and the EU, among others, did not escape Beijing's gaze. Viewing the Principles as targeting the Chinese cable industry for de facto exclusion, the Foreign

100 Ireland, Department of Defence, "Ireland in new agreement with Nato to counter potential threats to undersea infrastructure," 9 February 2024, https://www.thejournal.ie/ireland-nato-agreement-cyber-threats-undersea-infrastructure-6295188-Feb2024/

101 Winston Qiu, "EU Issues Recommendation on the Security and Resilience of Submarine Cable infrastructures," *Insights*, 23 February 2024, https://www.submarinenetworks.com/en/nv/insights/eu-issues-recommendation-on-the-security-and-resilience-of-submarine-cable-infrastructures

102 Winston Qiu, "G7 Issues Joint Statement on Cable Connectivity for Secure and Resilient Digital Communications Networks," *Insights*, 27 April 2024, https://www.submarinenetworks.com/en/nv/insights/g7-issues-joint-statement-on-cable-connectivity-for-secure-and-resilient-digital-communications-networks

103 Maya Mehrara, "Russia Issues Warning Over NATO Flotilla "Abuses" in Baltic Sea," *Newsweek*, 24 January 2025, https://www.newsweek.com/russia-issues-warning-over-nato-flotilla-abuses-baltic-sea-2020188

104 United Nations, General Assembly, *Resolution adopted by the General Assembly on 12 December 2024. Oceans and the law of the sea*, A/RES/79/144, 16 December 2024, para. 171.

Ministry accused the US of masterminding a statement to promote unilateralism and global hegemony in the cable laying, maintenance and repair sector.[105] To avoid undue escalation with NATO's strategic competitors, therefore, allied governments can be expected also to pursue a second trajectory of global or "universal" cooperative and confidence-building approaches to seabed security, including through the UN and other frameworks where China and Russa are represented. Once more, this will be done in tandem with delimited approaches, including the insurance policy against undersea aggression in the North Atlantic Area that NATO provides its member states for as long as it is required in accordance with Article 51 of the UN Charter.

The global or universal approach was recently on display at the UN agency, the International Telecommunications Union (ITU). Two months after the New York Principles were published, the ITU established the "International Advisory Body for Submarine Cable Resilience" in partnership with the ICPC. The body is currently co-led by NATO member state Portugal's National Communications Authority chairman, represents the ITU's global regions (regions 1 and 2 encompass the North Atlantic Area), and brings together cross-disciplinary experts from public and private sectors. The avowed aims are to enhance cable maintenance, prevent natural and unintentional damage, accelerate repairs, increase redundancy and promote sustainability [106] The International Maritime Organization (IMO), where all NATO member states, Russia and China are represented, similarly has been earmarked to improve the protection of seabed cables, pipelines and offshore installations. This includes investigation of acts of violence against them.[107] What is more, a number of NATO member state governments acting through the Intergovernmental Oceanographic Commission and International Hydrographic Organization are supporting the Nippon Foundation-GEBCO (General Bathymetric Chart of the Oceans) project to provide a publicly accessible detailed map of the world's seabed by 2030. Launched at the 2018 UN

The International Maritime Organization (IMO), where all NATO member states, Russia and China are represented, has been earmarked to improve the protection of seabed cables, pipelines and offshore installations.

105 Qiu, "US and its Allies Issue Joint Statement."

106 Jonathan Greig, "UN, international orgs create advisory body for submarine cables after incidents." *The Record*, 30 November 2024, https://therecord.media/un-international-orgs-create-advisory-body-submarine-cables;
"ITU Launches International Advisory Body for Submarine Cable Resilience," *Insights*, 30 November 2024, https://www.submarinenetworks.com/en/nv/insights/itu-launches-international-advisory-body-for-submarine-cable-resilience

107 United Nations, General Assembly, *Resolution adopted by the General Assembly on 12 December 2024*, para. 139.

Ocean Conference hosted by NATO member state United States, the initiative, when complete, will have a number of applications including identification of geohazards and cable routing.[108] The next UN Ocean Conference in 2025 will be hosted by another NATO member state, France. Here the focus will be on the new international treaty governing "Biodiversity Beyond National Jurisdiction" (BBNJ),[109] which carries implications for CUI, including the seabed mining of rare earth elements with defence applications discussed previously. The BBNJ Agreement, already ratified by NATO allies France and Spain,[110] will become the third implementing agreement to UNCLOS.

Crisis Prevention and Management

The third core task in NATO's repertoire is crisis prevention and management. Historically, it has taken the form of stabilization and counter-terrorism operations abroad often at strategic distance.[111] Where maritime forces have been involved, it has normally been in support of operations on land.[112] Given this history, and the nature of CUI, it is perhaps understandable that this core task receives less attention in contemporary NATO policy discourse on seabed security. It is still relevant,[113] however, and there is always a degree of overlap among NATO's core functions. In this regard, we may refer to the Alliance Maritime Strategy's crisis management section's emphasis on surveillance, mine clearance, and consequence management in austere operating conditions as applying to CUI at ever greater depths in current times.[114] Moreover, given the high bar and escalatory risks involved in triggering Article 5 in a critical CUI incident discussed previously, a declared maritime crisis and consequence management operation might be the preferable option in the face of severe

Crisis Management could apply to an attack perpetrated out-of-area with extreme detrimental effects on Atlantic Alliance communications and energy security, or that of its strategic partners in, for example, the Asia-Pacific theatre.

108 Nippon Foundation, *The Nippon Foundation GEBCO Seabed 2030*.

109 United Nations, *Agreement under the United Nations Convention on the Law of the Sea on the Conservation and Sustainable Use of Marine Biological Diversity of Areas beyond National Jurisdiction (BBNJ Agreement)*, 19 June 2023, https://www.un.org/bbnjagreement/en

110 United Nations, *Agreement under the United Nations Convention on the Law of the Sea on the Conservation and Sustainable Use of Marine Biological Diversity of Areas beyond National Jurisdiction - Status*, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXI-10&chapter=21&clang=_en

111 NATO, 2022 *Strategic Concept*, para. 36.

112 NATO, *Alliance Maritime Strategy*, para. 11.

113 Bukowski, "Do Nothing."

114 Ibid, 11.

disruption within the North Atlantic Area. It could also apply to one perpetrated out-of-area with extreme detrimental effects on Atlantic Alliance communications and energy security, or that of its strategic partners in, for example, the Asia-Pacific theatre. **Figure 5.**

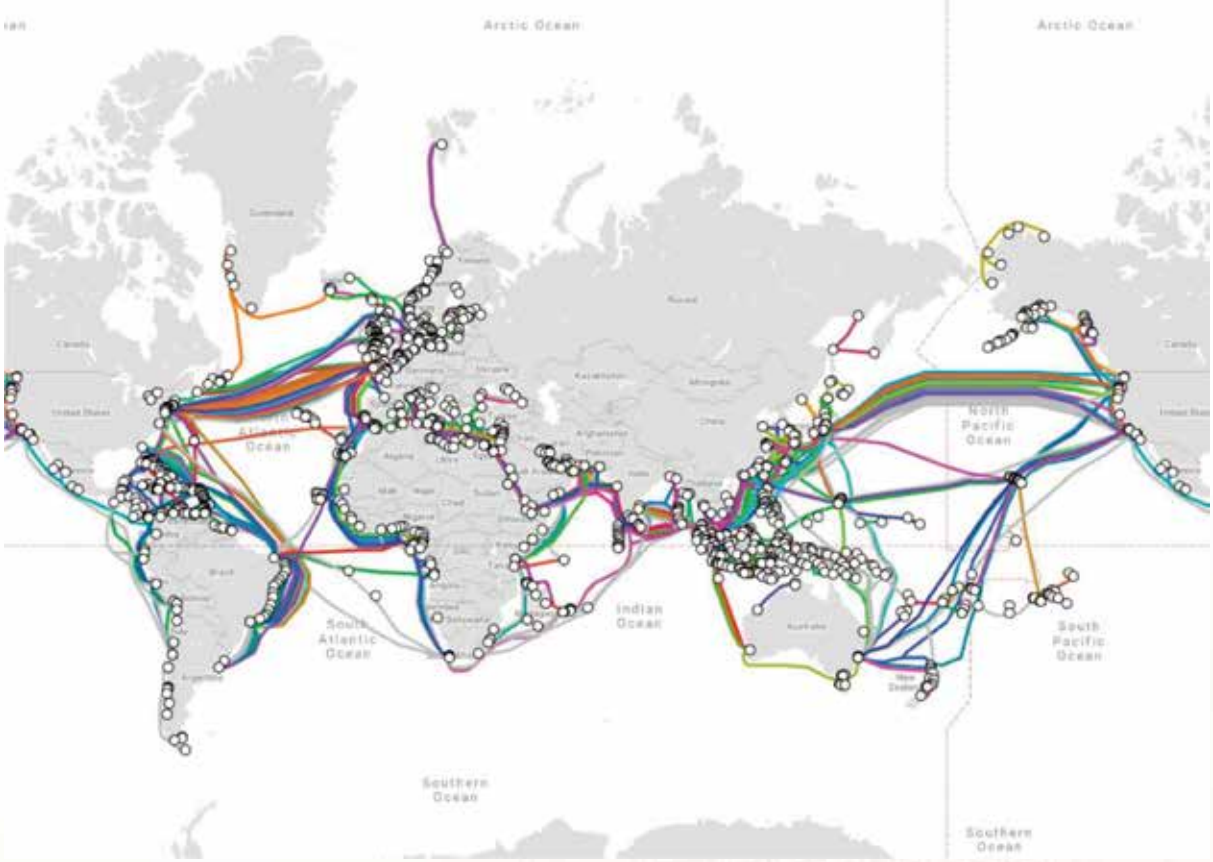

Figure 5. Distribution of Undersea Communication Cables Worldwide

Source: Dimitrios Eleftherakis and Raul Vicen-Bueno, 'Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors," *Sensors Review* 20 no. 737 (Basel: MDPI, 2020), 2, https://mdpi-res.com/d_attachment/sensors/sensors-20-00737/article_deploy/sensors-20-00737-v4.pdf?version=1581329530

Conclusion

Strategy at its core has been described as "an ability to assess vulnerabilities in situations, an appreciation of causes and effects, a capacity to link disparate activities in pursuit of shared purpose." [115] NATO's strategy for CUI protection, to be viable, must follow this prescription. This paper has sought to help explain and shape its application. The preeminently accidental and natural risks to CUI caution against a leading role for the Atlantic Alliance in addressing most disruptive contingencies. Rather, prevailing circumstances countenance the logical ascendance

115 John Lewis Gaddis, "Grammar, Logic, and Grand Strategy," in *The New Makers of Modern Strategy*, ed. Hal Brands (Princeton: Princeton University Press, 2023), 1120.

of NATO's cooperative security core task in this emergent maritime domain. As evidenced by the Network, this means working with likeminded public and especially private sector partners in often a supporting role to mitigate and address CUI and seabed resource vulnerabilities. At the same time, where possible, allies operating in a national capacity can and should be expected to work with shared purpose for universal or global cooperative approaches to secure the peaceable use of the world's seabed, from territorial to high seas, in the spirit of UNCLOS. Such aspiration, however, must not breed naivety. As long as there remains the chance of the albeit less common occurrence of CUI disruption by malign (most likely state) actors for geopolitical gain, NATO's deterrence and defence function necessarily applies. Given the risk of escalation and significant threshold for Article 5's invocation, including credible attribution, the military deterrence, maritime security, and if necessary timely crisis management, functions of allied maritime forces will remain a driver for judicious operationalization and investment. A collective commitment to surveilling and patrolling near CUI in NATO's maritime approaches, and deployment areas whether routine or contingency, will be required for the foreseeable future. To sum up in the words MARCOM's Political Advisor, "rapid response, new surveillance technology to map the threat, and sharing best practices in close networks with nations and industry can allow NATO to enhance its support to Allies in securing CUI." [116]

116 Bergeron, "Maritime NATO," 38.