CSIS BRIEFS

NATO's Role in Protecting Critical Undersea Infrastructure

By Sean Monaghan, Otto Svendsen, Michael Darrah, and Ed Arnold

DECEMBER 2023

THE ISSUE

NATO is not ready to mitigate increasingly prevalent Russian aggression against European critical undersea infrastructure (CUI). Despite its depleted ground forces and strained military industrial base, Russian hybrid tactics remains the most pressing threat to CUI in northern Europe. Despite its current limitations, NATO is the primary actor capable of deterring and preventing hybrid attacks on its allies and has expedited its approach to CUI protection by establishing new organizations to that aim. At the 2023 NATO Vilnius summit, allies agreed to establish the Maritime Centre for the Security of Critical Underwater Infrastructure within NATO's Allied Maritime Command (MARCOM), which focuses on preparing for, deterring, and defending against the coercive use of energy and other hybrid tactics. To help NATO planners and staff at the new center conceptualize and prioritize their efforts, this issue brief provides immediate and long-term recommendations to set the new center up for success.

INTRODUCTION

NATO is not prepared to defend its allies' critical undersea infrastructure (CUI) from increasingly prevalent Russian hybrid tactics. The recent Balticconnector pipeline incident highlighted the risk of deliberate damage to CUI across Europe. It follows last year's Nord Stream pipeline explosions, among other incidents, and bears the hallmarks of sabotage. Europe's expansive and growing network of undersea infrastructure will remain vulnerable to attacks aimed at disrupting transatlantic cohesion and economic activity, undermining Western support for Ukraine, and shaping potential future military operations.

Threats to undersea infrastructure are not new. In 2016 U.S. vice admiral James Foggo and Alarik Fritz warned of a "fourth battle of the Atlantic," which included threats to "underwater infrastructure–such as oil rigs and telecommunications cables."[1] In 2017 the UK chief of the defence staff went public with previously classified Russian threats to undersea cables that posed a "new risk to our way of life," while member of the UK Parliament Rishi Sunak (now UK prime minister) demanded enhanced protection of undersea data cables.[2] Yet the Nord Stream incident has catalyzed a new focus in Europe on CUI resilience, including national, multinational, and institutional efforts through NATO and the European Union. Notably, this included the launch of a new NATO Maritime Centre for the Security of Critical Undersea Infrastructure at the Vilnius summit in July 2023.[3]

This issue brief examines NATO's role in protecting CUI in more detail. It proceeds in four parts: It begins by assessing the threat "seascape" for CUI in northern Europe, including how the threat might evolve and how

Europe has responded so far. The paper then turns to NATO's approach to date, summarizing the key NATO initiatives related to CUI protection. The third part looks in more detail at the challenge of protecting CUI, proposing a basic framework to help understand the vast problem space. The final section draws on this framework to develop several immediate and longer-term recommendations to help planners in NATO's new center prioritize their efforts.

THE EVOLUTION OF THREATS TO UNDERSEA INFRASTRUCTURE IN NORTHERN EUROPE

The war in Ukraine has radically altered the threat landscape across Europe, particularly in the north. As the alliance remains focused on supporting Ukraine and shoring up its eastern flank, Sweden's and Finland's membership bids will provide new opportunities to deter Russian aggression in the Baltic and Arctic regions. But recent examples of CUI interference highlight vulnerabilities that will not be easily remedied. The sabotage of two Nord Stream pipelines off the Danish island of Bornholm in September 2022 forced European governments to grapple with their limited ability to deter and defend against hybrid tactics in the undersea domain.[4] Recent damage to the Balticconnector gas pipeline and a data cable between Finland and Estonia in October 2023 from a ship's anchor is suspected as being deliberate, although attribution has not yet been declared.[5]

In this context, the main focus of critical maritime infrastructure debates has shifted from emphasis on terrorism and cyber threats toward the increasing frequency and efficacy of hybrid tactics.[6] The aim of hybrid tactics is to cause significant damage to an adversary while operating below the threshold of detection, attribution, and response—and in so doing blur the conceptual lines between conflict and peace.[7] The issue is compounded in the maritime realm by several conceptual and practical challenges, mainly related to poor definitions highly dependent on moral or political choices, a unique geophysical space, and the multitude of potential threats.[8]

Russian hybrid tactics represent the most pressing threat to CUI in northern Europe. Russia's war against Ukraine has debilitated its ground forces and strained its military industrial base. Experts estimate it will take the Kremlin five to ten years to reconstitute its military.[9] Meanwhile, however, Russia's power projection capabilities in northern Europe—through naval, air, and missile bases in Kaliningrad and its Northern Fleet of submarines on the Kola Peninsula—have scarcely been depleted. In fact, while the Russian navy is underfunded and a large part of its fleet comprises Soviet legacy platforms, its underwater capacity continues to grow.[10] In particular, Russia's submarine program remains a priority amid other military budget cuts, exemplified by the Kremlin's authorization of 13 new nuclear and conventional submarines since 2014. In broader terms, Russia's ability to target critical infrastructure short of war and impose economic costs to deter external intervention in regional conflicts is an important component to Moscow's doctrine and thinking on escalation management.[11]

However, even in the absence of a broader Russia-NATO conflict, hybrid tactics have been a staple in the Kremlin's toolbox in Europe for years. As the Kremlin views itself in perpetual conflict with the West, hybrid tactics are instrumental to challenging NATO without resorting to conventional military means.[12] Russia has likely targeted critical infrastructure throughout Europe at an increased frequency since its full-scale invasion of Ukraine.[13] In the undersea domain, Russia appears committed to mapping and threatening European energy and communications infrastructure, particularly strategically important Norwegian gas pipelines and fiber-optic cables.[14]

The Nord Stream attacks resulted in a flurry of initiatives to bolster Europe's CUI. The European Union has updated its maritime strategy to better address evolving threats and adopted an expanded directive on CUI resilience, and the EU-NATO Task Force on Resilience of Critical Infrastructure was launched in January and reported its findings in June.[15] The EU Hybrid Toolbox, including the Hybrid Fusion Cell and new Hybrid Rapid Response Teams, support member states and NATO to detect, deter, and respond to threats.[16] More recently, the 10-nation Joint Expeditionary Force (JEF) agreed to focus on protecting CUI in its new vision and deployed a maritime task force in response to the Balticconnector incident to deter further attacks.[17] Bilateral examples include the recent UK-Norway strategic partnership on undersea threats.[18] Many nations have also expanded their ability to monitor and protect undersea infrastructure: France recently announced a new seabed warfare strategy and investments in ocean floor defense, and the United Kingdom has set up a Centre for Seabed Mapping and earmarked two new Multi-Role Ocean Surveillance (MROS) vessels to serve primarily as subsea protection ships.[19]

PROTECTING CRITICAL UNDERSEA INFRASTRUCTURE: A NEW FOCUS FOR NATO

While many stakeholders have increased their efforts to protect CUI, NATO remains the lead actor when it comes to deterring and preventing conventional and hybrid attacks on allies. NATO's role in protecting CUI is grounded in its founding principles, such as Articles 2 and 3 of the North Atlantic Treaty, which call for the strengthening of free institutions, economic collaboration, and growing resilience to attack.[20] At the 2023 Vilnius summit, allies reiterated that hybrid operations against the alliance could meet the threshold of armed attack and trigger Article 5, NATO's collective defense guarantee.[21]

THE VALUE OF NATO

Today, the functioning of allied civil society and the prosperity of member states depends on the extensive network of CUI across the Euro-Atlantic. NATO is critical to its protection for several reasons.

First, Russia—the primary threat—has the intent and capability, and it maximizes its opportunity to threaten allied CUI across NATO's area of operational responsibility. Moreover, the destruction, disruption, or tapping of CUI could be the precursor to conflict through attempting to sever military and government communications.[22] Second, the protection of CUI is part of NATO's defense and deterrence posture across the Euro-Atlantic. As hybrid attacks on CUI may meet the threshold for armed attack, NATO must be heavily invested in their protection to ensure it can act decisively.

Third, CUI spans NATO's entire area of operational responsibility, so maintaining seamless situational awareness across the whole network is a challenge far too large for individual nations.[23] Fourth, the challenge of protecting CUI will increasingly rely on technological solutions, and NATO possesses the financial heft and mechanisms to develop and scale these. Finally, there are complex political, legal, and technical considerations for the effective protection of CUI, and seams between national permissions and restrictions can create frictions best managed at the NATO level.

NATO'S APPROACH

NATO has been both proactive and reactive to CUI threats. In broad terms, NATO protects CUI in three ways. First, all of NATO's forces contribute to the alliance's Defence and Deterrence of the Euro-Atlantic Area (DDA), which coheres all activity by region and domain. Many capabilities that contribute to CUI protection also contribute to wider deterrence activities, including standing naval and mine countermeasures groups and CUI-focused exercises.[24]

Second, NATO assets detect threats through intelligence, surveillance, and reconnaissance (ISR) capabilities and space and cyber assets to gain and maintain situational awareness. Moreover, NATO can develop and scale new technologies to increase detection coverage, such as the Defence Innovation Accelerator for the North Atlantic (DIANA) pilot challenges, which include a focus on energy resilience and sensing and surveillance.[25] The alliance's new Digital Ocean Concept was endorsed in October 2023 to increase collective visibility of oceans, including

> the creation of a global scale network of sensors, from sea bed to space, to better predict, identify, classify and combat threats. It envisages maritime domain awareness, subsea sensors, unmanned surface vessels, drones and satellites, and exploits AI [artificial intelligence], big data, and autonomous systems, alongside conventional assets.[26]

Third, NATO has a range of response options once an incident or attack occurs, including counter hybrid support teams, the NATO Response Force (NRF) and Very High Readiness Task Force (VJTF), and ad hoc force deployments, such as the enhanced maritime patrol and mine hunter deployments in the Baltic Sea.[27] National missions and regional frameworks outside of NATO command structures can also bolster deterrence against threats to CUI, including the JEF and the aforementioned EU initiatives.

Table 1: European Institutions Relevant for Protecting CUI

Type/Function	Organization	Name	Location
Institutions	NATO	**Allied Maritime Command (MARCOM)**	Northwood, United Kingdom
	NATO	**Critical Undersea Infrastructure Coordination Cell**	Brussels, Belgium
	NATO	**Maritime Centre for the Security of Critical Underwater Infrastructure**	Northwood, United Kingdom
	NATO	**Shipping Centre**	Northwood, United Kingdom
	NATO	**Multinational Maritime Security Centre of Excellence (MARSEC COE)**	Istanbul, Turkey
	NATO	**Cooperative Cyber Defence Centre of Excellence**	Tallinn, Estonia
	NATO	**Strategic Communications Centre of Excellence**	Riga, Latvia
	NATO	**Civil-Military Cooperation Centre of Excellence**	The Hague, Netherlands
	NATO	**Counter Hybrid Support Teams**	N/A
	European Union	**Hybrid Fusion Cell**	Brussels, Belgium
	European Union	**Hybrid Rapid Response Teams**	N/A
	European Union/ NATO	**EU-NATO Task Force on Resilience of Critical Infrastructure**	N/A
	International Centre of Excellence	**European Centre of Excellence for Countering Hybrid Threats**	Helsinki, Finland
	International Centre of Excellence	**Euro-Atlantic Centre for Resilience**	N/A
	Framework nation construct	**Joint Expeditionary Force (JEF)**	N/A
Policy	NATO	**North Atlantic Treaty, Article 2—Economic collaboration**	N/A
	NATO	**North Atlantic Treaty, Article 3—Resilience**	N/A
	NATO	**North Atlantic Treaty, Article 5—Collective defense**	N/A
	NATO	**NATO Strengthened Resilience Commitment 2021**	N/A
	European Union	**Critical Entitites Resilience Directive**	N/A
Planning	NATO	**NATO Resilience Committee**	N/A
	NATO	**NATO Resilience Planning Process**	N/A
Fund	European Union	**Recovery and Resilience Facility**	N/A

Source: Authors' compilation.

NATO'S NEW CENTERS

In response to recent incidents in the Baltic Sea, NATO has expedited its approach to CUI protection by establishing two new organizations. In February 2023 the Critical Undersea Infrastructure Coordination Cell was created at NATO headquarters. The rationale was to coordinate allied activity; bring military and civilian stakeholders together by facilitating engagement with private industry, which owns much of the infrastructure; and better protect CUI through jointly detecting and responding to threats.[28] This new cell will be instrumental in building coordination across all the organizations, policies, and capabilities identified in Table 1 both within and external to NATO.

Then, at the July 2023 Vilnius summit, allies agreed to establish the Maritime Centre for the Security of Critical Underwater Infrastructure within NATO's Allied Maritime

Command (MARCOM). This new center focuses on

> identifying and mitigating strategic vulnerabilities and dependencies . . . to prepare for, deter and defend against the coercive use of energy and other hybrid tactics by state and non-state actors. . . . NATO stands ready to support Allies if and when requested.[29]

The center arrives at a crucial time for NATO as both new threats to CUI and new initiatives to deal with them proliferate across the alliance and beyond. To help NATO planners and staff at the new center conceptualize and prioritize their efforts, the next section considers in more detail the problem of protecting CUI.

UNDERSTANDING THREATS TO CRITICAL UNDERSEA INFRASTRUCTURE: A CONCEPTUAL FRAMEWORK

This section develops a basic framework for thinking about protecting CUI. The purpose is to help NATO planners—particularly those in the new center—to understand the vast problem space and prioritize some initial efforts over others. The following section draws on this framework to develop several recommendations.

The four elements of the framework for protecting CUI are outlined below.

1. **Infrastructure type:** What counts as CUI? Which parts are most critical or most vulnerable?
2. **Threat type:** What are the main threats to undersea CUI?
3. **Tasks:** What is NATO's role in protecting CUI?
4. **Geography:** Where should limited resources be prioritized and focused across the Euro-Atlantic area?

1. INFRASTRUCTURE TYPE

Maritime infrastructure is vital to basic societal functions such as trade, food and energy supplies, security and defense, communications, transport, tourism, and environmental management. The most important infrastructure is usually considered "critical," meaning without it, society could not function for long. But critical infrastructure differs between nations given that some economies depend on fishing or tourism while others rely more on maritime trade, energy infrastructure, or data cables. What counts as CUI, therefore, is often more of a political decision than a technical one. There is no one-size-fits-all definition: it depends on the nation and region in question.

Maritime infrastructure is often categorized by sector. One classification system lists five types: transport, energy, communication, fishing, and marine ecosystems.[30] Of these, four have substantial elements of underwater infrastructure. Above-water transport is often precluded, while commercial submersibles—such as remotely operated vehicles (ROVs) or autonomous underwater vehicles (AUVs) used in pipeline maintenance—are considered part of the energy infrastructure they serve.

Maritime infrastructure security policies traditionally focus on maritime transport (e.g., ports) and energy (e.g., gas and oil infrastructure) over other types.[31] However, the infrastructure picture is changing rapidly. Undersea cable projects have proliferated in recent years, while offshore renewable energy technologies like wind and tidal systems will increase to help nations meet global carbon emissions targets.[32] Future proliferation of AUVs—driven by new oil and gas exploration, military applications, reduced manufacturing costs, and improvements in AI and automation technology—could present both new types of CUI under the category of transport and new threats. As the recent NATO-EU task force on critical infrastructure summarizes,

> These challenges are compounded for undersea energy infrastructure, which is extensive and more difficult to survey and protect. Moreover, the network of undersea energy infrastructure in the Euro-Atlantic area is expected to grow as offshore energy platforms become more numerous.[33]

Meanwhile, fishing and marine ecosystems are increasingly important to some nations as fishing stocks decrease and marine habitats are degraded by pollution and the effects of climate change.

Beyond rapid change, there are several challenges associated with coordinating CUI protection, including interdependence, the physical characteristics of the subsea domain, and the complex, transnational nature of undersea infrastructure.[34] Meanwhile, fishing and marine ecosystems are increasingly important to some nations as fishing stocks decrease and marine habitats are degraded by pollution and the effects of climate change. This suggests a key challenge for NATO will be prioritizing between CUI sectors, which are critical to different NATO allies. This assessment will be driven to some extent by the next element of the framework: the threat picture.

2. THREAT

Although most definitions of critical infrastructure depend on how vital it is to the functioning of society, in practice governments tend to designate infrastructure as critical if it is vulnerable to harm. While pipeline sabotage has driven the headlines, the range of threats to CUI is much broader. The threat picture has also changed in recent years.

Maritime security threats have been driven by the rise of terrorism, international piracy, human trafficking, and the "blue economy," defined by the World Bank as "the sustainable use of ocean resources for economic growth, improved livelihoods, and ocean ecosystem health."[35] Protection of maritime and undersea infrastructure has typically focused on physical attacks from terrorism and blue crime (i.e., transnational organized crime at sea).[36] However, the threat environment has changed markedly over the last decade—and drastically since 2022. After invading Ukraine, Russia became "the most significant and direct threat to Allies' security," according to NATO's new Strategic Concept—a threat that includes the ability to "target our civilian and military infrastructure."[37]

NATO's new concept also points to hybrid threats to critical infrastructure and reaffirms their inclusion under Article 5.[38] The maritime domain has been viewed as particularly vulnerable to hybrid threats.[39] Attacks on underwater infrastructure have been a particular concern.[40] Recent events appear to confirm these fears, with several incidents such as the Nord Stream pipeline explosions in the Baltic Sea or severed subsea cables near Svalbard that appear to follow the hybrid playbook of deniable attacks on undersea infrastructure. These incidents highlight the difficulty of dealing with ambiguous hybrid threats, which are difficult to distinguish from accidental damage. For example, around 70 percent of undersea cable faults are caused by fishing vessels or ship anchors, alongside natural causes or even shark bites.[41] Hybrid aggressors can also use the cover of fishing, private, or research vessels, which are difficult to track. The rapid proliferation of AUVs will exacerbate the problem. Specialized vessels for the task also exist, such as Russia's dedicated fleet of submarines, designed for infrastructure sabotage and manned by the Russian navy and the Main Directorate for Deep Sea Research (GUGI).[42] Research vessels operated by GUGI are suspected of mapping networks of undersea infrastructure across Europe.[43]

For all these reasons, many assessments suggest a new era of hybrid threats is emerging and poses "a particular challenge" to protecting undersea infrastructure.[44] As the NATO-EU task force puts it, "The seabed is a field of growing strategic importance, due to increasing reliance on undersea infrastructure and the particular challenges in protecting it from hybrid threats and physical damage."[45]

3. TASKS

The final element of the framework comprises the tasks and missions NATO may have to carry out to protect CUI. The most important role, short of war, is deterrence, which holds the promise of avoiding armed attacks altogether. Beyond deterrence, military forces perform a wide range of roles relevant to protecting CUI.

One example is counterpiracy. During Operation Ocean Shield—NATO's contribution to international efforts to combat piracy off the Horn of Africa during 2008-16—the role of NATO forces spanned surveillance, interdiction, escort, and deterrence.[46] Cooperation with international bodies and the private sector was also vital to mission success, which contributed to the cessation of attacks after 2012.[47]

Another relevant example is protecting national infrastructure. The U.S. National Infrastructure Protection Plan outlines threats to national infrastructure and a framework of missions to protect them.[48] These are divided into two tasks: counterthreat missions and preparedness missions.[49]

- Counterthreat missions identify and counter threats and hazards: identify, deter, detect, disrupt, and prepare.
- Preparedness missions reduce vulnerabilities and mitigate the consequences of damage: prevent, protect, mitigate, respond, recover.

More broadly, several existing frameworks for countering hybrid threats may be applied to protecting CUI. NATO's strategy is to "prepare, deter, defend," while the European Union's approach is based on "awareness, resilience, and response."[50] Another framework is proposed by the 14-nation Multinational Capability Development Campaign (MCDC): "detect, deter, and respond."[51] This framework is used to examine NATO's role in protecting CUI regarding all three functions below. [52]

DETECT

Countering any threat requires first detecting and identifying it. Detection is even more important for hybrid threats, which rely on deniability or ambiguity to delay, complicate, or prevent reprisal. However, the variety and complexity of hybrid threats make detection challenging.[53]

For protecting CUI, the main focus is on enhancing maritime domain awareness (MDA).[54] MDA systems are "one of the core solutions in maritime security" but are focused on civil transport, fishing, and leisure.[55] To rectify this, a 2018 report by CSIS advocates a renewed focus on undersea MDA to combat hybrid threats.[56] Specific recommendations include establishing dedicated analytic centers (with teams focused on hybrid threats), training courses, a common classified data picture, and an operational framework that integrates surface and subsurface sensors. Another recent analysis recommends closing gaps in the surveillance of small boats, leisure craft, and underwater vehicles through "investments in new underwater sensors and drones which can enhance the overall picture of the domain."[57] The recent EU-NATO Task Force also recommends enhancing "maritime situational awareness."[58]

One detection challenge is that malign activity often appears, by design, as an accident, whereas some suspected attacks could actually be accidents (most damage to cables and pipelines is accidental). This means NATO does not have the luxury of ignoring apparent accidents. Here, a conceptual distinction between monitoring (known threats) and discovering (new, unknown threats) can help establish situational awareness and distinguish signal from noise in the realm of detection.[59] This task is also well suited to advances in AI and machine learning.[60]

DETER

Deterring hybrid threats to CUI is difficult but not impossible.[61] The most promising strategy is deterrence by denial, which reduces the prospects of successful attack by hardening the target and strengthening resilience to damage.[62] Denial in this context comprises two functions: prevention and resilience (see Figure 3). Preventing attacks is part of NATO's core business and is achieved through a combination of detection (see above) and physical presence. For example, NATO's Cold War deterrence strategy of basing substantial "shield forces" in central Europe was designed to physically prevent a Soviet attack.[63]

Resilience measures are designed to help CUI systems withstand or quickly recover from any damage sustained. Much of this amounts to good practice in the design and management of critical infrastructure systems.[64] Such measures are therefore generally low cost and less reliant on detecting threats; best practices for resilience are based on understanding and mitigating one's own vulnerabilities, regardless of whether they have been targeted. This is why resilience measures have become foundational to counter hybrid strategies.[65] However, resilience building is a long-term strategy that will take years to deliver given the vast size and complexity of Euro-Atlantic CUI.

RESPOND

Moreover, resilience is not a strategy on its own; deterrence by punishment also has a role.[66] When it comes to punishing low-level aggression, celerity beats severity most of the time, putting a premium on credible response options that can be deployed quickly and reliably.[67] These measures may not threaten vital interests but merely assure an aggressor will always face some costs for threatening CUI, however minor. This means simple measures such as enhanced presence or surveillance around key sites can work to deliver what has been referred to as "deterrence by detection."[68] More creative measures also play a role, such as attribution disclosure, legal interventions, or targeted sanctions (e.g., against implicated vessels, companies, or individuals).[69]

That credible responses are required suggests the utility of a preapproved playbook to counter hybrid threats to CUI.[70] Too often such measures are ad hoc or post hoc, or not sufficiently tailored to the specific demands of protecting CUI.[71] If military forces are part of the response (e.g., to provide surveillance or bolster presence), then a forward, flexible posture is required to ensure force elements are in the area of responsibility or held at high readiness to deploy to quickly generate effects.[72]

It is important to note that given the limited resources of allies, any increase in demand to protect CUI will likely require trade-offs with other tasks and missions. Any contribution to protecting CUI is important but not all-important. NATO's unique role—and the focus of the strategic concept—remains deterring armed attack above the threshold of war, not protecting against all forms of hybrid aggression.[73] Protecting CUI should therefore not be overemphasized in NATO's overall posture or capability development at the expense of conventional deterrence and defense.

4. GEOGRAPHY

The final element of the framework is geography. NATO is named after an ocean: the North Atlantic. But the alliance's undersea infrastructure picture is more complex. NATO's maritime areas of responsibility comprise the following:[74]

- High North region (including the Norwegian Sea, Greenland Sea, Barents Sea, and Arctic Ocean)
- Baltic Sea
- North Atlantic (including the North Sea, Irish Sea, English Channel, and Bay of Biscay)
- Mediterranean Sea (east and west)
- Black Sea
- North Pacific Ocean

Within these areas, the seascape of undersea infrastructure is extensive and complex. Figures 1-2 show the extent of underwater energy infrastructure (Figure 1) and subsea data cables (Figure 2) across Europe.

While data cables are uniformly spread across the Euro-Atlantic area, the picture is different for energy infrastructure, which is concentrated in northern Europe—namely the North Atlantic (North Sea) and High North (Norwegian Sea). This supply is critical to Europe: in the second quarter of 2023, the European Union imported 44.3 percent of its natural gas (in gaseous state) from Norway and 17.8 percent from the United Kingdom.[75] That 16.5 percent was from Algeria (through three subsea Mediterranean pipelines) also shows the importance of energy infrastructure in southern Europe.[76] This could increase in the future with new projects (such as the EastMed pipeline) and new gas field discoveries as Europe diversifies away from Russian supply.[77] Offshore wind energy infrastructure (along with subsea electrical cables) is also concentrated in northern Europe but present in significant amounts across Europe. Such infrastructure is also expanding quickly: under the European Green Deal, for example, offshore wind energy will expand over 25 times by 2030.[78]

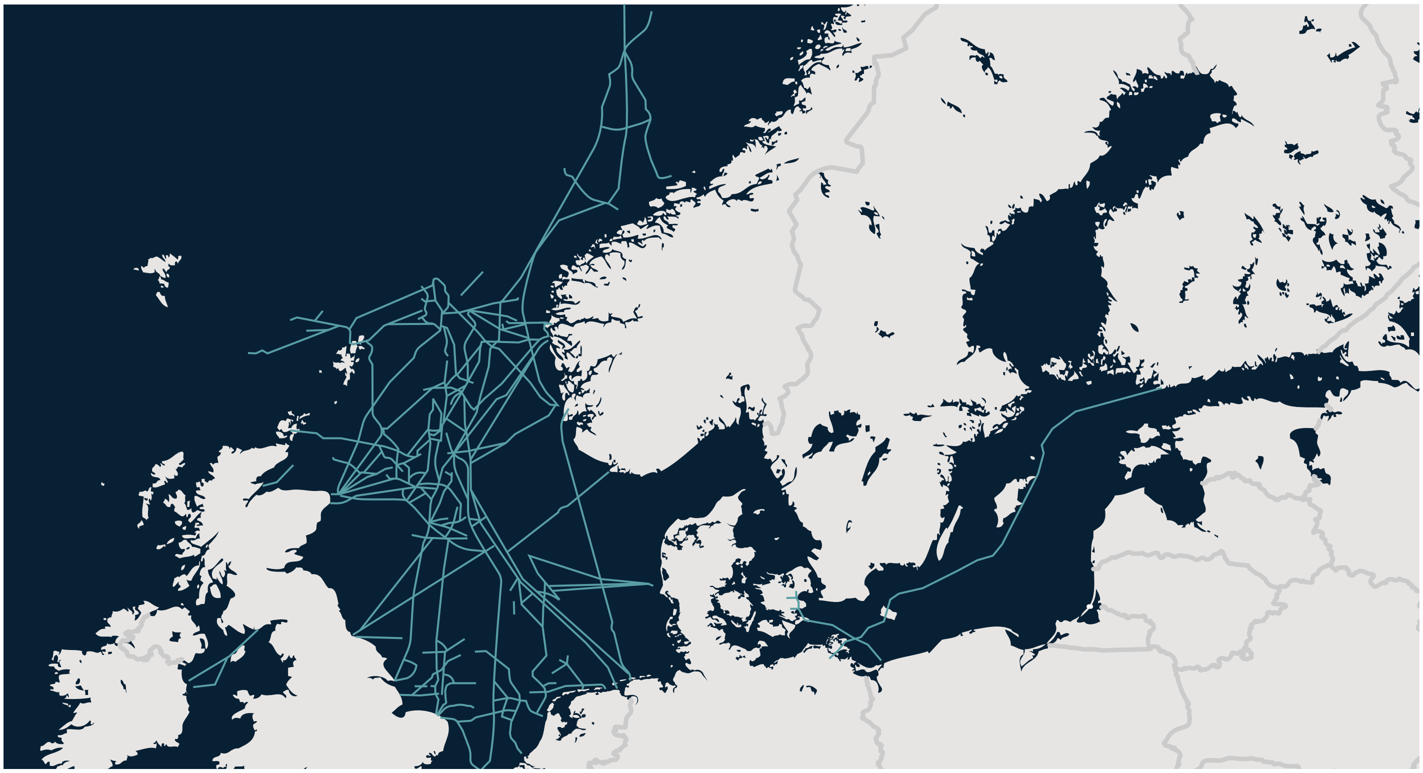
However, any judgment about prioritizing NATO's efforts to protect CUI in one region cannot rely on the density of infrastructure alone because all undersea infrastructure is proportionately important to each ally. In addition to including the views of all allies, any assessment must combine geography with the other elements of the framework. This task is explored in the final section of this brief.

RECOMMENDATIONS: WINNING THE FOURTH BATTLE OF THE ATLANTIC

The staff at NATO's new Maritime Centre for the Security of Critical Underwater Infrastructure do not have the luxury of pondering future threats. NATO's CUI is under attack right now. This situation may worsen as Russia tries to undermine Western support for Ukraine and cheaper, more advanced AUVs enable a wider range of actors to pose a threat. As Foggo, the former commander of the U.S. Naval Forces Europe and Allied Joint Force Command Naples, puts it: "the fourth battle of the Atlantic is underway." Like its predecessors, this battle is "a struggle between Russian forces that probe for weakness, and US and NATO anti-submarine warfare (ASW) forces that protect and deter. Just like in the Cold War, the stakes are high."[79]

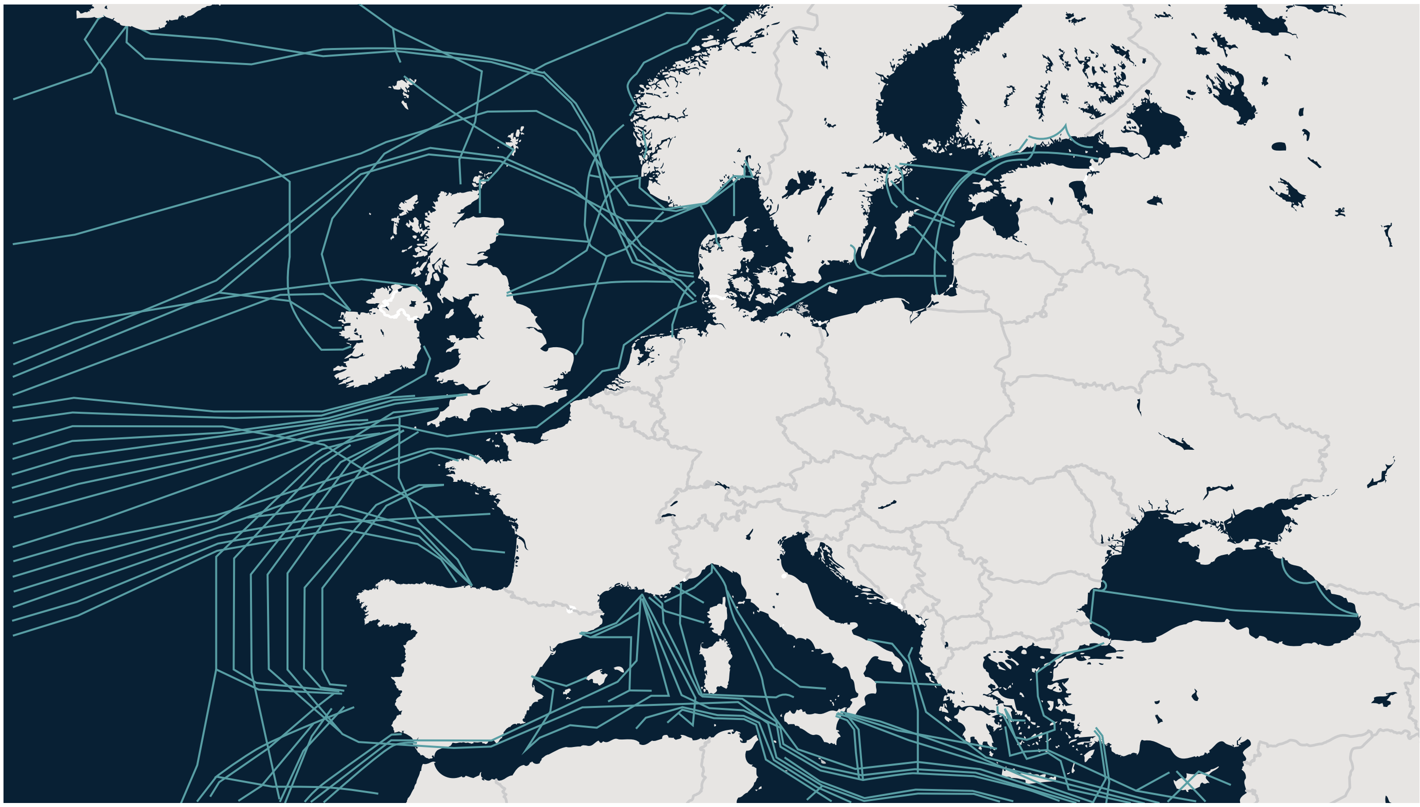
NATO and its new center must therefore act quickly. The final section provides a series of recommendations for NATO planners to conceptualize and prioritize their efforts in the coming years. The recommendations comprise two parts. The first is a general assessment of initial priorities for protecting CUI based on the four-part framework developed above. The second builds on this broad assessment to propose more specific and immediate actions.

Figure 1: Undersea Energy Infrastructure in Northern Europe



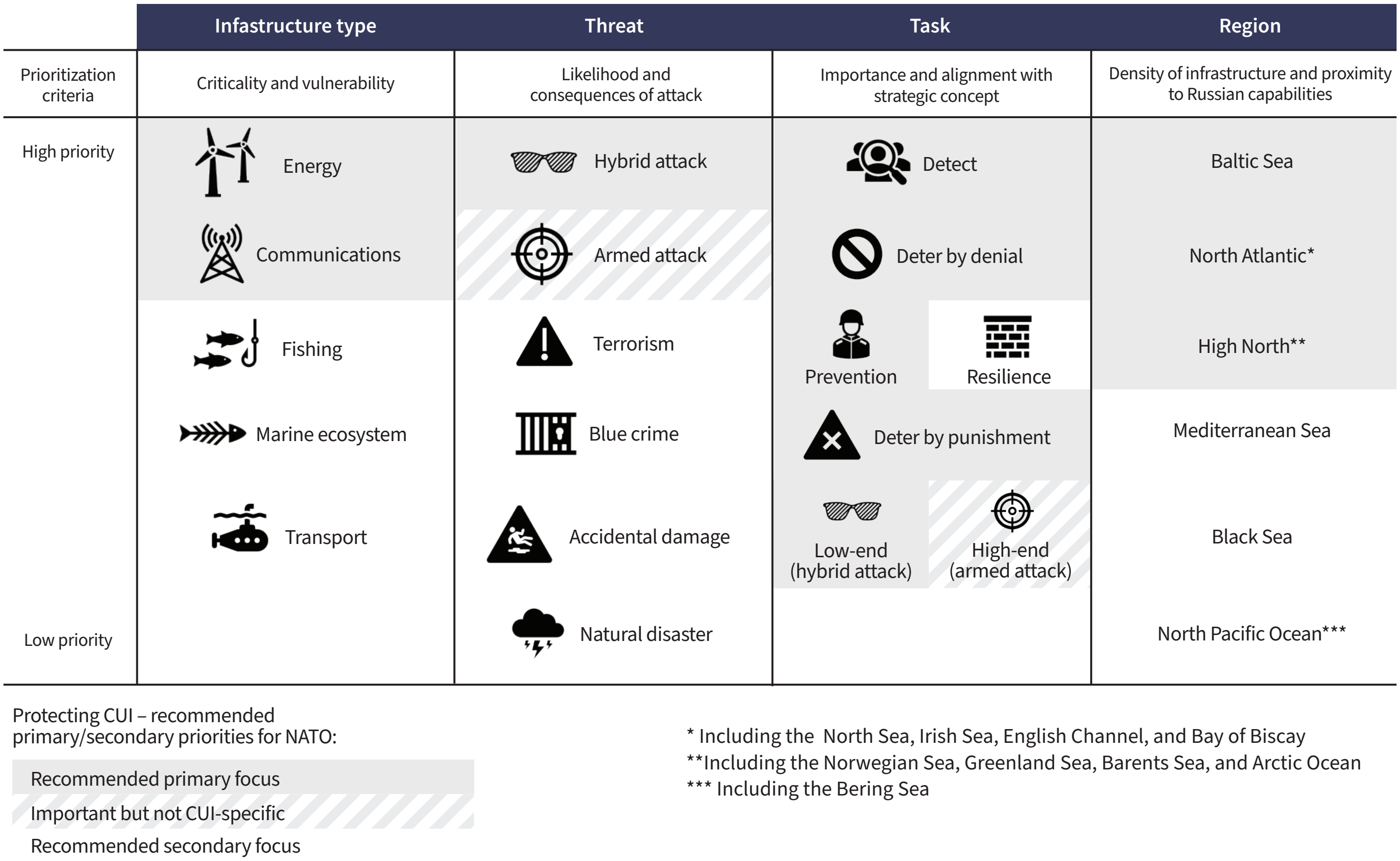
Source: Data from "European Atlas of the Seas," European Commission, https://ec.europa.eu/maritimeaffairs/atlas/maritime_atlas/.

Figure 2: Undersea Data Cables in Europe



Source: Data from "Submarine Cable Map," TeleGeography, https://www.submarinecablemap.com/, licensed under CC BY-SA 4.0.

Figure 3: A Framework for Protecting Critical Undersea Infrastructure



	Infastructure type	Threat	Task	Region
Prioritization criteria	Criticality and vulnerability	Likelihood and consequences of attack	Importance and alignment with strategic concept	Density of infrastructure and proximity to Russian capabilities
High priority	Energy	Hybrid attack	Detect	Baltic Sea
	Communications	Armed attack	Deter by denial	North Atlantic*
	Fishing	Terrorism	Prevention Resilience	High North**
	Marine ecosystem	Blue crime	Deter by punishment	Mediterranean Sea
	Transport	Accidental damage	Low-end (hybrid attack) High-end (armed attack)	Black Sea
Low priority		Natural disaster		North Pacific Ocean***

Protecting CUI – recommended primary/secondary priorities for NATO:

Recommended primary focus

Important but not CUI-specific

Recommended secondary focus

* Including the North Sea, Irish Sea, English Channel, and Bay of Biscay
**Including the Norwegian Sea, Greenland Sea, Barents Sea, and Arctic Ocean
*** Including the Bering Sea

Source: Authors' assessment.

GENERAL ASSESSMENT OF INITIAL PRIORITIES FOR PROTECTING CUI

This section presents a general indicative assessment of NATO's role in protecting CUI based on the framework discussed in Figure 3. The shaded area suggests where NATO's initial focus should be for protecting CUI. This assessment is discussed in more detail below, starting with the prioritization criteria for each element.

Infrastructure Type

Undersea infrastructure may be prioritized for protection by considering the criticality to NATO allies and vulnerability to different threats. Doing so suggests NATO focus on protecting energy and communications infrastructure—the most critical infrastructure to many NATO allies, whose developed economies depend on either importing or exporting energy and transmitting data. Such infrastructure is also the most vulnerable to attack, as recent attacks on pipelines and undersea cables have demonstrated. If further prioritization is required, it should be driven by an analysis of resilience of energy infrastructure compared to data cables: although both are vital and vulnerable, some systems are more resilient and easier to reconfigure in the event of damage.[80]

However, it is important to remember undersea infrastructure is much broader than pipelines and cables. Many NATO allies depend on fishing, the health of their marine ecosystems, and maritime security in the broadest sense. The rapid growth of AUVs may transform the transport sector, introducing new types of CUI and new threats. Most importantly, NATO's approach to protecting CUI will need to incorporate the preferences of all allies.

Threat

Threats may be prioritized by considering the likelihood and consequences of an attack. With this in mind, NATO should focus on hybrid or gray zone threats to CUI, as these are the most likely threats in the near term. At the same time, the most dangerous threat to NATO allies remains the threat of armed attack on CUI as a prelude to aggression or during conflict.

Terrorism targeted at CUI remains a risk, and blue crime is ever present. But other bodies should take the lead (e.g., national police and coast guards, multinational maritime security frameworks), with NATO providing support only where necessary, as with combating large-scale piracy. NATO can contribute to awareness of accidental damage through MDA and crisis response to natural damage and disaster, but these tasks should not drive alliance force structure or posture.

Task

The role of NATO assets in protecting CUI may be prioritized by considering the importance of relevant tasks and their role in NATO's Strategic Concept.[81] Deterrence and defense is the alliance's core task. Deterring armed aggression is NATO's raison d'être and remains its most important task. However, NATO's capacity to do this is dependent on its general deterrence posture and is not related to the specific problem of protecting CUI—so it is not considered a primary focus here (see Figure 3).[82] Within the context of protecting CUI, NATO should focus on three primary tasks:

- **Detect:** NATO should focus on detecting threats to CUI, as detection is the foundation of deterrence and critical for removing the cloak of ambiguity around hybrid threats. Detection can be strengthened through enhanced MDA in priority regions. This may require increasing the persistent presence of forces and assets that can contribute to MDA in the maritime, air, space, and cyberspace domains.
- **Deter by denial:** NATO should also focus on strengthening deterrence by denial by improving the defenses that can prevent attacks in the first place. This may also require strengthening the persistent presence of allied forces in regions of concern to protect key sites, reassure vulnerable allies, and deter aggressors. Wider resilience measures can also strengthen denial, but these are judged to be a lower priority for NATO because much of this infrastructure is owned and operated by civilian enterprises, not amenable to military solutions, and already subject to extensive efforts by other actors more suited to boosting public and private sector resilience—such as the European Union.
- **Deter by punishment:** Responses to imminent threats or attacks should prioritize speed and reliability over severity. In the context of deterring low-end hybrid threats (rather than high-end conventional threats) to CUI, this suggests the utility of maritime forces that are forward based in priority regions—or at least persistently present or rapidly deployable (i.e., held at high readiness). More broadly, existing NATO units such as countering hybrid threat teams also have a role to play in immediate incident response and recovery.[83]

However, although this assessment is focused on protecting allied CUI against hybrid threats, this should not unduly warp NATO's force posture. Any trade-offs in posture, capability, or readiness to deal with hybrid threats should not come at the expense of the credibility of NATO's ability to deal with—and thereby deter—armed aggression.

Region

Not all subregions within the Euro-Atlantic area are equal when it comes to protecting CUI. The extent of regional energy infrastructure, proximity to advanced Russian undersea capabilities, and track record of recent incidents (attacks and infrastructure mapping) suggest NATO should focus initially on the Baltic, North Atlantic, and High North regions. At the same time, NATO cannot afford to ignore other regions that are critical to allies and where Russian forces and other threats (such as terrorism and blue crime) are known to operate, including the Mediterranean and Black Sea region.

SPECIFIC RECOMMENDATIONS

The general assessment above, combined with the previous discussion of the four framework elements, suggests several more recommendations for NATO's role in protecting CUI. These are divided into two parts: immediate actions that the new NATO center should implement quickly and longer-term approaches that are equally important but may take more time.

Immediate Recommendations

- **Establish a new Standing NATO Maritime Group (SNMG) focused on protecting CUI.** NATO's four standing maritime groups are in high operational demand and none are focused on protecting CUI.[84] Considering the growing threat, NATO should consider establishing an “SNMG3” to focus on protecting CUI in northern Europe, focused on the Baltic Sea, North Sea, and Norwegian Sea (the areas of highest CUI density). The JEF task group that is currently deployed is a good example but only temporary.[85] The capabilities of the group should include submarines, anti-submarine warfare, maritime surveillance, and seabed mapping, with contributions from allies who specialize in this domain. The group would play a vital role in organizing and delivering the functions of detecting, deterring, and responding to attacks on CUI in priority regions described in this report.

- **Commission a CUI vulnerability triage.** Any approach to enhancing resilience starts with a vulnerability assessment.[86] An initial triage assessment of criticality versus vulnerability to a range of threats can help MARCOM and NATO direct limited resources to protecting and defending those assets most at risk. The initial assessment presented here forms a starting point, but NATO’s own assessment must consider all forms of infrastructure, threats, regions, and the preferences of all allies.
- **Develop a fused MDA picture.** A critical step in transforming MDA to improve detection and identification of threats to CUI will be fusing the existing intelligence picture across nations, the private and public sectors, and multinational and maritime domains (e.g., air, sea, subsea, space, and cyber).[87] Assessing the highest-priority infrastructure and threats can help identify which ISR capabilities and combinations not currently available to MARCOM are necessary to rapidly attribute malign activity.[88]
- **Produce regular CUI threat assessments.** NATO already produces maritime threat assessments for governments and the commercial sector that focus on threats such as terrorism—for example, through the NATO Maritime Shipping Centre (MSC).[89] These should either be expanded to include threats to CUI or be dedicated assessments that focus on nontraditional hybrid threats to CUI.
- **Clarify the role of NATO’s Critical Undersea Infrastructure Coordination Cell.** The cell is based in NATO headquarters, but its wide remit—which includes industry and civil-military engagement, best practice, and technology—and senior leadership may overlap with the new MARCOM center.[90] The coordination cell could perform the role the MSC did during Ocean Shield of protecting CUI, which will be even more important given CUI is mostly owned and operated by private companies.[91]
- **Implement a CUI exercise program.** Exercises are a vital part of NATO’s deterrence and reassurance efforts and have been stepped up over the last year. Yet CUI exercises have been limited and focused on technology.[92] A wider CUI exercise program using existing assets would deliver wider effects to deter adversaries and reassure allies and industry partners.[93]
- **Update NATO’s maritime strategy.** NATO’s maritime strategy is over 12 years old, does not mention Russia or China, and mentions undersea infrastructure only in passing.[94] It needs updating to reflect the new threat environment and NATO’s new Strategic Concept—including a focus on protecting CUI.[95] The new center should have a lead role in producing a new strategy—or at least a “Protecting CUI” annex.

Longer-Term Recommendations

- **Develop a NATO CUI resilience strategy.** Building on the vulnerability assessment, a longer-term effort that the new center could lead is developing a NATO CUI resilience strategy. This would meet NATO’s Strengthened Resilience Commitment and could inform (and be informed by) a NATO resilience planning process.[96]
- **Adopt a NATO CUI preparedness goal.** As part of a strengthened approach to CUI resilience, allies could commit to a NATO CUI preparedness goal to bolster national and pan-NATO approaches to preparing for attacks on CUI.[97]
- **Take a risk management approach.** The sheer variety of threats to CUI and the number of potential targets require an approach that prioritizes and manages risk. Even better than a risk-centric strategy would be an uncertainty-centric approach that seeks robustness against a range of unknowable threats.[98]
- **Develop a CUI attack response playbook.** Effective deterrence against CUI attacks requires a credible

and reliable set of measures to respond to threats or attacks on CUI. A counter-CUI playbook of military (and nonmilitary) response options would help.[99] This playbook could also be the basis of a robust exercise program.

- **Adopt a framework nation approach to regional CUI protection.** A regional framework nation approach to protecting CUI could help tailor CUI protection to the differing concerns of regional allies.[100] One example is the JEF, newly focused on protecting northern Europe's CUI.[101] Whatever the framework, any regional approach to protecting CUI should be directed by the alliance's DDA concept, NATO's guiding framework for all operations short of war, and align with new regional plans agreed at the Vilnius summit.[102] ■

***Sean Monaghan** is a visiting fellow with the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C. **Otto Svendsen** is a research associate with the CSIS Europe, Russia, and Eurasia Program. **Mike Darrah** is a military fellow with the CSIS International Security Program. **Ed Arnold** is a research fellow with the International Security department at the Royal United Services Institute.*

This brief is made possible by general funding to CSIS and generous support from the Norwegian Ministry of Foreign Affairs.

Cover Photo: JONATHAN NACKSTRAND/AFP via Getty Images

ENDNOTES

[1] James Foggo and Alarik Fritz, "The Fourth Battle of the Atlantic," *Proceedings* 142, no. 6 (June 2016), https://www.usni.org/magazines/proceedings/2016/june/fourth-battle-atlantic.

[2] See "Russia a 'Risk' to Undersea Cables, Defence Chief Warns," BBC News, December 15, 2017, https://www.bbc.com/news/uk-42362500; and Rishi Sunak, "Undersea Cables: Indispensable, Insecure," Policy Exchange, December 1, 2017, https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/.

[3] NATO, "Vilnius Summit Communiqué," Press release, July 11, 2023, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

[4] Sean Monaghan, "Five Steps NATO Should Take after the Nord Stream Pipeline Attack," CSIS, *Commentary*, October 6, 2022, https://www.csis.org/analysis/five-steps-nato-should-take-after-nord-stream-pipeline-attack.

[5] Richard Milne, "Finland Investigates Potential Sabotage to Baltic Gas Pipeline," *Financial Times*, October 10, 2023, https://www.ft.com/content/8d9baf58-22c2-4456-905c-15fd7f9dcd69; Claudia Chiappa and Pierre Emmanuel Ngendakumana, "'Everything indicates' Chinese ship damaged Baltic pipeline on purpose, Finland says," *Politico*, December 1, 2023, https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/.

[6] Christian Bueger and Tobias Liebetrau, "Critical Maritime Infrastructure Protection: What's the Trouble?" *Marine Policy* 155 (September 2023): 105772, https://doi.org/10.1016/j.marpol.2023.105772.

[7] Helmi Pillai, "Protecting Europe's Critical Infrastructure from Russian Hybrid Threats," Centre for European Reform, April 25, 2023, https://www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid.

[8] Bueger and Liebetrau, "Critical Maritime Infrastructure Protection."

[9] Paul Schwartz, *A War of Attrition* (Washington, DC: CSIS, July 2023), https://www.csis.org/analysis/war-attrition.

[10] Geoffrey F. Gresh, *Europe's New Maritime Security Reality: Chinese Ports, Russian Bases, and the Rise of Subsea Warfare* (Washington, DC: Brookings Institution, February 2023), https://www.brookings.edu/articles/europes-new-maritime-security-reality-chinese-ports-russian-bases-and-the-rise-of-subsea-warfare/.

[11] Michael Kofman, Anya Fink and Jeffrey Edmonds, "Russian Strategy for Escalation Management: Evolution of Key Concepts", Center for Naval Analyses, April 2020, https://www.cna.org/reports/2020/04/DRM-2019-U-022455-1Rev.pdf; and Sidharth Kaushal, "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," Royal United Services Institute for Defence and Security Studies, May 25, 2023, https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.

[12] Vladimir Putin, "Russian President's Decree about National Security Strategies," Russian Military and Security Research Group, July 2, 2021, https://rusmilsec.files.wordpress.com/2021/08/nss_rf_2021_eng_.pdf.

[13] Pillai, "Protecting Europe's Critical Infrastructure."

[14] Ibid.

[15] European Commission, "Maritime Security: EU Updates Strategy to Safeguard Maritime Domain against New Threats," Press release, March 10, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1483; European Commission, "New Stronger Rules Start to Apply for the Cyber and Physical Resilience of Critical Entities and Networks," Press release, January 16, 2023, https://digital-strategy.ec.europa.eu/en/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks; and EU-NATO Task Force on the Resilience of Critical Infrastructure, *Final Assessment Report* (Brussels: European Commission, June 2023), https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf.

[16] European Union, *A Strategic Compass for Security and Defence* (Maastricht, Netherlands: European Union, n.d.), 34, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

[17] UK Ministry of Defence and Ben Wallace, "Joint Statement by Joint Expeditionary Force Ministers," UK Government, June 13, 2023, https://www.gov.uk/government/news/joint-statement-by-joint-expeditionary-force-ministers-june-2023; and Melisa Cavcic, "After pipeline incident, JEF partners pool resources for subsea infrastructure protection in Baltic Sea," *Offshore Energy*, December 5, 2023, https://www.offshore-energy.biz/after-pipeline-incident-jef-partners-pool-resources-for-subsea-infrastructure-protection-in-baltic-sea/.

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

[19] Ministère des Armées, *Ministerial Strategy for Seabed Warfare* (Paris: Ministère des Armées, February 2022), https://archives.defense.gouv.fr/content/download/636000/10511901/file/20220214_FRENCH%20SEABDED%20STRATEGY_key%20points.pdf; Peter O'Brien, "France Tightens Subsea Cable Security amid Growing Fear of Sabotage," *Politico*, October 13, 2022, https://www.politico.eu/article/france-tighten-subsea-cable-security-fear-sabotage-pipeline-gas-leak/; "What Is the UK Centre for Seabed Mapping (UK CSM)?" UK Hydrographic Office, https://www.admiralty.co.uk/uk-centre-for-seabed-mapping; and Naval News Staff, "First of Two MROS Ships Arrives in the UK," Naval News, January 19, 2023, https://www.navalnews.com/naval-news/2023/01/first-of-two-mros-ships-arrives-in-the-uk/.

[20] "The North Atlantic Treaty," NATO, October 19, 2023, https://www.nato.int/cps/en/natohq/official_texts_17120.htm.

[21] NATO, "Vilnius Summit Communiqué."

[22] Colin Wall and Pierre Morcos, "Invisible and Vital: Undersea Cables and Transatlantic Security," CSIS, *Commentary*, June 11, 2021, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security.

[23] Njall Trausti Fridbertsson, *Protecting Critical Maritime Infrastructure–The Role of Technology* (Brussels: NATO Parliamentary Assembly, October 7, 2023), 1.

[24] "NATO Focus Is on Critical Undersea Infrastructure during Series of Multi-domain Exercises with Latest Autonomous Vehicles in Portugal," MARCOM, October 4, 2023, https://mc.nato.int/media-centre/news/2023/nato-focus-is-on-critical-undersea-infrastructure-during-series-of-multidomain-exercises-with-latest-autonomous-vehicles-in-portugal.

[25] "Challenges," NATO Defence Innovation Accelerator for the North Atlantic, https://www.diana.nato.int/challenges.html.

[26] "Maritime Unmanned Systems Innovation Advisory Board Discuss NATO Innovation in the Maritime Domain," NATO, November 9, 2021, https://www.nato.int/cps/en/natohq/news_188548.htm?selectedLocale=en.

[27] "NATO Steps Up Baltic Sea Patrols after Subsea Infrastructure Damage," NATO, October 19, 2023, https://www.nato.int/cps/en/natohq/news_219500.htm.

[28] "NATO Stands Up Undersea Infrastructure Coordination Cell," NATO, February 15, 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.

[29] NATO, "Vilnius Summit Communiqué."

[30] Bueger and Liebetrau, "Critical Maritime Infrastructure Protection."

[31] Ibid.

[32] Brian Quigley, "Meet Nuvem, a Cable to Connect Portugal, Bermuda, and the U.S.," Google Cloud, September 25, 2023, https://cloud.google.com/blog/products/infrastructure/introducing-the-nuvem-subsea-cable; and Brian Quigley, "Connecting the South Pacific with New Subsea Cables," Google Cloud, October 25, 2023, https://cloud.google.com/blog/products/infrastructure/honomoana-and-tabua-subsea-cables-connect-south-pacific. See also Morcos and Wall, "Invisible and Vital." On offshore energy, see "Offshore Renewable Energy," European Commission, https://energy.ec.europa.eu/topics/renewable-energy/offshore-renewable-energy_en.

[33] EU-NATO Task Force, *Final Assessment Report*.

[34] Bueger and Liebetrau, "Critical Maritime Infrastructure Protection."

[35] "What Is the Blue Economy?," World Bank, June 6, 2017, https://www.worldbank.org/en/news/infographic/2017/06/06/blue-economy; Christian Bueger and Timothy Edmunds, "Beyond Seablindness: A New Agenda for Maritime Security Studies," *International Affairs* 93, no. 6 (2017): 1293–1311, https://doi.org/10.1093/ia/iix174; and "Alliance Maritime Strategy," NATO, June 17, 2011, https://www.nato.int/cps/en/natohq/official_texts_75615.htm;

[36] Bueger and Liebetrau, "Critical Maritime Infrastructure Protection."

[37] "NATO 2022—Strategic Concept," NATO, 2022, https://www.nato.int/strategic-concept/.

[38] Ibid.

[39] See, for example, Martin Murphy, Frank G. Hoffman and Gary Schaub Jr., *Hybrid Maritime Warfare and the Baltic Sea Region* (Copenhagen, Denmark: Centre for Military Studies, November 2016), https://cms.polsci.ku.dk/publikationer/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf; Andrew Metrick and Kathleen H. Hicks, *Contested Seas: Maritime Domain Awareness in Northern Europe* (Washington, DC: CSIS, 2018), https://www.csis.org/programs/international-security-program/global-threats-and-regional-stability/contested-seas; Tiia Lohela and Valentin Schatz (eds.), "Hybrid CoE Working Paper 5: HANDBOOK ON MARITIME HYBRID THREATS – 10 Scenarios and Legal Scans," Hybrid COE, November 22, 2019, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-5-handbook-on-maritime-hybrid-threats-10-scenarios-and-legal-scans/; Georgios Giannoulis (ed.), "Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans," Hybrid COE, March 2, 2023, https://www.hybridcoe.fi/publications/hybrid-coe-paper-16-handbook-on-maritime-hybrid-threats-15-scenarios-and-legal-scans/; and Teresa Usewicz and Jarosław Keplin, "Hybrid Actions and Their Effect on EU Maritime Security," *Journal on Baltic Security* 9 (2023), no. 1, 32–68, https://journalonbalticsecurity.com/journal/JOBS/article/112/info.

[40] See "Russia a 'Risk'," BBC News; and Sunak, "Undersea Cables."

[41] "The Biggest Threat to Subsea Cables," Ultramap Global, September 3, 2020, https://ultramapglobal.com/the-biggest-threat-to-subsea-cables/; Nicholas Kazaz, "Subsea Cable Damage Claims: The Legal Approach," Holman Fenwick Willan, April 2020, https://www.hfw.com/Subsea-Cable-Damage-Claims-The-Legal-Approach-April-2020; and Olivia Solon and Mark Bergen, "Fishing Boats Can't Stop Running over Ocean Internet Cables," Bloomberg, April 24, 2023, https://www.bloomberg.com/news/articles/2023-04-24/fishing-boats-keep-running-over-ocean-internet-cables. Because undersea infrastructure is so vulnerable to accidental damage, companies who own it often make their location public for navigation purposes—information that is also useful to would-be saboteurs.

[42] Kaushal, "Stalking the Seabed."

[43] Sabine Siebold, "NATO Says Moscow May Sabotage Undersea Cables as Part of War on Ukraine," Reuters, May 3, 2023, https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/; and Morten Soendergaard Larsen, "Russian 'Ghost Ships' Are Turning the Seabed into a Future Battlefield," *Foreign Policy*, May 2, 2023, https://foreignpolicy.com/2023/05/02/russia-europe-denmark-spy-surveillance-ships-seabed-cables/.

[44] Bueger and Liebetrau, "Critical Maritime Infrastructure Protection."

[45] EU-NATO Task Force, *Final Assessment Report*.

[46] "In sum, NATO's role was to prevent and stop piracy through direct actions against pirates, by providing naval escorts and deterrence, while increasing cooperation with other counter-piracy operations in the area in order to optimise efforts and tackle the evolving pirate trends and tactics." See "Counter-Piracy Operations (2008–2016)," NATO, May 19, 2022, https://www.nato.int/cps/en/natohq/topics_48815.htm?selectedLocale=en.

[47] Christian Brueger, "'Ocean Shield' Achieved Its Mission," *The Maritime Executive*, January 2, 2017, https://maritime-executive.com/blog/ocean-shield-achieved-its-mission.

[48] Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: Department of Homeland Security, 2013), https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

[49] Ibid., 18–19.

[50] "Countering Hybrid Threats," NATO, last updated August 18, 2023, https://www.nato.int/cps/en/natohq/topics_156338.htm; European Commission, *A Europe That Protects: Countering Hybrid Threats* (Brussels: European Commission, June 2018), https://www.dsn.gob.es/sites/dsn/files/hybrid_threats_en_final.pdf.

[51] Sean Monaghan, *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare* (London: UK Government, March 2019), https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf.

[52] The NATO and EU strategies are too high-level for this purpose.

For example, the "prepare" and "awareness" functions are too broad to develop specific tasks, while "prepare" is a function of deterrence (by denial). The NATO term "defend" is too limiting, as responses to hybrid attacks may involve broader goals such as reestablishing deterrence, reassuring allies, or recovering failed systems. Hence, the MCDC framework is used herein.

[53] Patrick Cullen, *Hybrid Threats as a New 'Wicked Problem' for Early Warning* (Helsinki: Hybrid CoE, May 2018), https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/.

[54] MDA is a broad term for "effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment" of a given region. Department of Homeland Security, *National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security* (Washington, DC: Department of Homeland Security, October 2005), https://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf.

[55] Bueger and Liebetrau, "Critical Maritime Infrastructure Protection."

[56] Metrick and Hicks, *Contested Seas*.

[57] Bueger and Liebetrau, "Critical Maritime Infrastructure Protection."

[58] EU-NATO Task Force on the Resilience of Critical Infrastructure, *Final Assessment Report*.

[59] Monaghan, *MCDC Countering Hybrid Warfare Project*, 22, 25–32; and Sean Monaghan and Tim McDonald, "Campaigning in the Grey Zone: Towards a Systems Approach to countering Hybrid Threats," The Hague Center for Strategic Studies, October 31, 2023, https://hcss.nl/report/campaigning-grey-zone-towards-systems-approach-countering-hybrid-threats/, 8.

[60] Jake Harrington and Riley McCabe, "Detect and Understand: Modernizing Intelligence for the Gray Zone," CSIS, *CSIS Briefs*, December 7, 2021, https://www.csis.org/analysis/detect-and-understand-modernizing-intelligence-gray-zone.

[61] Sean Monaghan, *Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice*, Hybrid CoE Paper 12 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, March 2022).

[62] Ibid., 15.

[63] Sean Monaghan, "Resetting NATO's Defense and Deterrence: The Sword and the Shield Redux," CSIS, *CSIS Briefs*, June 28, 2022, https://www.csis.org/analysis/resetting-natos-defense-and-deterrence-sword-and-shield-redux.

[64] Examples including designing systems to fail safely, exceeding basic requirements for critical components, and mitigating resilience failures. See "Principles for Resilient Infrastructure," UN Office for Disaster Risk Reduction, March 14, 2022, https://www.undrr.org/publication/principles-resilient-infrastructure.

[65] Ibid., 18. The EU-NATO Task Force focuses on resilience, for example.

[66] Ibid., 19. The limits of resilience include the challenge of highly motivated adversaries, the size of the task (of addressing every potential vulnerability across government and society), and the desirability of shoring up open societies.

[67] See, for example, Lawrence Freedman, *Deterrence* (Hoboken, NJ: Wiley, 2004); Matus Halas, "NATO's Sub-conventional Deterrence: The Case of Russian Violations of the Estonian Airspace," *Contemporary Security Policy* 43, no. 2 (2022): 350–381, https://doi.org/10.1080/13523260.2022.2028464; and "Why Is America's Capital So Violent?" *The Economist*, October 30, 2023, https://www.economist.com/united-states/2023/10/30/why-is-americas-capital-so-violent.

[68] Thomas G. Mahnken, Travis Sharp, Chris Bassler, Bryan W. Durkee, "Implementing Deterrence by Detection: Innovative Capabilities, Processes, and Organizations for Situational Awareness in the Indo-Pacific Region," Center for Strategic and Budgetary Assessments, July 14, 2021, https://csbaonline.org/research/publications/implementing-deterrence-by-detection-innovative-capabilities-processes-and-organizations-for-situational-awareness-in-the-indo-pacific-region.

[69] Ibid., 20–21.

[70] Ibid., 20–21; Monaghan, "Five Steps NATO Should Take after the Nord Stream Pipeline Attack."

[71] "NATO Boosts Baltic Patrols after Undersea Infrastructure Damage," Reuters, October 19, 2023, https://www.reuters.com/world/europe/nato-boosts-baltic-patrols-after-undersea-infrastructure-damage-2023-10-19/.

[72] Sean Monaghan, "A New Vision to Deal with Familiar Threats in Northern Europe," CSIS, *Commentary*, October 27, 2023, https://www.csis.org/analysis/new-vision-deal-familiar-threats-northern-europe.

[73] Sean Monaghan, "Bad Idea: Winning the Gray Zone," *Defense360*, CSIS, December 17, 2021, https://defense360.csis.org/bad-idea-winning-the-gray-zone/.

[74] See the European Atlas of the Seas project: https://ec.europa.eu/maritimeaffairs/atlas/maritime_atlas/.

[75] "EU Imports of Energy Products Continued to Drop in Q2 2023," Eurostat, September 25, 2023, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230925-1.

[76] Kimberly Peterson and Eric Han, "In 2021, Algeria Produced Record Amounts of Natural Gas," U.S. Energy Information Administration, May 23, 2023, https://www.eia.gov/todayinenergy/detail.php?id=56580.

[77] Joshua Krasna, "A Long, Hot Summer for Eastern Mediterranean Gas Politics," Foreign Policy Research Institute, September 26, 2023, https://www.fpri.org/article/2023/09/a-long-hot-summer-for-eastern-mediterranean-gas-politics/; and "Rethinking Gas Diplomacy in the Eastern Mediterranean," International Crisis Group, April 26, 2023, https://www.crisisgroup.org/middle-east-north-africa/east-mediterranean-mena-turkiye/240-rethinking-gas-diplomacy-eastern.

[78] "Offshore Renewable Energy," European Commission, https://energy.ec.europa.eu/topics/renewable-energy/offshore-renewable-energy_en.

[79] James Foggo, "The Fourth Battle of the Atlantic Is Underway," Center for European Policy Analysis, January 17, 2023, https://cepa.org/article/the-fourth-battle-of-the-atlantic-is-underway/.

[80] The Balticconnector pipeline that was damaged in October 2023, for example, is a bidirectional pipeline allowing excess natural gas to easily be transferred between Estonia and Finland. While valuable, it is "not critical to Finland's energy supply." Emily Rauhala, "Finland Raises Specter of Sabotage of Baltic Sea Gas Pipeline," *Washington Post*, October 10, 2023, https://www.washingtonpost.com/world/2023/10/10/finland-gas-pipeline-leak-sabotage/. See also Toomas Pott, "Elering: No Impact on Gas Supply If Estonia-Finland Pipeline Damaged," ERR, September 28,

2022. https://news.err.ee/1608731584/elering-no-impact-on-gas-supply-if-estonia-finland-pipeline-damaged.

81 "NATO 2022–Strategic Concept," NATO.

82 The alliance's general deterrence posture is delivered by its nuclear and conventional deterrence posture. The latter includes DDA and NATO's regional plans.

83 Monaghan, "Five Steps."

84 All four are commanded by MARCOM to provide operational presence and rapid response across the Euro-Atlantic area. Two groups are general purpose and two are focused on mine clearance and countermeasures. See "NATO's maritime activities," NATO HQ, last updated August 3, 2023, https://www.nato.int/cps/en/natohq/70759.htm.

85 UK Ministry of Defence, "Royal Navy task force to deploy with JEF partners to defend undersea cables," Press release, November 30, 2023, https://www.gov.uk/government/news/royal-navy-task-force-to-deploy-with-jef-partners-to-defend-undersea-cables.

86 This is advocated in the U.S. National Infrastructure Protection Plan, among other places. See Department of Homeland Security, *NIPP 2013*.

87 Metrick and Hicks, *Contested Seas*.

88 While transparency around undersea vulnerabilities will enable quick work with government and industry partners with little risk of exposing new vulnerabilities (unlike cyberspace), the fact that many undersea surveillance capabilities were developed to find and track nuclear submarines and remain highly classified will provide a challenge.

89 "NATO Shipping Centre Threat Summary for the Mediterranean," NATO, July 12, 2023, https://shipping.nato.int/nsc/operations/news/-2022/threat-assessment-to-commercial-shipping-in-the-mediterranean.

90 "NATO Stands Up," NATO.

91 The success of Ocean Shield was due to "a revolution" in NATO's coordination with the private sector through the MSC. Brueger, "'Ocean Shield' Achieved."

92 "NATO Focus Is on Critical Undersea Infrastructure," MARCOM.

93 For example, NATO's robust response to the Balticconnector incident could have been exercised and not delivered ad hoc. See "NATO Steps Up," NATO.

94 See "Alliance Maritime Strategy," NATO; Steven Horrell, "NATO's Maritime Strategy Is Badly Outdated," Center for European Policy Analysis, July 10, 2023, https://cepa.org/article/natos-maritime-strategy-is-badly-outdated/; and Steven Horrell, Magnus Nordenman, and Walter B. Slocombe, "Updating NATO's Maritime Strategy," Atlantic Council, July 5, 2016, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/updating-nato-s-maritime-strategy/.

95 For example, the European Union updated its maritime strategy in March to "enhance our defences against cyber and hybrid threats, and reinforce the protection of critical maritime infrastructure," according to EU commissioner Virginijus Sinkevičius, quoted in European Commission, "Maritime Security."

96 "Strengthened Resilience Commitment," NATO, September 13, 2022, https://www.nato.int/cps/en/natohq/official_texts_185340.htm; and Anna Dowd and Cynthia Cook, "Bolstering Collective Resilience in Europe," CSIS, *CSIS Briefs*, December 9, 2022, https://www.csis.org/analysis/bolstering-collective-resilience-europe.

97 One example is the U.S. National Preparedness Goal: "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." See "National Preparedness Goal," U.S. Federal Emergency Management Agency, March 21, 2023, https://www.fema.gov/emergency-managers/national-preparedness/goal.

98 Vincent A. W. J. Marchau, Warren E. Walker, Pieter J. T. M. Bloemen, and Steven W. Popper, eds., *Decision Making under Deep Uncertainty: From Theory to Practice* (Berlin: Springer Nature, 2019).

99 Monaghan, "Five Steps."

100 Sean Monaghan and Ed Arnold, "Indispensable: NATO's Framework Nations Concept beyond Madrid," CSIS, *CSIS Briefs*, June 27, 2022, https://www.csis.org/analysis/indispensable-natos-framework-nations-concept-beyond-madrid.

101 Monaghan, "A New Vision."

102 Sean Monaghan, Sissy Martinez, Otto Svendsen, Carlota García Encina, and Mathieu Droin, "What Happened at NATO's Vilnius Summit?" CSIS, *Critical Questions*, July 14, 2023; and Kevin Ryan, "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA)," Belfer Center for Science and International Affairs, August 2, 2023. https://www.belfercenter.org/publication/natos-concept-deterrence-and-defence-euro-atlantic-area-dda.