NATO PARLIAMENTARY ASSEMBLY
ASSEMBLEE PARLEMENTAIRE DE L'OTAN

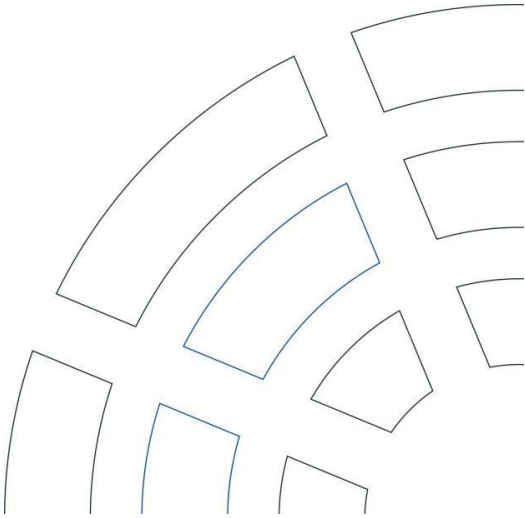
SCIENCE AND TECHNOLOGY COMMITTEE (STC)

PROTECTING CRITICAL MARITIME INFRASTRUCTURE – THE ROLE OF TECHNOLOGY

General Report
Njall Trausti FRIDBERTSSON (Iceland)
General Rapporteur

032 STC 23 E rev.2 fin – Original: English – 7 October 2023

Founded in 1955, the NATO Parliamentary Assembly acts as a consultative interparliamentary organisation which is institutionally separate from NATO. This document was adopted by the Science and Technology Committee at the 2023 NATO PA Annual Session in Copenhagen, Denmark. It is based on information from publicly available sources or NATO PA meetings – which are all unclassified.



EXECUTIVE SUMMARY

Critical infrastructure in the maritime domain facilitates the continuous delivery of basic services such as energy and communication, particularly the internet. The importance of these networks has dramatically increased in recent years, yet the responsibilities for protecting and regulating them have become less clear.

The need for action is in large part driven by technology. Seabed activities are transforming rapidly due to the proliferation of undersea technology such as remotely operated devices capable of conducting sophisticated operations deep under water. These advancements provide new possibilities for defence, but also enable adversaries to capitalise on existing vulnerabilities. 'Seabed warfare' is no longer a distant concept: it represents an immediate and legitimate threat to Allies.

Further complicating the issue, the majority of maritime infrastructure is controlled or operated by private entities, rendering protection, threat detection, and regulation of these vital networks even more complex.

For too long, this essential equipment has been increasingly utilised yet insufficiently surveyed, protected, and regulated. Although some Allied governments are working to patch vulnerabilities, particularly following the Nord Stream sabotage, additional effort, investment, and coordination are urgently needed. The paper deals with critical maritime infrastructure in general. However, the focus of the report is primarily on the challenges to the Allied underwater critical infrastructure.

TABLE OF CONTENTS

I- INTRODUCTION

1. The first British action against Imperial Germany at the start of the First World War was to cut the German undersea communication cables. This forced Germany to use British cables for its overseas communications and allowed London to read German cable traffic throughout the war. The security of critical maritime infrastructure (CMI) has always been an important issue. This is particularly the case for the Allies; NATO is, after all, a transatlantic *maritime* alliance, and the need for secure communications and the safe deployment and replenishment of forces in the event of war has always been a paramount issue.

2. Thanks to globalisation, which has led to a significant increase in maritime trade and the Internet, the importance of the CMI has only grown. The Nord Stream pipeline attacks in September 2022 have drawn attention to the vulnerability of Allies' CMI. Though it is vital for our economies and national security, the protection of CMI is still hampered by a persistent lack of awareness of the threats and coordination of responses. The 'critical' aspect of CMI refers to the necessity of these systems, networks, and objects to facilitate vital functions of states, including governmental and non-governmental actors. These essential connection points enable international economies and governments to function, yet they remain vulnerable to damage and disruption, including malicious attacks.

3. Myriad types of sabotage could bring international finance to a standstill, cut off diplomatic communications, or threaten energy supplies, as the Nord Stream incidents illustrated. Effects could be similarly damaging for militaries, which is why they must prioritise, among other objectives, knowledge gathering and sharing now that 'seabed warfare' poses a real and immediate threat to Alliance security (Gosselin-Malo, 2022).

4. As the report focuses on current and future technological developments, other aspects, such as international law issues or the question of who is responsible for protecting these CMIs (private operators or state authorities), are dealt with only cursorily or not at all. This report highlights the importance of CMI to NATO countries and, in particular, the challenges the Allies face in protecting this critical infrastructure. It focuses on the work of NATO's Science and Technology Organization (STO) in developing technologies to protect undersea infrastructure.

II- RELEVANCE FOR ALLIED SECURITY

A. WHAT IS CRITICAL MARITIME INFRASTRUCTURE?

5. Critical maritime undersea infrastructure is vital for Allied resilience and security, both in the military and civilian realms. The European Union defines critical infrastructure as "an asset or system which is essential for the maintenance of vital societal functions" (European Commission (a)). Maritime infrastructure that is widely accepted to be 'critical' includes undersea cables for telecommunication and energy transmission. This equipment facilitates 99% of transoceanic digital communications, including phone calls, internet, data transmission, and trillions of international financial transactions daily (Gallagher, 2022).

6. Critical maritime infrastructure includes ports, navigation channels, marine terminals, offshore installations, and related communication systems, and plays a vital role in global supply chains and international trade (European Commission (f), n.d.). Ninety percent of materials and goods are shipped by sea, making seaports an integral part of international trade. Seaports are also crucial for a wide range of military tasks, including prompt and efficient deployment of personnel and military equipment, (re-) supply of deployed forces, and conducting military operations. For example, shipping channels like the Suez, Panama, or Kiel Canal expedite maritime trade and support the strategic mobility of Allied forces.

7. Natural gas pipelines and also offshore gas platforms are a crucial part of maritime infrastructure because they make, or are projected to make, a significant contribution to the energy supply of a number of NATO member states. The Baltic Sea has served as a key hub for such infrastructure, including housing Nord Stream 1 and 2. Additionally, the North Sea is becoming an increasingly important pipeline channel, with the new Baltic Pipe having become fully operational in December 2022. The Black Sea is also an area of particular significance for the energy security of a number of Allies.

8. Moreover, offshore energy farms, such as wind farms, harness clean energy, reduce dependence on fossil fuels and promote energy diversification. For example, offshore wind farms already provide 10% of electricity in Belgium; their contribution to energy production will increase further (Loctier, 2023).

9. Undersea cables underpin vital services, including communications and energy, connecting countries across the globe. These networks are crucial for data storage, energy grids and supplies, and other basic services. Furthermore, critical seabed and undersea infrastructure is directly linked to the wider grid that societies rely on for energy, electricity, and water distribution. The infrastructure systems that comprise this 'grid' are quickly becoming "more complex and more reliant on networks of interconnected devices" (Allianz, 2016). Since the end of the Cold War, both the size of undersea infrastructure networks and civil society's dependence on them have increased exponentially (Salerno-Garthwaite (a), 2022). Fibreoptic cables, for example, carry 99% of digital data globally (Machi (a), 2022).

B. WHY INFRASTRUCTURE PROTECTION SHOULD REMAIN HIGH ON ALLIES' AGENDAS

10. Critical maritime infrastructure such as canals and seaports are vulnerable to disruption, as demonstrated by the closure of the Suez Canal in 2021 (Pivariu, 2023). Ports and their associated shipping operations are challenging to protect. Most ports are large, covering hundreds of hectares of land and sea. They may manage container handling, freight, and cargo movement (solid or liquid), ship, truck and rail traffic, petroleum product/liquid unloading, storage, or pipelines (NATO, CoECSW, 2017). An attack on a seaport could render it inoperable, hampering NATO's ability to transport troops, equipment, and supplies, which could affect its ability to respond to threats or crises. In addition, attacks on seaports could lead to disruptions in trade and commerce that could have regional or even global economic consequences. Indeed, this is Russia's strategy in its war against Ukraine. It is targeting Ukrainian ports on the Black Sea, and lower Danube, in the immediate vicinity of Allied territory, trying to damage Ukraine's maritime infrastructure and destroy its agricultural sector.

11. Maritime natural gas infrastructure strengthens overall energy security through diversification. However, it is vulnerable to physical attacks and natural disasters (Humpert, 2022). In addition, its reliance on complex computerised systems makes it susceptible to cyber-attacks. Offshore wind farms also have vulnerabilities due to their exposed location in the sea, making them easy targets for potential aggressors. It is therefore vital to implement robust security measures to protect them and maintain their uninterrupted operation, thus ensuring the resilience of NATO member states' energy systems.

12. The vital nature of critical maritime infrastructure extends from the provision of basic services to financial transactions to telecommunications. From water distribution to internet access, billions of citizens rely on undersea networks daily. Taking only the financial sector as an example, undersea cables are estimated to carry 10 trillion USD in transfers every day (Wall and Morcos, 2021).

13. In addition to significant commercial implications, critical maritime infrastructure also plays a vital role in transatlantic security. For example, the largest concentration of undersea cables is found in the Atlantic, linking North America and Europe, making their protection a relevant and timely issue

for Allies in particular. The seabed is quickly becoming a hotspot for strategic competition. Significant vulnerabilities in communication and energy infrastructure persist, while increasingly sophisticated capabilities are being developed for exploitation activities in the maritime domain (Machi (a), 2022).

14. While government communications utilising commercially owned undersea cables are typically unclassified, inter- and intragovernmental communication traffic across the Atlantic is immense. Daily communications between embassies, militaries, and other offices depend on these networks (Wall and Morcos, 2021). It is also common for the cables that connect military bases equipped with satellite receiving stations to be located under the seabed (Bueger, 2022).

15. Data storage, an increasingly important issue for states and their citizens, also relies on undersea systems. This is particularly important for European Allies, as the majority of Europe's data is stored in US centres (Wall and Morcos, 2021). Furthermore, current dependency on undersea cables is expected to increase over time as demand for both data storage and bandwidth continues to grow rapidly (Wall and Morcos, 2021).

16. In case of attack or sabotage, Allies could face significant repercussions. In a study by the Center for International Security Studies (CSIS), analysts lay out possible scenarios following an undersea incident: "*There are several conceivable objectives severing a cable might achieve: cutting off military or government communications in the early stages of a conflict, eliminating internet access for a targeted population, sabotaging an economic competitor, or causing economic disruption for geopolitical purposes"* (Wall and Morcos, 2021). The authors also rightfully point out that a combination of these tactics could be used simultaneously. Furthermore, negative repercussions from undersea espionage and manipulation would likely engender similar damage for Allies.

17. Enhancing capabilities for the seabed is also necessary for protecting industrial and governmental secrets. Undersea cables play a crucial role for internet traffic and in the transmission of large amounts of data, including sensitive or classified information. It is therefore important to improve the resilience of these communication channels and protect undersea cables against threats such as hacking or sabotage. Moreover, in case of sinkage, crashes, or technical failures, valuable equipment must be searched for and retrieved, sometimes from great depths, or else sensitive technology may fall into adversarial hands (Machi (a), 2022). For this reason, experts consider advanced undersea capabilities to be "not only a technical issue, but also a strategic one" (Machi (a), 2022).

18. Not surprisingly, maritime experts assert that seabed security concerns present an already significant threat that requires immediate defensive action (Salerno-Garthwaite (a), 2022). Therefore, it is vitally important that Allies increase intelligence, surveillance, and reconnaissance (ISR) in the maritime domain. These activities will be crucial for enabling vehicle tracking, threat detection, communication, and broader strategic planning and awareness (Gosselin-Malo, 2022).

19. The work of NATO's Maritime Unmanned Systems Innovation Advisory Board and the new Critical Undersea Infrastructure Coordination Cell (CUICC) at NATO Headquarters, established in early 2023, demonstrate the growing importance of CMI protection to the Alliance (NATO (a), 2023). The aim of the CUICC is to reduce the risk of attacks on critical maritime infrastructure by using NATO's military, intelligence and planning capabilities to identify and promote cooperation between all stakeholders (Willet, 2023; Heise, 2023). Rather than relying solely on aircraft and ships to monitor the sea, the aim is to increase sensor density to the point where any potential attacker would be detected when targeting the infrastructure (Defense Aerospace, 2023). Additionally, national efforts by, for example France, the UK, and US, mentioned in more detail below, illustrate how protecting critical maritime infrastructure has become a topic of increased interest. However, substantial vulnerabilities in Allies' networks remain as threats in this domain increase; therefore, additional and persistent effort will be required to secure these vital systems.

III- MAIN THREATS TO CRITICAL MARITIME INFRASTRUCTURE

20. A 2017 report on the security of commercial undersea telecommunication cables commissioned and published by the US Office of the Director of National Intelligence (ODNI) found that there are “few disruptions of cables in proportion to their heavy presence and use”; however, it noted that risks were already increasing before 2017, due to “heavy reliance on undersea cables, increasing volume of data transmitted through undersea cables, and technological improvements to cable systems that have created new vulnerabilities” (Gallagher, 2022). These challenges are even more pressing today.

21. In addition to the damaging environmental effects of gas leaks, the recent Nord Stream pipeline incidents underscored the persistent vulnerability of Allies’ undersea infrastructure. However, the sabotage of gas delivery systems merely represents one of many ways that Allies’ critical maritime infrastructure can be targeted. Although the investigation is still ongoing at the time of writing, the September 2022 incident was a sophisticated operation, which, according to newspaper reports, likely involved experienced divers who were able to plant explosive devices on the Baltic Sea floor while evading detection (Entous et al., 2023). Allied infrastructure remains vulnerable to similar acts of sabotage, damage, and espionage carried out by manned or unmanned underwater vehicles, and accidental damage from commercial activities and extreme weather events.

22. The September 2022 sabotage is not the only recent incident of deliberate damage or manipulation of Allied critical maritime infrastructure. In Norway alone, an undersea cable that connected a satellite ground station on the island of Svalbard in the Arctic Ocean to the Norwegian mainland was severed in January 2022, which government officials believe was the result of human action (Humpert, 2022). More recently, in February 2023, military intelligence officials in the Netherlands issued a warning indicating that Russia had begun “espionage” activities and appeared to be “preparing operations for disturbance and sabotage” of underwater cables in the North Sea, in addition to wind farms and gas pipelines (Hancock and Sheppard, 2023). These incidents and others illustrate that Allies’ infrastructure remains vulnerable to attacks, and that attributing malicious actions on and under the seafloor remains extremely difficult (Machi (a), 2022).

23. As is true for many other security threats for Allies, climate change is a threat multiplier in the maritime domain, including with critical infrastructure. Cable landing stations, for example, need to be better protected against extreme weather events, as they connect undersea cables to land-based networks and are therefore more exposed than subsea equipment.

A. DEFINING THE THREAT

24. There are two primary forms of likely physical attack on undersea infrastructure, each of which involves unique threats relevant to Allies. The first is a traditional physical attack, such as explosions or severing of cables, which may be carried out by a state or non-state actor, caused unintentionally by commercial activities such as shipping and fishing, or by extreme weather or earthquakes. In the case of accidental damage, private entities bear the primary responsibility for mitigating these threats (Wall and Morcos, 2021). In the case of a malicious attack, an adversary may use surface vessels and/or submarines to deploy manned or unmanned equipment capable of disrupting or destroying undersea cables or pipelines.

25. The second form of likely physical attack is tapping undersea cables for espionage purposes, including recording, copying, and stealing sensitive data, which would likely require similar manned or unmanned capabilities (Wall and Morcos, 2021). The likelihood of physical damage and/or tapping using such equipment has increased rapidly in recent years, due to the proliferation of subsea technology.

26. According to a recent study published by the European Parliament (EP), submersible technology is increasingly widespread and available to a wide range of actors. The 2022 report notes that “such technology is not only available to high capability naval forces”, as there have been recent instances of criminal organisations implementing submersible assets in smuggling operations (Bueger et al., 2022). This equipment can easily be repurposed to place mines and explosive devices on or under the seafloor. The report also highlights the ability of malicious actors to “employ higher-end technologies, such as self-propelled underwater weapons (torpedoes) and prospectively chemical or laser weapons” (Bueger et al., 2022).

27. Critical maritime infrastructure not only has physical vulnerabilities, but digital ones as well, since an adversary can cause equally significant damage via offensive cyber operations. For example, data and communication networks can be manipulated, disrupted, or even partially destroyed in the cyber domain. Moreover, cybersecurity incidents targeting energy and commodities infrastructure are rapidly increasing (Graphus, 2022).

28. Not only can these activities cause catastrophic damage, but they remain very difficult to detect. Some high-tech capabilities include clusters of autonomous weapons that lay on the ocean floor until activated, which can then become “movable mine fields” that are difficult to notice until after damage has occurred (C4ISRnet, 2023). Identifying equipment, especially submersible equipment, requires “sophisticated underwater surveillance infrastructure across the entire length of cables” (Bueger et al., 2022). This necessitates monitoring what happens on and under the seabed with a complex network of advanced sensors across an area so vast that it is nearly impossible to observe all activities at the scale needed (C4ISRnet, 2023). The fact that threats to critical maritime infrastructure can be physical and digital further complicates monitoring, detection, and attribution, as these are notoriously difficult aims in the cyber domain as well. The growing threat of cyber-attacks against maritime infrastructure is being increasingly recognised. This is reflected, among other things, in the launch of the Maritime Cyber Attack Database (MCAD) at NHL Stenden University of Applied Sciences in the Netherlands, a database of incidents affecting the global maritime sector (O’Dwyer, 2023).

B. Challenges to Safeguarding Critical Maritime Infrastructure

1. Potential for Malicious Action

29. Allies face threats to critical maritime infrastructure from a variety of actors, most notably Russia. Experts consider Russia to be one of, if not, the most capable nation of conducting malicious undersea operations, and it has a motive to conduct such operations given the Russian Federation’s stated aims to undermine Allies’ security. According to David Cattler, NATO's Assistant Secretary General for Intelligence and Security, "Allied critical infrastructure could be targeted by Russia as part of its war against Ukraine or in any future conflict. Russia is actively monitoring Allied critical infrastructure, recognising that the ability to compromise the security of energy, information and financial systems provides a significant strategic advantage” (Willet (b), 2023).

30. Russia possesses capabilities in each threat category discussed: physical attack, tapping, and cyber operations. Its seabed operations can include cutting off vital undersea supply channels, laying sensors for espionage and tracking purposes, conducting cyber-attacks that directly affect infrastructure above and below the seabed, and mapping Allies’ infrastructure for future sabotage. Several factors make Russia a threat to Allied CMI. First, Russia uses hybrid warfare to exploit weaknesses. Russia's proximity to critical maritime areas like the Arctic and Black Sea gives it strategic advantages. Russia is able to execute covert operations with plausible deniability thanks to its excellent cyber and intelligence capabilities. These features make it hard for NATO to identify and link attacks to Russia, hampering response and countermeasures.

31. Currently, Russia is repairing its Losharik spy submarine, renowned for its unique offensive and surveillance capabilities, which is expected to be completed in 2024 (Navy Recognition, 2023). According to Russian media reports, the country has successfully produced its first autonomous,

nuclear-powered unmanned underwater vehicle (UUV) that can supposedly deliver a nuclear bomb, in January 2023, known as “Poseidon”. It can be fired from a nuclear submarine and is essentially a hybrid of a torpedo and a drone. It is purportedly designed to avoid adversary detection and pursue targets at considerable depths and distances. The “Poseidon” is part of a project first announced in 2018 (Saballa, 2023).

32. Iran’s activities have the potential to pose a threat to Allied critical maritime infrastructure. Some recent developments illustrate the potential for aggressive maritime action by Iran. For example, in August 2022, the Islamic Revolutionary Guard Corps Navy tried to capture a USV Saildrone Explorer belonging to the US 5th Fleet in the Persian Gulf (Gosselin-Malo, 2022). A few days later, the Islamic Republic of Iran Navy removed American USVs from the Red Sea (Shelbourne, 2022), and initially denied having captured the vessels (Stewart, 2022). The vessels were eventually recovered by US forces without incident (The Guardian, 2022). Nevertheless, these occurrences reflect Iran’s potential for aggressive behaviour in the maritime domain, especially as Iran continues to increase its naval presence in the region, particularly in the Red Sea near Yemen (The Guardian, 2022).

33. Although China continues to act aggressively in the South China Sea and is boosting its presence in the Arctic (Irving, 2022), its activities do not appear to pose a direct threat to Allied critical maritime infrastructure at this time. However, in 2020, the US Department of Justice (DOJ) issued a statement raising safety concerns over cables connecting the US and China, which cited “the current national security environment, including the PRC government’s sustained efforts to acquire the sensitive data of millions of U.S. persons” as reason to refuse cable licensing (DOJ, 2020). China continues to develop its capabilities and expertise in the maritime domain, including undersea. Additionally, it is noteworthy that China holds more deep-sea mining contracts than any other nation and is leading the race to mine the deep sea for scarce and valuable materials such as rare earth minerals (Machi (a), 2022). Furthermore, China’s leaders remain keen to control global digital technology infrastructure and continue to use national companies to achieve political and economic gains in this space (Bueger, 2022).

34. Despite the *potential* for malicious action by certain states, maritime trade remains the dominant method of economic exchange between global actors. Therefore, even countries which are potential competitors of NATO have an interest in maintaining secure international trade routes. Secure maritime routes are particularly relevant for China, as the vast majority of its foreign trade is conducted via ships (Jie and Wallace, 2021).

35. In addition to threats from state actors, it is likely that threats from non-state actors will increase over time, particularly as submersible technology capable of threatening critical infrastructure becomes more widely available.

2. Governance

36. One of the key obstacles to safeguarding critical maritime infrastructure is determining who controls what equipment as well as fostering public-private cooperation concerning protection, repair, and regulatory frameworks, because much of this infrastructure is owned or controlled by the private sector. In Europe, 80% of critical infrastructure assets are owned by private entities, which complicates the role of national governments in protecting this vital equipment (Umbach, 2023). In addition to issues of private ownership, the sheer vastness of the area covered by this equipment that connects numerous countries further complicates the governance of these essential communication, energy, and finance networks (C4ISRNET, 2023).

3. Logistics

37. From an operational-logistical point of view, the massive area that must be protected, the depth at which some operations must be completed, and persistent technological challenges all present obstacles with regard to ensuring the safety of maritime infrastructure. For example, regarding

navigation, the primary method used by militaries and civilians known as GPS or the “Global Positioning System”, cannot be used underwater since it depends on radio frequencies. Undersea navigation therefore necessitates the use of innovative technologies such as advanced sensors.

IV- TECHNOLOGY’S ROLE IN PROTECTING CRITICAL MARITIME INFRASTRUCTURE

38. As with many domains and applications, technology enables greater defence capabilities for Allies while also representing a threat to their security if used for malicious aims by adversaries. Therefore, it is necessary for Allies to further develop defensive capabilities to protect against growing threats and vulnerabilities in the maritime domain, including by incorporating advanced technologies as part of this effort.

A. KEY TECHNOLOGIES FOR CRITICAL MARITIME INFRASTRUCTURE PROTECTION

1. Sensors

39. Sensors are among the most important technologies for protecting critical maritime infrastructure, as they provide the primary method for identifying, monitoring, and intercepting existing and potential threats. The term "sensors" encompasses a wide range of devices, both acoustic and non-acoustic, with some of the most complex versions being devices that detect biological agents or provide all-weather imaging systems (National Research Council, 1997). Sensor technologies are “constantly evolving. According to BAE Systems current and potential applications for this technology include:

- High-power, wide-band, efficient low-frequency acoustic transducers
- Novel applications of undersea technologies to evolving Navy missions
- Low size, weight, and power open-architecture unmanned undersea vehicle payloads
- Undersea positioning systems
- Underwater acoustic communications
- Algorithms for underwater target detection, classification, localization and tracking
- High-frequency hardware technology and processing[1]

40. Advanced sonar systems, sensors, autonomous systems, and broader ranging/deeper-sea capabilities will become increasingly important in the maritime domain as Allies work to protect critical infrastructure. RAND Corporation experts highlight mine countermeasures, denied-area intelligence, surveillance, and reconnaissance (ISR), and operational deception as areas in which autonomous capabilities can add significant value to maritime operations (Martin, et al., 2019). Autonomous systems are also likely to become more integrated into anti-submarine warfare, intelligence collection, and operational deception (STO, 2020).

41. Regarding the use of sensors, which are vital for maintaining situational awareness underwater and undersea, quantum sensors and magnetic and gravity sensing are expected to be used in the maritime domain in the future. Quantum sensors are more sensitive than currently used systems and potentially more resistant to jamming by adversaries, and “will support the development of counter-stealth and covert radars” (STO, 2020). Magnetic and gravity sensing can be used by aerial patrol aircraft to determine the precise location of, for example, submarines or underground

[1] *Source :* BAE Systems

structures. These technologies are especially useful when combined with UAVs, as current sensor systems suffer from “size-weight-power constraints” (STO, 2020).

42. Sonar capabilities are also advancing. For example, Thales Group recently illustrated that advanced sonar systems can be applied on a ship in just 48 hours (Weisgerber, 2023). This technology has already been deployed on British, French, and Spanish ships, and the US plans to apply similar systems (Weisgerber, 2023). Sonar technology are also being used together with advanced sensor capabilities, for example in the new intruder detection or “passive listening” system announced by the British company Forcys in January 2023 (Salerno-Garthwaite (b), 2023).

2. Autonomous Systems

43. Autonomous systems represent another vital aspect of utilising technology to safeguard critical maritime infrastructure. These systems include unmanned surface vehicles (USVs) and autonomous surface vehicles (ASVs), which are typically equipped with radars, cameras, and other equipment used for monitoring underwater activities. These systems are now a common and vital aspect of a wide range of maritime activities, especially conducting surveillance and maintaining situational awareness. According to the Thales Group, additional uses for unmanned maritime systems include:

- Mine warfare
- Maritime surveillance
- Anti-submarine warfare
- Communication nodes
- Early warning
- Rapid response
- Search and rescue [2]

3. Additional Technologies

44. In addition to the technologies mentioned above, including additional applications of AI in the maritime domain (for example, for sifting through large amounts of data collected from surveillance devices), the following areas will become increasingly important in the protection of critical maritime infrastructure: Advanced materials, augmented reality, big data, robotics, smarter ship propulsion, and 3D printing (Menon, 2021).

B. Alliance Efforts to Safeguard Critical Maritime Infrastructure and Enable Technological Solutions

1. NATO Initiatives

45. Following the Nord Stream pipelines sabotage, “NATO and Allies increased their patrolling presence in the North and Baltic Seas and stepped up intelligence sharing” as part of a broader effort to enhance joint efforts to protect undersea infrastructure (MARCOM, 2023). This has included utilising NATO as a channel for increasing coordination between Maritime Patrol Aircraft and Unmanned Aerial Vehicles from the High North to the eastern Mediterranean (MARCOM, 2023).

46. When it comes to collective maritime security efforts, NATO’s Allied Maritime Command (MARCOM) in Northwood, UK plays an essential role in ensuring the safety of Allies’ critical infrastructure. One of NATO’s key initiatives in this area is Operation Sea Guardian, a maritime security operation focused on situational awareness, counterterrorism, and capacity building, among other tasks. The operation is vital for Allied maritime security and information sharing as it provides a comprehensive picture of what occurs in the Mediterranean on a daily basis.

---

[2] *Source: Thales Group*

47. As Allies seek to integrate new and emerging technologies into their maritime forces, NATO's Science and Technology Organization will likely play a larger role in future NATO efforts to apply innovative, science- and technology-driven solutions to existing maritime capability gaps. The STO will be pivotal for the coordination of future activities on the research and development of disruptive technologies relevant for improving Allies' capabilities in this area. The STO's Centre for Maritime Research and Experimentation (STO CMRE) in La Spezia, Italy, conducts valuable research and experimentation at sea, enabling scientifically tested solutions to be applied to persistent gaps in Allies' maritime capabilities.

48. The new CUICC at NATO Headquarters was established in recognition of the vulnerabilities of Allied CMI. The CUICC will "facilitate engagement with industry and bring key military and civilian stakeholders together" as well as share best practices, leverage innovative technologies, and boost the security of Allied undersea infrastructure, according to Secretary General Jens Stoltenberg (NATO (a), 2023). Moreover, at the Vilnius Summit Allied Heads of State and Government agreed to establish NATO's Maritime Centre for the Security of Critical Undersea Infrastructure within NATO's Maritime Command (MARCOM). These efforts reflect a growing understanding of the importance of critical maritime infrastructure and existing vulnerabilities within the Alliance. This is expressed in the Communique issued by NATO Heads of State and Government at the end of the Vilnius Summit which notes that Allies will "work towards identifying and mitigating strategic vulnerabilities and dependencies, including with respect to our critical infrastructure, supply chains and health systems" and "to set up a network that brings together NATO, Allies, private sector, and other relevant actors to improve information sharing and exchange best practice" (NATO (d), 2023).

2. Allies' Initiatives

49. Different approaches to CMI protection can be observed among NATO members. The French Navy published a new strategic doctrine on seabed warfare in February 2022 (France, 2022; Salerno-Garthwaite (a), 2022). The doctrine states that "autonomous and remotely operated drones are at the heart of France's ambitions to further explore and exploit the deep-sea waters under a new seabed strategy" (Machi (a), 2022). "The goal of the new strategy is to equip the French military with the ability to reach depths of 6,000 meters, or nearly 20,000 feet", said then-Minister of Defence Florence Parly in a press conference. "This makes it possible to cover 97 percent of the seabed and effectively protect our interests, including sub-marine cables," she said. (Machi (a), 2022). By 2023, the military should have developed one AUV and one ROV to serve as initial surveillance assets and be used for testing and assessment purposes. A larger program is expected to be launched by 2025, Chief of the General Staff, General Burkhard said. (Machi (a), 2022). The French government has also invested in contracts for developing additional Unmanned Aerial Systems, such as the Airbus VSR700, in recent years (Naval Technology (a), 2022), and by 2030, the French Navy aims to have 1,200 Unmanned Systems (Gain, 2019). Regarding countermine capabilities, France also joined a Belgian-Dutch initiative in October 2022 (Machi (b), 2022).

50. The UK Ministry of Defence announced in November 2022 that it would prioritise procuring two Multi-Role Ocean Surveillance (MROs) ships (Salerno-Garthwaite (a), 2022), and the first ship entered the Royal Navy's fleet in January 2023 (Naval Technology (b), 2023). The MROS ships will bring deep-diving operations back into the mission set of the Royal Navy's Hydrographic squadron, building on the capabilities of its multiple surveillance ships. Its inclusion in the Royal Fleet Auxiliary is intended to advance British security by monitoring and protecting seabed communications cables and energy pipelines, and the ships are expected to carry Autonomous Underwater Vessels (AUV) for this purpose. In December 2022, the Royal Navy revealed that it had placed order for its first uncrewed submarine, which will monitor activities that could threaten critical infrastructure, including deep-sea cables and pipelines (Salerno-Garthwaite (a), 2022) and drone-teaming will also be part of this effort (Chuter (b), 2022). The UK also reportedly plans to acquire a deep-water remotely operated vehicle in the near future (Chuter (a), 2022). In May 2023, the United Kingdom and Norway signed a security partnership to prevent attacks against undersea infrastructure including gas

pipeline and cables. The agreement foresees intelligence exchange, and cooperation on counter mine threats and hostile submarine detection (Gallardo, 2023).

51. In the US, the Defense Advanced Research Projects Agency (DARPA) has been developing a system for deep-sea navigation, called the Positioning System for Deep Ocean Navigation (POSYDON), which was first announced in 2015 (Keller, 2015). This system resolves the problem of GPS ineffectiveness by using a combination of long-range acoustic signals to navigate and surveil as well as to identify mines and submarines (DSIAC, 2017). The US has also made more recent strides in developing its maritime capabilities, including unmanned capabilities for air, surface, and sub-surface operations (Armada International, 2022). In January 2022, the US Naval Forces Central Command tested the Explorer, a 23-foot-long solar- and wind-powered system, for the first time (Gosselin-Malo, 2022). This is part of a broader US effort to scale up USV presence in the Middle East (Eckstein, 2022), as part of Task Force 59, which aims to boost unmanned and AI tools, creating an "integrated network of sensors and unmanned systems" capable of flagging unusual activity or a "digital ocean" (Vincent, 2023). The first-ever unmanned surface fleet is expected by summer 2023 (Ziezulewicz, 2023).

3. Partner Initiatives

52. Even before the Nord Stream 2 attacks, the European Union (EU) had demonstrated a strong commitment to protecting critical maritime infrastructure. In June 2022, the European Parliament published a report titled *"Security threats to undersea communications cables and infrastructure consequences for the EU"*, which points out the importance of technology for protecting undersea networks. It also notes that some of the necessary technology is already in place, but lack of coordination and mandate complicates further protection and surveillance of cables (Bueger, 2022).

53. In October 2022, the European Commission published a 5-point plan to improve critical maritime infrastructure and pledged to increase the protection of undersea internet cables (Kabelka, 2022). In March 2023, the Commission updated the EU Maritime Security Strategy and related Action Plan, to enhance the strategy in light of evolving maritime threats. The updated strategy underscores the vital need to implement innovative technologies into the EU response to underwater threats (European Commission (b), 2023) and to "develop common requirements for defence technologies in the maritime domain" (European Commission, (c), 2023).

54. The EU and NATO also directly cooperate on maritime-related issues. For example, NATO has supported EU efforts in the Aegean Sea to address the ongoing refugee and migrant crisis. NATO also provides ISR to the EU's Border and Coast Guard Agency, FRONTEX (NATO (b), 2022).

55. Additionally, on 16 March 2023, the new NATO-EU Task Force on Resilience of Critical Infrastructure was launched, which aims to strengthen the resilience and protection of critical infrastructure by stepping up existing cooperation in the following areas: energy, digital infrastructure, transport, and space. Although the task force is not limited to the maritime domain, the statement announcing its launch notes the "heightened attention" on infrastructure protection following the Nord Stream 2 attacks (European Commission (d), 2023).

56. NATO also cooperates with individual partners to enhance maritime capabilities, including through increasing interoperability and preparedness for a wide range of operations. Exercises, such as the one conducted between NATO and Japan's Maritime Self-Defense Force vessels in June 2022, are essential to this cooperation. Partners also provide direct contributions to ongoing NATO operations (NATO (b), 2023). For example, Australia contributed a maritime patrol aircraft to Operation Sea Guardian in October 2022 (NATO (c), 2022).

57. Many ongoing efforts to protect critical maritime infrastructure are also made possible by partnerships with industry. For example, the development of the SeaSpider anti-torpedo torpedo, is a joint effort by Canadian and German firms that began in 2019 and is expected to be completed in

2023 (Eshel, 2022). American and Norwegian companies are also currently coordinating on the development of underwater drones (Peck, 2016).

V- CONCLUSIONS

58. Critical maritime infrastructure is both likely to become increasingly important for essential services and activities and more exposed to malicious action as advancing technologies create new vulnerabilities or fall into the hands of adversaries. Therefore, building awareness of how maritime infrastructure networks enable vital daily activities and how Allies can increase the protection of these networks through national, bilateral, and multilateral cooperation is paramount. Since maritime infrastructure nodes connect numerous countries simultaneously, increasing coordination and sharing data, intelligence, national risk assessments, incident reports, and best practices using existing fora is essential.

59. NATO plays a vital role in safeguarding maritime infrastructure, as many Allies rely heavily on the Alliance for monitoring and protection, especially in areas like the Baltic Sea that serve as a hub for critical maritime infrastructure in a key geostrategic region. However, Allies must look to partners outside NATO as well. Work with partners, including private sector actors, will be crucial for increasing the resilience and protection of critical maritime infrastructure. Likewise, coordination with the EU, including via the new NATO-EU Task Force on Resilience of Critical Infrastructure, will be instrumental for building redundancies into existing systems, contingency planning in case of interference or damage to infrastructure, and promoting protection standards.

60. Given that much of critical maritime infrastructure is owned or operated by private entities, Allies should also seek to deepen cooperation and dialogue with the private sector. Fora such as the NATO Maritime Unmanned Systems (MUS) Innovation Advisory Board and the Critical Undersea Infrastructure Coordination Cell should therefore be utilised to the fullest extent possible to improve public-private coordination. Moreover, they can be used to encourage the development and implementation of technological solutions that can close existing maritime capability gaps. Industry actors are already finding innovative ways to respond to threats, particularly after the Nord Stream incidents. Allies should utilise similarly creative thinking and harmonise efforts with industry as much as possible.

61. Furthermore, new technologies can provide cost-effective ways for Allies to improve maritime capabilities, including for those nations that are not historical maritime powers. The US Navy's Task Force 59 has illustrated how unmanned vehicles used in combination with AI tools can improve coastal security in an affordable manner for NATO partners such as Israel, Jordan, and the UAE (Eckstein, 2022). These lessons can be applied elsewhere by relying on technology to monitor maritime activity, identify patterns, and increase situational awareness without requiring frigates or manned patrol vehicles.

62. Critical maritime infrastructure has facilitated communications, financial transactions, energy transmission, and numerous other essential daily activities across the globe for decades. Societies' reliance on these systems as well as vulnerabilities within existing infrastructure networks have also increased dramatically over time. Hence, the rationale for prioritising the protection of critical maritime infrastructure existed well before the Nord Stream sabotage of September 2022. However, these incidents served as an alarm bell for citizens, governments, and industry. It is now crucial that new and heightened awareness regarding infrastructure vulnerabilities be followed by concrete steps to protect Allies and the equipment and networks their citizens, militaries, and policymakers rely on in the maritime domain.

BIBLIOGRAPHY

Allianz, "Cyber Attacks on Critical Infrastructure", June 2016.

BAE Systems, "Maritime Sensing: Supporting Naval Strategies for Countering Adversarial Capabilities".

Bueger, Christian, Liebetrau, Tobias, and Franken, Jonas, "Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU", European Parliament, June 2022.

C4ISRNET, "Europeans Wade Into Fighting Seabed Threats with Drones and Sensors", 9 January 2023.

Chuter, Andrew:

(a), "UK Military Ups Investments in Undersea Surveillance", Defense News, 16 November 2022.

(b), "UK Navy to Take Drone-Teaming Operations Underwater with New Submarine", Defense News, 1 December 2022.

Cooper, Charlie, "Russia 'Mapping' Critical Energy Infrastructure, Say Dutch Intelligence Agencies", Politico, 20 February 2023.

Council on Foreign Relations, Territorial Disputes in the South China Sea, 4 May 2022.

Eshel, Tamir, "Sea Spider to Protect Surface Vessels from Submarine's Attacks", Defense Update, 19 October 2022.

Defense Aerospace, "European Ex-General Leads NATO Cell to Protect Underwater Infrastructure", 09 May, 2023.

Defense Systems Information Analysis Center (DSIAC), "POSYDON: DARPA Working to Develop Robust Undersea Navigation System", 13 March 2017.

Eckstein, Megan, "Navy Boosting USV Presence, Network Capability in Middle East", Defense News, 13 October 2022.

Entous, Adam, Barnes, Julian E., and Goldman, Goldman, "Intelligence Suggests Pro-Ukrainian Group Sabotaged Pipelines, U.S. Officials Say", The New York Times, 7 March 2023.

European Commission:

(a), "Migration and Home Affairs: Critical Infrastructure, European Commission".

(b), "Joint Communication to the European Parliament and the Council", 10 March 2023.

(c), "Maritime Security Strategy", 2023.

(d), "Launch of The EU-NATO Task Force: Strengthening Our Resilience and Protection of Critical Infrastructure", 16 March 2023.

France, Ministère des Armées, Seabed Warfare Strategy, February 2022.

Gain, Nathan, "French Navy Aiming For 1200 Unmanned Systems By 2030", 29 July 2019.

Gallagher, Jill C., "Undersea Telecommunication Cables: Technology Overview and Issues for Congress", Congressional Research Service, 13 September 2022.

Gallardo, Cristina, "UK and Norway team up to protect undersea cables, gas pipes, in wake of Nord Stream attacks", Politico, 18 May 2023.

Gosselin-Malo, Elisabeth, "Saildrone USVs to Expand Seabed Mapping in Atlantic, Pacific", C4ISRNET, 9 November 2022.

Graphus, "Cyberattacks on Critical Infrastructure Are Surging", 18 November 2022.

Hancock, Alice, and Sheppard, David, "Netherlands Warns of Russian Attempts to Sabotage Its Energy Infrastructure", Financial Times, 20 February 2023.

Heise, Rene, Office of the Secretary General, Private Office, Critical Undersea Infrastructure Coordination Cell, Interview on August 7, 2023

Humpert, Malte, "Nord Stream Pipeline Sabotage Mirrors Svalbard Cable Incident",
High North News, 29 September 2022.

Irving, Doug, What Does China's Arctic Presence Mean to the United States?, RAND Corporation, 29 December 2022.

Jie, Dr Yu, Wallace, Jon, "What is China's Belt and Road Initiative (BRI)?", Chatham House, 13 September 2021.

Kabelka, Laura, "EU Aims to Tackle Threats to Submarine Data Cables", Euractiv, 6 October 2022.

Keller, John, "DARPA approaches industry for new kinds of underwater navigation for undersea drones and submarines", Military & Aerospace Electronics, 24 April 2015.
Loctier, Denis, "A wake-up call: How to protect Europe's vital marine infrastructure from emerging threats?" Euronews, 30 May 2023.
Machi, Vivienne:
(a), "French Military Tees Up New Tech in Rush to Conquer the Seabed", Defense News 14 February 2022.
(b), Vivienne, "France, Belgium, Netherlands Team Up on Mining Countermeasures", 19 October 2022.
MARCOM, "NATO Maritime Assets Play Key Role in Offshore Critical Infrastructure Security", 14 February 2023.
Martin, Bradley, Tarraf, Danielle C., Whitmore, Thomas C., DeWeese, Jacob, Kenney, Cedric, Schmid, Jon, DeLuca, Paul, "Advancing Autonomous Systems: An Analysis of Current and Future Technology for Unmanned Maritime Vehicles", RAND Corporation, 2019.
Menon, Ajay, "10 Smart Ship Technologies For The Maritime Industry", Marine Insight, 18 June 2021.
National Research Council, "Technology for the United States Navy and Marine Corps, 2000-2035: Becoming a 21st-Century Force: Volume 2: Technology", The National Academies Press, 1997.
NATO:
(a), "NATO Stands Up Undersea Infrastructure Coordination Cell", 15 February 2023.
(b), "The Secretary General's Annual Report 2022", 21 March 2023.
(c), "NATO Allies and Partners Discuss Maritime Security", 21 November 2022.
(d), "Vilnius Summit Communique", 19 July 2023.
NATO, Centre of Excellence for Operations in Shallow and Confined Waters - CoECSW, "The Role and Relevance of the Maritime Domain in an Urban-Centric Operational Environment", September 2017.
Navy Recognition, "Russia AS-31 Nuclear Submarine Losharik to Be Ready in 2024", 10 January 2023.
Naval Technology:
(a), "Airbus VSR700 Unmanned Aerial System (UAS), France", 20 April 2022.
(b), "British Navy's First Future MROS Ship Arrives in UK", 20 January 2023.
O'Dwyer, Rob, Maritime Cyber Attack Database launched, Smart Maritime Network, 16 July 2023
Peck, Michael, "Underwater Drone Makers Team Up", 30 September 2016.
Pivariu, Corneliu, "The Suez Canal Incident: Lessons Learned for the Geopolitics of Critical Infrastructure", IENE. 23 March 2023.
Saballa, Joe, "Russia Produces First Poseidon Nuclear-Powered Torpedoes: Report", The Defense Post, 18 January 2023.
Salerno-Garthwaite, Andrew:
(a), "Seabed Warfare Is a 'Real And Present Threat'", Global Defence Technology, December 2022.
(b), "Intruder Defence 'Passive Listening' Saves Lives in Seabed Warfare", Naval Technology, 18 January 2023.
Shelbourne, Mallory, "Iran Temporarily Captures Two U.S. Saildrones in Red Sea", United States Naval Institute, 2 September 2022.
Stewart, Phil, "Iran Initially Denied Having Seized U.S. Sea Drones, U.S. Official Says", Reuters, 2 September 2022.
STO (NATO Science and Technology Organization), "Science & Technology Trends 2020-2040: Exploring the S&T Edge", March 2020.
Thales Group, "Unmanned Maritime Systems".
The Guardian, "Iran Forced to Return US Sail Drones Seized at Sea for Second Time", 2 September 2022.
Umbach, Frank, "New Challenges in Protecting Critical EU Infrastructure", GIS, 6 February 2023.

United States Department of Justice (DOJ), "Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States", 17 June 2020.
Vincent, Brandi, "Navy's Task Force 59 Reaches Full Operational Capability as It Works to Build a 'Digital Ocean' of Connected Assets", DefenseScoop, 10 January 2023.
Wall, Colin, and Morcos, Pierre, "Invisible and Vital: Undersea Cables and Transatlantic Security", Center for Strategic and International Studies, 11 June 2021.
Weisgerber, Marcus, "New Sonar For Navy Frigates Could Turn Any Ship into Submarine Hunter, Maker Says", Defense One, 13 January 2023.
Willett, Lee:
(a), "CNO Sets Out Timeframe and Headmarks for Delivering Uncrewed Capability", Armada International, 23 January 2023.
(b), "NATO Steps Up Response To Clear and Present Undersea Infrastructure Risk", 16 May 2023.
Ziezulewicz, Geoff, "New in 2023: Here Comes the First-Ever Surface Drone Fleet", C4ISRNET, 4 January 2023.