HYBRID FRONTLINES:

Russian Threats and the Future of Maritime Infrastructure in the Black Sea and the North Sea

AUTHORS:

Dr. Jakub Godzimirski, Research Professor,
Norwegian Institute of International Affairs

Sergiu Mitrescu, Program Director,
New Strategy Center

NEW STRATEGY CENTER

NUPI Norwegian Institute of International Affairs

Dr. Jakub GODZIMIRSKI is a Research Professor at NUPI. He has been working on Russian foreign and security policy issues for more than 20 years, paying special attention to the role of energy resources in Russian grand strategy. In addition, he also has worked on European policy and its impact on developments in Central and Eastern Europe, including relations with Russia.

Sergiu MITRESCU is the Program Director of New Strategy Center and a senior expert on hybrid threats and maritime security, with a particular focus on critical maritime infrastructure. His work centres around the intersection of hybrid threats and maritime security, focusing on Black Sea dynamics.

Editor: **George SCUTARU**, Chief Executive Officer, New Strategy Center

The development of this policy paper benefited from the careful documentation work carried out during its preparation, with particular support from Dilara Kalliloglu, Ion Cristea and Răzvan Ceuca, whose contributions proved essential at key stages of the research process.

The study is published under the Strategic Initiative for Defending Critical Maritime Infrastructure (SIDMI) project financed through the Romania Norway Bilateral Fund 2014-2021, financing contract 17369/26.04.2024.

Disclaimer: This text contains the personal opinions and perspective of the authors and does not necessarily reflect the views of the New Strategy Center or the Norwegian Institute of International Affairs

Cover Photo: @starline, Free

Hybrid Frontlines: Russian Threats and the Future of Maritime Infrastructure in the Black Sea and the North Sea

1. Introduction

Critical Maritime Infrastructure (CMI) has emerged as a focal point in the intensifying competition within the maritime domain. The interconnected maritime areas of the North Sea, Baltic Sea, and Black Sea form a strategic continuum of insecurity, which the Russian Federation views as a single front in its geopolitical calculations. Incidents in the Baltic Sea, such as attacks on undersea pipelines and communication cables, have underscored the growing complexity of maritime security threats. These incidents are often shrouded in ambiguity, making attribution difficult and allowing such actions to be disguised as accidents, thereby reinforcing the concept of plausible deniability.

In this context, the Black Sea stands as a critical arena where geopolitical, economic, and security interests converge. Its status as a hub for vital energy resources, global data transmission, and emerging renewable and non-renewable energy projects makes it increasingly vulnerable to hybrid threats. The region's complex security landscape, marked by the overlapping interests of NATO, the European Union, and Russia, has heightened its strategic importance. The growing militarization and geopolitical rivalry in the Black Sea amplify the stakes, turning CMI into both a target and a tool in the broader competition for regional dominance.

The importance of protecting CMI is further underscored by its role in facilitating global connectivity and economic growth. Beyond its traditional functions as a space for commerce and fishing, the maritime domain has transformed into a crucial infrastructure nexus. The undersea cables, which carry 99% of global data traffic, exemplify this transformation, making oceans indispensable to modern communication networks. Contrary to popular belief, satellites

carry only 0.37% of U.S.[1] data. Offshore energy platforms and wind farms, integral to efforts at decarbonization and energy security, add another layer of vulnerability, blending economic aspirations with national security concerns.

Against this backdrop, understanding the evolving nature of threats to CMI is essential for ensuring the security and stability of the Black Sea region. As incidents in neighboring seas have shown, the absence of clear attribution and the non-linear dynamics of hybrid warfare present unique challenges to security frameworks. This study will first examine what makes CMI important in the current context and will follow with mapping the threat landscape in the context of the ongoing war in Ukraine. Although the Black Sea region is the main geographical focus of this study, we will present a comparative assessment examining also how questions related to protection of critical maritime infrastructure are dealt with in Norway, a country that is the main supplier of energy to Europe. Norwegian energy – first and foremost gas and electricity – reach markets in Europe via an extensive network of pipelines and cables that must be protected against various types of risks, challenges and threats. For that reason examining Norway's approach to protection of critical maritime infrastructure can provide some insights that are also relevant in the Black Sea context. One of the key reasons why such a comparative examination can be useful is the fact that in both the Black Sea and the North Sea context Russia is defined as the main possible source of threats to critical infrastructure, both on land and at sea. A good understanding of what threats to critical infrastructure originating from Russia must be dealt with is therefore of high relevance to policy- and decision-makers in all regions where one could expect Russian actions targeting elements of critical infrastructure. Here it is also important to understand what is sometimes referred to as Russia's full-spectrum approach to conflict in which boundaries between competition, confrontation and conflict are often blurred which makes reading of Russia's intentions and actions more complicated.

[1] Federal Communications Commission (2014) – Fact Sheet: Submarine Cables – The Backbone of Global Communications, Federal Communications Commission, available at: https://docs.fcc.gov/public/attachments/DOC-334397A2.pdf

2. Understanding Critical Maritime Infrastructure: *Definitions, Functions, and Strategic Importance*

Critical Maritime Infrastructure (CMI) which is understood 'as the systems and assets that are essential for the functioning of a society, economy, and country from a maritime perspective'[2] plays a pivotal role in ensuring economic stability, energy security, and geopolitical balance, particularly in strategically significant regions like the Black Sea. The term "infrastructure" was originally a military concept dating back to the early 20th century and gained prominence during the Vietnam War.[3] However, its evolution into a broader concept of critical infrastructure became a key feature of national security discourse with U.S. President Bill Clinton's Executive Order 13010 in 1996, which established the President's Commission on Critical Infrastructure Protection (PCCIP).

Since then, the use of the concept of critical infrastructure has continuously expanded alongside rapid technological advancements. To illustrate this substantial change, one could mention that the term "critical infrastructure" was mentioned 135 times in articles published in *Foreign Affairs* between 1945 and 1991 (3 mentions per year on average), 872 times in period between 1991 and 2022 (28 mentions per year on average) and 360 times between 2022 and 2024 (120 mentions per year on average in these three years). In the 21st century, digitalisation has revolutionized essential services, encompassing everything from communication and energy supply to healthcare and economic activity. In addition, growing geopolitical competition has increasingly placed critical infrastructure in the spotlight, turning it into a battleground for strategic influence and control.[4]

There are various definitions of critical infrastructure. What makes infrastructure important is the fact that economies and societies rely on critical infrastructure, which provides essential services to citizens and underpins economies. Military forces also rely to a great degree on public and private civilian infrastructure to be able to fulfil their tasks. From the point of view of

---

[2] Doğan, D. and Çetikli, D. (2023). *Maritime critical infrastructure protection (MCIP) in a changing security environment*. Maritime Security Center of Excelence at https://www.marseccoe.org/wp-content/uploads/2023/10/Maritime-Critical-Infrastructure-Protection-.pdf

[3] The Emergence of Infrastructure as a Decisive Strategic Concept (1999). Parameters, 29(4). Available at: https://doi.org/10.55540/0031-1723.1946

[4] For more on that see for instance Godzimirski, J.M and Andersen, M.S. (2024). The Political Economy of National Security, Critical Infrastructure and securitisation of Foreign Investments. Palgrave Macmillan.

policymakers who operate in Europe it is important to understand how critical infrastructure is understood by both the EU and by NATO.

The EU defines critical infrastructure as 'a system or part thereof located in the Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'. [5] What makes critical infrastructure important is not only the fact that it is related to policies and legislation ensuring the functioning of the internal market of the EU, but also to its security and defence agenda, including the strategic priority of the protection of the Union and its citizens and the EU's freedom of action.

NATO defines critical infrastructure as 'a nation's infrastructure assets, facilities, systems, networks, and processes that support the military, economic, political and/or social life on which a nation and/or NATO depends'.[6] From the point of view of NATO critical infrastructure is important because it enables the fulfillment of the organisation's core tasks of deterrence and defence; crisis prevention and management; and cooperative security. Recognizing the importance of the security of maritime subsea infrastructure not only to its own operations but to societies in general NATO decided therefore to establish its Maritime Centre for Security of Critical Undersea Infrastructure in May 2024 to be better prepared to address challenges stemming from this domain.[7] When launching this new centre NATO also proposed to adopt an approach to antagonist actors who could be suspected of conducting malign operations against this infrastructure based on the idea of denying deniability which could help the alliance deal with the difficult issues of attribution and plausible deniability.

---

[5] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection at https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng

[6] NATO. (2019). Infrastructure Assessment, ACO Directive 084-002, October 17, 2019. For more on the role of infrastructure in NATO strategy see Evans, C.V. (2022). Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency. NATO COE-DAT Handbook 1.
US Army War College Press at https://press.armywarcollege.edu/monographs/955/.

[7] NATO. (2024). NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure at https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui

The importance of these security and infrastructure related questions is also increasingly recognized by the EU. In its White Paper on Defence published on 19 March 2025[8] the EU identified four priority multi-modal corridors (rail, road, sea and air) for military mobility for short-notice and large-scale movements of troops and equipment that the armed forces need access to. These four elements of critical transport infrastructure are fit for a dual-use purpose and are to play a crucial part in a crisis with which both the EU and NATO will have to deal with when necessary.

Recognizing the importance of protection of critical infrastructure the EU and NATO decided therefore to embark on a closer cooperation to address serious challenges emerging in this area in the period of high tension in relations between the collective West and Russia. The launching of the EU-NATO Task Force on resilience of critical infrastructure took place on 16 March 2023 and has opened a new era of cooperation between these two key organisations.[9]

In June 2023 EU-NATO Task Force on the Resilience of Critical Infrastructure presented its Final Assessment Report[10] in which four sectors – energy, transport, digital infrastructure and space – were identified as critically important in the current context characterized by the growing assertiveness of strategic competitors and the increasing complexity of security threats.

There are several factors that make the need to protect energy infrastructure, including its maritime elements, important. These are:[11]

- **Energy Dependence and Trade**: Economies and societies rely on a mix of energy sources, highlighting the importance of international cooperation.

---

[8] European Commission. (2025). Joint White Paper for European Defence Readiness 2030 at https://defence-industry-space.ec.europa.eu/eu-defence-industry/white-paper-future-european-defence-rearming-europe_en

[9] NATO and European Union launch task force on resilience of critical infrastructure at https://www.nato.int/cps/en/natohq/news_212874.htm For more on the context see https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564

[10] European Commission and NATO, Final Assessment Report of the EU-NATO Task Force on Resilience of Critical Infrastructure, 2024, https://commission.europa.eu/document/download/34209534-3c59-4b01-b4f0-b2c6ee2df736_en?filename=EU-NATO_Final%20Assessment%20Report%20Digital.pdf

[11] For more details see the Final Assessment Report at https://commission.europa.eu/document/download/34209534-3c59-4b01-b4f0-b2c6ee2df736_en?filename=EU-NATO_Final%20Assessment%20Report%20Digital.pdf

- **Geopolitical Challenges**: Energy security is threatened by hostile actors, cyber-attacks, and economic coercion, impacting both civilian and military energy networks.

- **Infrastructure Vulnerability**: Incidents like the Nord Stream pipeline sabotage and attacks on hydroelectric dams in Ukraine and other elements of energy infrastructure show the vulnerability of energy infrastructure.

- **Digital and Undersea Risks**: Digital and undersea infrastructures are particularly challenging to protect against cyber-attacks and physical sabotage.

- **Supply Chain Vulnerabilities**: The production of renewable energy components is concentrated outside NATO and the EU, posing supply chain risks, especially in a situation when China controls important elements of value chains.

- **Transition to Renewables**: Efforts to reduce dependence on Russian energy and emissions have led to increased use of LNG and renewable energy sources, which bring new infrastructure protection-related challenges.

For instance, offshore wind energy has emerged as a cornerstone of decarbonization efforts. Countries like Denmark have taken the lead in harnessing wind potential from offshore areas, exemplifying how renewable energy projects can redefine maritime spaces. Yet this economic promise has been accompanied by rising security concerns. Sweden's decision to withdraw plans for offshore wind farm investments due to security risks underscores how economic interests are deeply intertwined with broader security considerations. Such tensions impact not only freedom of navigation but also a state's ability to pursue economic goals within its Exclusive Economic Zones (EEZs).

As far as LNG supplies are concerned the threat picture has also changed because of the increased importance of LNG supplies in the European energy mix. At the same time, the fixed gas infrastructure connecting for instance Norwegian gas fields with the European and UK markets must also be protected against various types of natural and man-made threats, which creates additional incentives to Norway and to countries that depend on gas supplies coming from Norway. One of the important initiatives aiming at increasing the level of resilience and protection of subsea infrastructure in the regional context was the setting up of a new format in April 2024 involving six North Sea countries: Belgium, the Netherlands, Germany, Norway, the

UK, and Denmark. The main objective of this cooperation is to protect subsea infrastructure in the North Sea through joining forces, taking appropriate measures and exchanging information and best practices.

This initiative focuses on resilience and prevention and is therefore complementary to NATO's endeavours, which all participants involved are members of.[12] It is expected that this experience can also be highly relevant in other regional context, especially in the Baltic Sea region where questions related to protection of critical infrastructure have over the past months received more attention due to several incidents involving Chinese and Russian vessels suspected of inflicting damage to elements of national and international critical infrastructure in the region. Also the Black Sea region could be considered as an area where similar solutions could be tested, but the situation along the Black Sea rim is for the time being complicated by the Russian war in Ukraine that has put serious constraints on various forms of regional cooperation in this region.

3. Conceptualizing threats to maritime security

In his seminal study on challenges related to maritime security Bueger described this concept as one of the buzzwords emerging in the study of international relations. He argued that maritime security can be understood in a matrix of its relation to other concepts, such as marine safety, sea power, blue economy and resilience. He also claimed that the issue of maritime threats should be studied using the securitisation framework that allows us to study how maritime threats are made. Finally, he also proposed to pay more attention not only to the question of conceptualization of the concept of maritime security but also to how the questions related to dealing with various types of threats to maritime security are translated into actual policy practices that are to enhance maritime security as understood by actors operating in this domain.[13]

---

[12] Six North Sea countries join forces to secure critical infrastructure at https://www.regjeringen.no/contentassets/03b6ba0be17e4ea0a57517a771ab5d8b/20240409_press-release_six-north-sea-countries-join-forces-to-secure-critical-infrastructure.pdf

[13] Bueger, C. (2015). What is maritime security? *Marine Policy*, *53*, 159-164. https://doi.org/https://doi.org/10.1016/j.marpol.2014.12.005

In his article Bueger noticed also the growing importance of maritime infrastructure in the debates on maritime security as well as the importance of offshore energy resources in this context.[14]

It is important to understand that questions related to maritime security and threats to maritime security should be viewed in the broader context of debate on the management of various types of maritime resources and activities. A good overview of this broader context is provided in the UN study on oceans and the law of the sea.[15]

A 2020 study on classification of maritime security threats[16] presents a useful framework for the examination of what risks, challenges and threats should be addressed in the maritime domain. Based on examination of various previous academic studies as well as official documents dealing with questions related to maritime security the authors proposed a three-level classification of maritime threats. Threats related to maritime interstate disputes, energy, food and resource security, maritime terrorism, cyber security and security of information systems and piracy were classified as the first-grade threats to maritime security. Threats related to human trafficking, smuggling of weapons and narcotics, illegal fishing, harming the maritime environment, climate change, armed robbery at sea and biological and chemical threats were defined as less challenging grade two or three threats. One can of course discuss whether such a classification should be accepted, but we find this classification useful as a starting point for mapping the maritime threat landscape in the Black Sea region in the current geopolitical context.

There are two important elements any adequate assessment of threats to maritime security in the Black Sea region in 2025 should consider. The first issue affecting maritime security and threat perceptions in the region is the kinetic warfare in Ukraine after the launching of the full-scale Russian invasion of the country in 2022. However, in addition to the kinetic warfare also other types of possible threats to maritime security should be considered. The Joint White Paper

---

[14] Ibid.

[15] United Nations. (2008). Oceans and the law of the sea. Report of the Secretary- General, UN General Assembly Document A/63/63, New York.

[16] Çetin, O. and Köseoğlu, M. (2020). A study on the classification of maritime security threat topics. *International Journal of Environment and Geoinformatics* (IJEGEO), 7(3):365-371. DOI: 10.30897/ijegeo.742336

for European Defence published in March 2025[17] presents a list of hybrid threats such as cyber-attacks, sabotage, electronic interference in global navigation and satellite systems, disinformation campaigns and political and industrial espionage, as well as weaponisation of migration as issues to be dealt with in the current geopolitical context. The same document lists sabotage activities in the Baltic and the Black Seas as serious concerns and adds that marine and maritime activities and associated traffic and critical undersea infrastructure are also under threat.

The same EU document as well as official threat assessments presented by national authorities and NATO identify Russia as a fundamental threat to Europe's security for the foreseeable future. It is therefore important to examine what kind of threats in general and to maritime security in the Black Sea region more specifically, can be posed by Russian actions in the years to come.

Russian Next-Generation Warfare (NGW)

Russia's Next-Generation Warfare (NGW), often equated with what the Western world defines as hybrid threats, reflects a deep strategic recalibration of conflict in the 21st century.[18] This approach does not focus on traditional military victories but rather on achieving strategic objectives through a comprehensive blend of military, economic, informational, and political tools. NGW emerged as a response to what Russia perceives as an ongoing Western campaign aimed at undermining its sovereignty and global influence. Rooted in the belief that since the collapse of the Soviet Union, the West has waged war on Russia using liberalism, international institutions, non-governmental organisations (NGOs), and strategic communication, Russian

---

[17] European Commission. (2025). Joint White Paper for European Defence Readiness 2030

[18] These ideas were first outlined in Gerasimov, V. (2013). Tsennost' nauki v predvidenii. *Voyenno-promyshlennyi kurier* (27 February) at http://www.vpk-news.ru/articles/14632. For an English translation see Gerasimov, V. (2016). The Value of Science Is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military Review* (January-February), 23–29 at https://www.armyupress.army.mil/portals/7/militaryreview/archives/english/militaryreview_20160228_art008.pdf

military thinkers sought a doctrine that could counteract and subvert these pressures in a highly adaptive manner.[19]

At the heart of NGW lies a profound understanding of the cascading nature of hybrid threats—where multiple domains such as cyber, information, political, and military are engaged simultaneously to achieve overlapping and reinforcing effects. These operations are designed to remain below the threshold of conventional armed conflict, exploiting legal and political grey areas to delay or complicate an adversary's response. Unlike conventional conflict, which relies on sequential operations aimed at achieving decisive end states, NGW is non-linear and adaptive, operating within a dynamic and evolving environment.

In NGW, actions are not directed toward fixed objectives; instead, they follow a sense-probe-respond approach, constantly adjusting to the evolving strategic context. This adaptive model reflects a significant departure from the linear means-ways-ends logic of traditional military operations. Each tactical action generates new information and potential opportunities, allowing strategies to evolve in real time. Such non-linear dynamics foster an environment where no single event or action can be clearly identified as a turning point, making attribution difficult and responses slow.

The complexity of NGW lies in its ability to create complex, not merely complicated, situations. In complicated scenarios, actions are predictable and solutions follow known cause-and-effect patterns. In contrast, complex situations—like those engineered by NGW—are fluid and shaped by emergent behaviors, where seemingly minor actions can cascade into major consequences. Military logic, which traditionally emphasizes sequential or individual actions to achieve clear outcomes, is replaced here by iterative strategies that rely on continuous feedback loops, enabling rapid adjustments and creating persistent pressure on the adversary.

This feedback-driven approach is less concerned with achieving a conclusive military victory and more focused on gaining incremental advantages across various domains. These advantages are often temporary but, when accumulated, create significant strategic leverage. In

---

[19] Galeotti, M. (2014) – The "Gerasimov Doctrine" and Russian non-linear war, In Moscow's Shadows, available at: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war, as cited in: Mitrescu, S. & Sokolov, A. (2025), In the Crosshairs: Hybrid Threats and the Challenge to Maritime Infrastructure, in: G. Scutaru & M. Margvelashvili (eds.), Defending Maritime Assets: Approaches to Critical Infrastructure Protection, Springer, Cham, available at: https://link.springer.com/book/10.1007/978-94-024-2300-6

this framework, the objective is not to shape the battlefield physically but to influence behavior, coercing adversaries into adopting suboptimal decisions without realizing they are being manipulated.

The Helsinki Centre of Excellence's CORE model and the European Commission's Landscape of Hybrid Threats Conceptual Model offer valuable insights into how Russia's NGW operates. These models conceptualize hybrid warfare as a highly adaptive system, where threats interact across multiple domains and phases—priming, destabilization, and coercion. The non-linear and iterative nature of NGW makes it difficult to differentiate between conventional influence and more subversive interference. Actions oscillate between low and high activity, avoiding direct confrontation while continuously exerting pressure and gaining leverage.

In this context, the distinction between military and civilian targets becomes increasingly blurred, with state and non-state actors playing complementary roles. Russia's use of cyber operations, disinformation campaigns, and political interference exemplifies this approach. It often begins with efforts to prime the environment—spreading false narratives, cultivating divisions within target societies, and conducting cyber reconnaissance. As vulnerabilities are exposed, operations transition into active destabilization, targeting critical infrastructure, media ecosystems, and political institutions. Finally, in the coercion phase, Russia seeks to force adversaries into concessions through a combination of overt and covert pressure.

Understanding Russian NGW requires abandoning the expectation of clear starting and ending points. It is an open-ended, evolving process that thrives on ambiguity and unpredictability. Rather than seeking a decisive victory, it aims to keep adversaries in a constant state of uncertainty, forcing them to respond to multiple, simultaneous challenges across different domains. This constant adjustment and strategic fluidity are what make NGW a particularly formidable challenge for conventional security frameworks.

In essence, NGW is more about reshaping the strategic environment to Russia's advantage. By blurring the lines between peace and war, military and civilian, influence and interference, Russia has developed a strategic model that keeps adversaries off-balance, ensuring its actions remain below the threshold of conventional retaliation while continuously expanding its influence.

Cyber threats

The digitization of critical services and increased connectivity through industrial control systems (ICS) and operational technology (OT) have exposed vulnerabilities that malicious actors can exploit. Offshore energy installations, particularly in oil, gas, and renewable energy sectors, are increasingly targeted due to their strategic and economic importance.

The range of cyber threats to maritime infrastructure encompasses sophisticated attacks such as ransomware, advanced persistent threats (APTs), and supply chain compromises. Ransomware attacks can disrupt operations, halt energy production, and compromise sensitive data by targeting supervisory control and data acquisition (SCADA) systems and ICS. Phishing and social engineering are commonly employed to deceive personnel into revealing credentials or installing malware, providing attackers with unauthorized access to critical systems. Additionally, distributed denial of service (DDoS) attacks can cripple communication and control networks, causing widespread operational disruptions.[20]

The Russian Federation plays a central role in orchestrating cyber threats in the region, leveraging a combination of hybrid tactics, cyberattacks, and electronic warfare. Russian state-sponsored groups such as APT28 (Fancy Bear) and Sandworm have targeted critical infrastructure, often as part of broader geopolitical campaigns. These attacks seek to compromise energy and maritime systems, disrupt essential services, and manipulate public opinion through coordinated disinformation campaigns.[21]

The interconnected nature of modern offshore infrastructure makes it highly susceptible to cyberattacks. Legacy systems limited physical security, and the absence of robust cybersecurity practices heighten the risk. The integration of IT and OT systems has expanded the attack surface, allowing threat actors to exploit vulnerabilities in SCADA and ICS environments. Supply chain attacks have also become a growing concern, with attackers compromising third-party vendors to gain unauthorized access to primary infrastructure

---

[20] Burlacu, M. (2025) – Exploring and Mitigating Cyber Threats Related to Energy Offshore Critical Infrastructure in the Black Sea Region, in: G. Scutaru & M. Margvelashvili (eds.), Defending Maritime Assets: Approaches to Critical Infrastructure Protection, Springer, Cham, available at: https://link.springer.com/book/10.1007/978-94-024-2300-6

[21] ibid.

4. Mapping the Maritime Threat Landscape:
National Assessments from the Black Sea Rim

Romania

For Romania, the Black Sea is a space of multiple significance in military, economic, energy, and commercial terms. The region's strategic relevance is reflected in fundamental state documents such as the National Defence Strategy, the Defence White Paper, and Romania's Military Strategy, which outline the country's role as a pillar of security in the Black Sea region. In this regard, Romania is committed to consistently promoting the region on NATO's security agenda, emphasizing its importance for European and Euro-Atlantic stability, and intensifying cooperation with allies and strategic partners to strengthen regional energy security.

Romania has a 245 km coastline along the Black Sea and an Exclusive Economic Zone (EEZ) covering approximately 25,000 km². Following the illegal annexation of Crimea by the Russian Federation in 2014, efforts to raise awareness among allies about the region's strategic importance have been intensified. Located less than 400 km from Sevastopol, Romania is a frontline state on NATO's Eastern Flank, with direct proximity to Russian air and naval forces.

Starting in 2027, Romania will become the largest natural gas exporter in the European Union, due to the exploitation of resources in the Neptun Deep perimeter of the Black Sea. Located approximately 170 km offshore, in waters between 100 and 1,000 meters deep and covering an area of 7,500 km², Neptun Deep is estimated to hold reserves of around 100 billion cubic meters of natural gas. The drilling platform was delivered to Romania in 2024, and exploitation is planned to begin in 2027.

Romania is making significant strides in the development of offshore wind energy, with the Romanian Parliament having passed the Offshore Wind Energy Bill proposed by the Ministry of Energy.[22] According to the World Bank, Romania has a vast offshore wind energy potential, with estimates suggesting 76 GW of technical potential. This includes 22 GW suitable for fixed-

[22]Mihai, C. & Rotaru, S. (2023) – *Romanian Government Approves Offshore Wind Law for Black Sea Power Plants,* Euractiv, 22 December 2023, available at: https://www.euractiv.com/section/politics/news/romanian-government-approves-offshore-wind-law-for-black-sea-power-plants/

bottom turbines and 54 GW for floating turbines.[23] A road map by the European Commission and the World Bank suggests two scenarios: a moderate 3 GW target, which would meet 16% of Romania's electricity needs and contribute €1.4 billion to the economy by 2035, and a high-growth 7 GW target, which would cover 37% of Romania's electricity demand and contribute €5.3 billion to the national economy.[24]

Romania is also actively engaged in other major projects in the Black Sea region, including the Memorandum signed in October 2022 with Azerbaijan's SOCAR company, aimed at developing a liquefied natural gas (LNG) facility in the Black Sea. Additionally, on December 17, 2022, under the auspices of the European Commission, Romania, Azerbaijan, Georgia, and Hungary signed an agreement in Bucharest for the construction of a submarine power cable designed to transport Azerbaijani green energy to Europe.

A key priority for Romania is strengthening NATO's presence in the region through the modernization of the 57th Mihail Kogalniceanu Air Base, which currently hosts approximately 3,000 U.S. troops. The modernization process, carried out in phases over a 20-year period, aims to transform the base into one of the most modern and expansive military facilities in Europe, covering an area of 2,800 hectares.

In the current context marked by the conflict in Ukraine, the Danube River complements the strategic importance of the Black Sea for Romania, serving as the second maritime access route to the Black Sea region after the Bosporus and Dardanelles straits. Crucial in supporting Ukraine after the 2022 Russian aggression, the Danube became vital for maintaining export flows following Russia's withdrawal from the Black Sea grain deal, with Sulina Channel transport increasing from 5 million tons in 2021 to 16.5 million tons in 2023. Additionally, the Danube holds significant potential for Ukraine's reconstruction plans, contributing to economic development and enhancing regional cooperation. The Danube represents the second access route to the Black Sea after the Bosporus and Dardanelles straits and serves as a vital transport

---

[23] Power Technology (2024) – OWC to Support Offshore Wind Development in the Black Sea, Power Technology, 9 May 2024, available at: https://www.power-technology.com/news/owc-offshore-wind-black-sea/

[24] World Bank (2024) – A Roadmap for Offshore Wind in Romania, World Bank, 27 September 2024, available at: https://www.worldbank.org/en/news/infographic/2024/09/27/a-roadmap-for-offshore-wind-in-romania

artery to the heart of Europe. The ports of Galați and Brăila in Romania, Giurgiulești in the Republic of Moldova, and Reni and Izmail in Ukraine can form a major logistics hub, playing a key role in Ukraine's reconstruction and in connecting both Ukraine and the Republic of Moldova to Western Europe.

Romania is the country closest to the southern regions of Ukraine, among the most affected by the war. At the same time, it is also the closest country to the areas in Ukraine that contain rare metals and earths, in which the United States has expressed direct interest. Securing the western Black Sea basin through a NATO presence, and especially an American presence, is vital for the exploitation of the region's energy resources.

Ukraine

In July 2024, Ukraine adopted a new Maritime Security Strategy tailored to the current challenges in the Black Sea, primarily stemming from Russia's invasion in February 2022. The strategy reaffirms Ukraine's commitment to European Union and NATO integration, as well as the development of international partnerships to enhance regional security. A central objective is to transform the Black Sea and the Sea of Azov into peaceful and secure areas for trade and free navigation by strengthening maritime defense capabilities, reclaiming occupied territories, and fostering international cooperation frameworks.

An important element of Ukraine's strategy is its intention to establish the conditions for a temporary international naval military presence on the territory of the Crimean Peninsula after its liberation. Additionally, Ukraine aims to leverage all available international legal instruments to restrict Russia's naval presence in the Azov-Black Sea basin. Among the key initiatives is the creation of the international platform "Secure Black Sea," which will bring together regional states and other countries affected by the economic and food supply disruptions caused by Russia's obstruction of free navigation.

To strengthen its maritime security, Ukraine plans to conclude bilateral and multilateral agreements with Black Sea littoral states (excluding the Russian Federation) and other interested countries, establishing security guarantees and specific mechanisms for the Azov-Black Sea region. The strategy also envisions the formation of an anti-mine coalition, the conduct of joint military exercises, and the creation of a new naval formation in the Black Sea

alongside NATO member states and other partners. The primary objective of this initiative is to counter threats posed by Russia and enhance regional stability and security.

Ukraine, possessing a coastline of roughly 1,300 km, is a key player in global grain exports, its trade being largely dependent on transit through the Black Sea. Additionally, the Ukrainian continental shelf in the Black Sea and the Sea of Azov holds substantial hydrocarbon resources, estimated at 2.3 billion tonnes of oil equivalent, while natural gas reserves within Ukraine's Exclusive Economic Zone are estimated at 1,751 billion cubic meters.

In this context, the Maritime Security Strategy emphasizes the importance of attracting investment, particularly foreign investment, for the exploration, development, and exploitation of natural gas resources on the continental shelf. It also focuses on creating and modernizing a robust protection system for critical maritime energy infrastructure, through the implementation of advanced underwater protection solutions and defense technologies against drone threats.

Russia

The 2022 Maritime Doctrine of the Russian Federation[25] outlines six priority areas for its global maritime policy: the Atlantic, the Arctic, the Pacific, the Caspian Sea, the Indian Ocean, and Antarctica. Within the Atlantic region, particular emphasis is placed on the Black Sea and the Baltic Sea, which are considered areas of strategic importance. In the Atlantic, Russia's maritime policy is focused exclusively on its relationship with NATO, which it perceives as a threat to its security. The doctrine highlights that the primary point of tension lies in NATO's plans to expand its military infrastructure closer to Russia's borders and the Alliance's aspirations to strengthen its global influence.

In the Black Sea and Azov Sea basin, Russia's maritime policy aims at the rapid restoration and consolidation of its strategic position. To achieve this, Russia is focused on modernizing and expanding the Black Sea Fleet, enhancing port and logistics infrastructure in Crimea and along the Krasnodar Krai coastline, and maximizing the region's transport and transit potential through the development of international transport corridors.

---

[25] Government of the Russian Federation. (2022). Morskaya Doktrina Rossiyskoy Federatsii at http://www.scrf.gov.ru/security/military/document34/

From a historical perspective, Russia views the Black Sea as a strategic gateway, providing the shortest route to the Mediterranean Sea and, by extension, to the Middle East, Africa, Asia, and Latin America. The Black Sea Fleet plays a central role in this strategy, with its primary base located in Sevastopol. This city, situated on the Crimean Peninsula—illegally annexed by Russia in 2014—holds major strategic importance due to its deep-water port, which remains operational year-round. Following the annexation of Crimea in 2014, Russia has significantly strengthened its military capabilities in the region by deploying advanced air defense and anti-ship systems and increasing the strength of the Black Sea Fleet. These enhancements have enabled Russia to establish extensive surveillance and control over the entire Black Sea region.

The Russian invasion of Ukraine, initiated on 24 February 2022, has yielded unexpected repercussions for Russia's naval operations in the Black Sea. Effective Ukrainian strikes using naval drones and missiles exposed the vulnerability of Russian vessels in Crimea, compelling Russia to withdraw its Black Sea Fleet from the peninsula in 2023, marking the end of a two-and-a-half-century-long presence. Consequently, even Russia's efforts to establish a land corridor through Donetsk, Zaporizhzhia, and Kherson to bolster Crimea's security have failed to restore the safety of Crimean ports for its fleet.

The Black Sea is not only a region of strategic military importance for Russia but also plays a crucial role in connecting the country to global markets, serving as a key commercial artery. With a cargo volume exceeding 160 million tons handled in 2023, the port of Novorossiysk stands as Russia's primary commercial port. Additionally, in 2023, ports in the Azov-Black Sea Basin handled 32% of the total exported goods, highlighting the region's crucial economic significance. Lastly, approximately 25% of Russian oil exports leave from the Black Sea, representing a crucial share of profits that are used by the Kremlin to fund its war efforts.[26]

Russia has the capability to transfer naval forces between the Caspian Sea and the Black Sea, and vice versa, through the Volga-Don canal network. It is not out of the question that we may see joint naval exercises in the Black Sea involving Russian and Iranian naval forces, aimed primarily at sending a strong signal to NATO.

---

[26] Black Sea News (2024) – Ukraine’s Maritime Strategy: Security, International Presence, and Resource Development, Black Sea News, 10 September 2024, available at: https://www.blackseanews.net/en/read/221802

A ceasefire agreement will not bring peace to the Black Sea. Even if kinetic actions cease, Russia will maintain an aggressive naval posture to disrupt freedom of navigation and impact connectivity and energy supply routes. Russia will resort to various hybrid tactics to achieve its objectives, such as blocking areas within Romania's and Bulgaria's EEZ under the pretext of military exercises, laying mines, and engaging in electronic warfare to disrupt the GPS signals of vessels. Due to these hybrid actions, the Black Sea will remain a battlefield. This is precisely why NATO and the EU must cooperate to mitigate and counter these risks.

Türkiye

Türkiye's strategic priorities in the Black Sea are integral to its broader regional and geopolitical ambitions. Positioned at the crossroads of Europe, Asia, and the Middle East, the Black Sea serves as a critical maritime corridor, making it a focal point of Türkiye's efforts to assert control and expand its influence. By strengthening its naval capabilities, emphasizing its stance on the Montreux Convention, and developing its role as an energy hub through offshore gas projects and pipelines, Türkiye aims to bolster its leadership in the region. Türkiye's approach in the Black Sea highlights its regional ambitions and preoccupation with ensuring that no single power dominates the region.

Türkiye's strategic priorities in the Black Sea are closely linked to its broader goal of reducing external influence and solidifying its position as a regional leader. A key component of this vision is the relatively recent emergence of the *Mavi Vatan* doctrine. Named after a large-scale naval exercise conducted in 2019, Türkiye's *Mavi Vatan*, or "Blue Homeland," doctrine has garnered significant attention within Turkish political, military, and foreign policy circles. It should not be construed as a rigid naval strategy but rather as a declaration of intent, emphasizing Ankara's imperative for a robust and capable blue-water navy. The prevailing understanding is that *Mavi Vatan* rests on three core principles. Firstly, it entails expanding Türkiye's sphere of influence through the bolstering of its navy and the establishment of overseas military bases, notably in regions like Africa and the Persian Gulf. Secondly, the doctrine emphasizes a heightened role for Türkiye's navy in energy-related geopolitical competitions, coercive measures, and naval diplomacy. Lastly, it aims to support the growth of Türkiye's indigenous defense industry, aligning with the nation's broader strategic objectives.

Furthermore, Türkiye’s strategic position in the Black Sea is heavily influenced by the Montreux Convention, which grants Ankara significant authority in regulating the presence of extra-regional fleets in the region, complemented by its control of the Turkish Straits. This control is reinforced by treaty-based tonnage limitations for non-littoral states' warships permitted temporary access to the area. Under the convention, Türkiye has the authority to regulate and restrict the transit of military ships belonging to non-Black Sea states, ensuring the security and stability of the region. This gives Türkiye a unique leverage in controlling access to the Black Sea, allowing it to assert its dominance and safeguard its national interests in the strategically important maritime corridor. Additionally, the convention grants Türkiye the ability to mobilize its navy to protect its territorial waters and respond to any threats or provocations, further enhancing its position as a key player in Black Sea geopolitics. According to a recent intervention of Zeki Levent Gümrükçü, Deputy Minister of Foreign Affairs, Republic of Türkiye during the Antalya Diplomacy Forum 2025, a ceasefire will not be sufficient to warrant the opening of the straits, which will only be re-opened if a comprehensive peace deal is achieved.

As global energy dynamics shift due to the ongoing Russian-Ukrainian conflict, Türkiye's focus in the Black Sea is on its offshore sector, particularly the Sakarya gas project. This multi-phase project is expected to tap into 710 billion cubic meters of recoverable gas, potentially supplying one-third of Türkiye's gas needs for the next 25-30 years. Phase Two alone is projected to deliver 11 billion cubic meters per year, with an estimated 13 billion cubic meters annually by 2050. Meanwhile, Türkiye’s role as an energy transit hub is also strengthened by key pipelines like TurkStream, which has a capacity of 31.5 bcm and transported 26.75bcm to Türkiye in 2023, directly connecting Russia's vast gas reserves to Türkiye and Europe, and Blue Stream, which transported 15.98 bcm in 2021. Additionally, the country is diversifying its energy sources through projects like TANAP (Trans-Anatolian gas pipeline) and TAP (Trans Adriatic Pipeline) automat, part of the Southern Gas Corridor, with plans to increase their capacity to 20 bcm annually by 2027. In 2023, Türkiye imported 51.48 bcm and exported 0.89 bcm, underscoring the country’s growing energy consumption and the critical importance of its pipelines in ensuring energy resilience and regional influence.

In order to protect its critical infrastructure, Türkiye is undertaking a significant naval modernization program. The Ministry of Defense reports that 31 ships, including an aircraft carrier and a destroyer, are being built in domestic shipyards as part of a broader plan to make naval shipbuilding a domestic affair, with an estimated cost of $8 billion. A recent example of a

cooperative action is the joint initiative with Bulgaria and Romania to address drifting sea mines in the Black Sea by establishing the Mine Countermeasures Naval Group to clear these threats. At the time of the writing of the study, there are ongoing discussions about the expansion of the initiative to include critical maritime infrastructure.[27]

In conclusion, Türkiye's strategic priorities in the Black Sea are vital to its regional leadership and broader geopolitical aspirations. By strengthening its military capabilities, enhancing energy infrastructure, and fostering multilateral cooperation, Türkiye aims to solidify its role as a key player in the Black Sea, safeguarding its interests and ensuring regional stability. This approach has enabled Türkiye to play an influential role in the Black Sea's security architecture, balancing its relationships with both NATO and Russia to maximize its strategic autonomy and regional influence. A reset in relations between Washington and Ankara, following the return of President Donald Trump to the White House, would further increase Turkey's strategic relevance in the Black Sea, Central Asia, and the Middle East. This would have an impact on the development of connectivity projects of interest to the United States, such as the Middle Corridor, for example.

Future Threat Landscape in the Black Sea Region

The Black Sea has long held a pivotal position in the foreign policy strategies of the surrounding countries. Its significance extends beyond regional maritime interests, deeply intertwining with global security concerns and geopolitical maneuvering. The area's strategic importance is amplified by its critical role in facilitating trade, energy exports, and undersea communication, placing it at the forefront of geopolitical competition. The current developments in the Black Sea's Critical Maritime Infrastructure (CMI) not only overlap with regional economic interests but are increasingly synchronized with the geopolitical ambitions and military actions of external actors, particularly the Russian Federation.

The cessation of hostilities in Ukraine will likely initiate a transformation in the Black Sea's geopolitical landscape. With the potential lifting of the Montreux Convention provisions—which regulate naval passage through the Turkish Straits—the internationalization of the Black Sea becomes a real possibility. This scenario would usher in a new phase of heightened competition,

[27] Zeki Levent Gümrükçü, Intervention at the Antalya Diplomacy Forum 2025, Deputy Minister of Foreign Affairs, Republic of Türkiye, 1 March 2025.

as Russian maritime assets, which were constrained during the conflict, are expected to return in full force. The reassertion of Russia's naval capabilities in the region would lead to a perpetually contested environment, where political, military, and economic confrontations are bound to become a norm rather than an exception.

Moreover, the Black Sea's security dynamics are increasingly synchronized with other regions that Russia perceives as frontlines in its confrontation with the West. The synchronization between conflicts in the Black Sea and other flashpoints, such as the Arctic and the Baltic Sea, reveals a broader pattern of Russia's strategic thinking. This approach underscores the interconnected nature of Russia's regional policies, viewing these areas as parts of a continuous battlefront rather than isolated zones of interest. This broader geopolitical strategy allows Russia to exert pressure simultaneously across multiple regions, complicating the response efforts of NATO and the European Union.

In essence, the Black Sea is no longer just a regional maritime domain but a contested geopolitical space where economic aspirations, national security concerns, and global power rivalries intersect. The growing complexity of this environment demands continuous vigilance and adaptability, as developments in one region inevitably ripple across others in a broader strategic theater. It is therefore important to map how questions related to developments in the Black Sea region are addressed in other areas in which the insecurity caused by Russian recent actions in Ukraine has been factored in national threat assessments. Norway provides some interesting insights in that matter as questions related to protection of infrastructure have over the past years, for obvious reasons related to Russian actions, drawn more attention.

5. Norwegian Security Outlook: Critical Infrastructure and Hybrid Threats, 2022–2025

In February 2025 the three Norwegian organisations responsible for security presented their open threat assessments to the Norwegian and international audience. In this brief examination of these three threats assessments, we will focus first on the more general aspects and then narrow this examination to questions related to security of infrastructure and energy sector in Norway. Because threat map presented in these official Norwegian threat assessments has evolved since Russia's full-scale invasion in Ukraine, we will conduct a comparative examination of the set of official threat assessments between 2022 and 2025.

Norwegian threat perceptions 2022-2025

On 5 February 2025 the three Norwegian organisations presented their open threat assessments.[28] In the annual, open threat assessment "Focus", the Norwegian Intelligence Service (NIS) presented its analysis of external threat actors and trends that the service believes are particularly relevant to Norwegian security in the coming year.[29] The open threat assessment presented by the Norwegian Police Security Service (PST) focuses on expected developments within PST's areas of responsibility, including terrorism, espionage and threats against government officials within the country's borders.[30] National Security Authority (NSM) presented its annual risk assessment "Risk 2025" to help to see security in a broader context focusing on how authorities and businesses must protect themselves against the threats that the NIS and PST point to in their threat assessments.[31]

NIS is Norway's foreign intelligence service. The main tasks of NIS are to warn of external threats to Norway and high-priority Norwegian interests, to support the Norwegian Armed Forces and the defence alliances Norway is part of, and to assist in political decision-making processes by providing information of significance to Norwegian foreign, security and defence policy. In the annual threat assessment *Focus*, NIS presents its analysis of the current situation and expected developments in geographic and thematic areas considered particularly relevant to Norwegian security and national interests.

According to NIS 2025 threat assessment Norway faces increasing security challenges due to rising tensions between Russia, China on the one hand and the West on the other. This has led to deterioration of international cooperation escalation of conflicts, an arms race, and heightened terrorist threats. The main challenge is still Russia's war in Ukraine that is going to

---

[28]Norwegian Government. (2024). Årets trusselvurderinger er presentert, available at: https://www.regjeringen.no/no/aktuelt/arets-trusselvurderinger-er-presentert/id3086625/

[29] Norwegian Intelligence Service.(2025) Fokus 2025 at https://www.etterretningstjenesten.no/publikasjoner/fokus. For an English version see https://www.etterretningstjenesten.no/publikasjoner/focus/focus2025_contents

[30] Norwegian Police Security Service. (2025). Nasjonal trussel vurdering at https://www.pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/nasjonal-trusselvurdering-2025_no_web.pdf. For an English version see https://www.pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/_nasjonal-trusselvurdering-2025_uu-engelsk.pdf

[31] National Security Authority. (2025).Risiko 2025. Et sikkert Norge i en ussikker verden (A safe Norway in an unsafe world) at https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2025

continue in 2025. Although there is a slow progress in Russia's favour, the war's cost is very high. Western military support to Ukraine is obstructing Russia from achieving its aims in Ukraine and Russia is seeking to exert pressure on the West, including through sabotage operations. This could impact Norway.

It is expected that a Russian victory would bolster the Kremlin's belief in using military force for its authoritarian and expansionist policies, increasing the threat to Europe, especially to states in Russia's neighbourhood, including Norway. Also the fact that China and Russia are cooperating more closely is a source of concern. It is also expected that the growing tensions in relations between Russia and China on the hand and the West on the other will result in accelerating arms race, causing even more tensions and unpredictability when the relationship involves not two but three key global actors. In addition, the conflicts in the Middle East have caused a significant shift in power and have heightened the terrorist threat to Europe.

PST is Norway’s domestic security service and is responsible for preventing and investigating crimes that pose a threat to national security. One of the key tasks of the service is to identify and assess threats relating to intelligence, sabotage, the spreading of weapons of mass destruction, terrorism and extremism. The assessments are meant to assist policy formulation and support political decision-making processes. PST’s annual threat assessment is a part of the service’s public outreach, explaining the expected development in the threat environment.

PST’s 2025 threat assessment describes the security situation as being in flux, which places demands on society’s ability to adapt. It also claims that war, conflict and rivalry in the world will continue to mark the threat situation in Norway. This document describes Russia as the greatest threat against security in Europe and concludes that Russia has demonstrated its resolve and ability to carry out sabotage operations on European soil, arguing that this may also affect Norway. In addition, it describes the intelligence threat from China as also increasing. The use by other states of various types of proxy actors against Norway is also considered a serious challenge. According to this annual threat assessment 2025 is to be marked by hybrid threats, such as sabotage, influence operations and illegal intelligence. The threats to Norway posed by state actors are more unpredictable, extensive and demanding than they have been for many decades.

Sharing this opinion with the threat assessment presented by the NIS, the PST argues that escalation in the level of conflict in the Middle East could affect threat actors in Norway and lead

to more radicalisation, polarisation and unrest in the Norwegian society. A special attention is being paid to threats related to various types of influence operations because it is expected that both non-state and state actors will seek to influence our opinions, thoughts and feelings, to manipulate public opinion to either increase support for their own views or to undermine trust in society. This could pose a serious challenge in the run-up to the elections to the Norwegian Parliament (Storting) and Sámi Parliament (Sámediggi) coming in 2025.

NSM is Norway's agency for national preventive security. The agency's mission is to strengthen Norway's ability to counter espionage, sabotage, terrorism and hybrid threats. NSM helps organisations protect civilian and military information, systems, objects and infrastructure that are relevant to national security by giving advice and performing control activities, supervision, security testing and security research. To provide a better protection of digital infrastructure, NSM operates a national warning system for critical infrastructure (VDI) and coordinates national efforts to handle serious cyberoperations. Risiko, NSM's annual risk assessment, aims to help Norwegian enterprises and authorities to manage security risks by providing information about vulnerabilities, threats and security measures.

In its Risiko 2025 assessment the NSM focused on the following set of questions various actors in Norway, including authorities and business community will have to address:

- **Increased Security Measures**: Both public and private sectors must implement new and enhanced measures to protect national security interests, considering the worst-case scenarios like the destruction of critical infrastructure.

- **Sabotage Prevention**: Emphasis must be put on backup solutions and repair preparedness as crucial. Better understanding the consequences of losing access to essential goods or services is also considered very important.

- **Value Assessment**: Businesses need to evaluate their assets and their overall value in the national context, balancing local development against national security needs.

- **Human Factor**: Employees are vital as they have daily access to information and systems. Threat actors may try to build relationships with individuals to gain access and questions related to the so-called insider-related threats must be considered important.

- **Daily Security Management**: Effective daily security management, procedures and routines can contribute to reducing insider risks.

- **Digitalization Vulnerabilities**: While digitalization offers benefits, it also creates new vulnerabilities. Exploitation of software vulnerabilities and the introduction of new vulnerability surfaces through mobile phones, modern vehicles, and AI are increasing and this threat must be addressed.

- **Supply Chain Security**: Businesses rely on technology and services from third parties and suppliers, becoming part of national security efforts. Proper security level monitoring throughout the supply chain is essential to avoid unnecessary risks and interruptions.

- **National Importance**: Norway manages significant assets, including being a critical supplier of gas and energy to Europe and an increasingly important space nation. NATO allies depend on supply lines through Norway to provide support to new members, such as Sweden and Finland.

- **Total Defence**: Norway's total defence requires both military and civilian sectors to be prepared for crises and war. Resisting complex threats, and supporting military efforts are therefore crucial elements of the system. The "Total Preparedness Report (2024-2025)" highlights the risks of sabotage and challenges related to technological development and defence enhancement.

Having in mind that Russia's war against Ukraine is the biggest challenge to European and national security and that Russia has during the war in Ukraine consistently attacked elements of critical infrastructure, including energy infrastructure, it must be expected that those issues are also addressed in the set of official threat assessments in Norway presented in February 2025. Also the fact the West's – and Norway's – political, economic and military support to Ukraine has played a crucial part in preventing Russia from winning this ongoing war one should expect that in the worst-case scenario Russia can consider conducting various types of hybrid operations against elements of critical infrastructure in the West, including in Norway. In addition, having in mind the importance of the Norwegian critical energy infrastructure in providing access to energy in Europe in the context of this ongoing conflict one should also consider to what extent the issue of possible Russian operations against Norwegian critical energy infrastructure has been internalized by the Norwegian policymaking community. This

section will therefore present whether and how these questions are addressed in the current set of official Norwegian threat assessments and how the approach to these issues has evolved after the outbreak of the full-scale war in Ukraine in 2022. In the first subsection an examination of how these issues are addressed in the 2025 threat assessments is presented. The following subsection presents what attention has been given to these important questions in the threat assessments published between 2022 and 2024.

Threats to critical infrastructure and energy sector 2025

The NIS 2025 threat assessment mentions the term 'infrastructure' 29 times. According to this document Russia will be able to target both weapons supplies and critical infrastructure with sabotage (p.8) and Norwegian infrastructure also can be targeted because Russia will respond with increased risk-taking and expanded use of instruments against Ukraine's Western supporters to prevent and weaken support for Western arms support. Because Russia has been consistently attacking Ukraine's energy infrastructure during this war (p.20-21), one should expect that also energy infrastructure in countries providing support to Ukraine could be exposed to this type of aggressive operations if the conflict were to escalate. Questions related to protection of subsea critical infrastructure in the Baltic Sea regions received a lot of attention in 2024 and 2025 and are also addressed in the NIS 2025 assessment (pp.30-31). The NIS 2025 concludes that in 2025, Russian threat actors will carry out network-based interception operations against Norwegian decision-making bodies, foreign missions, the Armed Forces, critical infrastructure, academia and technology companies. The aim of interception against critical infrastructure may also be to prepare for future digital sabotage (p. 29).

According to NIS 2025 challenges to critical infrastructure can be posed not only by Russia but also by China that takes control over elements of critical infrastructure through investments but also maps infrastructure to prepare for possible actions against it.

Concerning energy-related threats the NIS 2025 mentions energy 7 times and threats to energy supplies via critical infrastructure are considered the most serious security challenge (p.31).

PST 2025 mentions infrastructure 10 times. The official view is that since 2013 Russian intelligence services organised several actions against property and logistics infrastructure linked to deliveries to Ukraine, but also against civilian infrastructure, including means of

transport and shops. Although no actions targeting infrastructure in Norway have so far been observed in Norway, the PST considers it likely that Russian intelligence will attempt to carry out such actions against targets in Norway in 2025 (p.12). The purpose of any actions against targets in Norway will be to prevent Norwegian deliveries to Ukraine or to negatively influence public opinion's attitude towards support for Ukraine. Targets for any actions in Norway will likely be similar to what was seen in Europe, but also in addition, Norwegian-owned energy infrastructure could also be targeted for sabotage. It is also expected that such actions could be conducted by proxy actors without formal ties to intelligence and security services or other government agencies in Russia which will make the question of attribution more difficult. It is also expected that Russian intelligence service will continue to map critical infrastructure in Norway to expose its vulnerabilities and prepare for future malign actions (p.12). Especially the use of civilian vessels for this purpose is viewed as posing a challenge (p.24). Another infrastructure-related challenge is the acquisition of property near critical infrastructure, military installations or infrastructure of military importance because strategically located property may be used to carry out intelligence activities and pose a threat to national security (p.26).

PST considers it likely that Russian intelligence will attempt to carry out actions against targets in Norway in 2025. The purpose of any actions against targets in Norway would be to prevent Norwegian deliveries of help to Ukraine or to negatively influence public opinion's stance on Ukraine support. The targets of any actions in Norway will likely be similar to those seen in Europe. In addition, Norwegian-owned elements of energy infrastructure could also be targets for sabotage (p.12).

NSM 2025 mentions infrastructure 19 times. To start with, it concludes that critical infrastructure, such as fiber cables, power lines, and gas pipelines, are examples of assets that will be difficult to completely secure (p.7). It says for instance that negative scenarios related to destruction of critical infrastructure that some years ago were considered unthinkable should be viewed as thinkable in 2025 (p.8). Since the overall security situation has become more challenging also issues related to protection of critical infrastructure have been internationalized, especially after Finland and Sweden became NATO members (p.10). Because according to PST 2025 threat assessment malign actions against infrastructure are considered likely in 2025, the NSM 2025 argues for introduction of stronger measures aiming at a better protection of various elements of infrastructure (fiber optic cables, power lines, transport hubs, communication infrastructure and subsea infrastructure) as well as at increasing the level of its resilience. In addition, NSM 2025

recommends prioritizing backup solutions and resilience, monitoring and detection measures, and practicing contingency plans. The NSM 2025 calls also for a greater awareness concerning risks and threats related to access to sensitive infrastructure-related information through insiders having access to this type of information (p.17), as well as challenges related to access to critical infrastructure via cyberspace (p.26).

Concerning energy, the NSM 2025 mentions energy 3 times. It underlines the importance of Norwegian energy supplies to Europe (p.8), identifies Norwegian energy infrastructure as a potential target of sabotage operations (p.14) and makes a reference to the U.S. energy sector as a target of malign operations (p.15).

Evolution of the official threat landscape in Norway 2022-2025

In this section on the evolution of the threat landscape in Norway between 2022 and 2025 the focus is on how questions related to infrastructure and broadly understood energy sector have been framed in the official Norwegian threat assessments published in this period. Because the main question this study seeks to address is the Norwegian understanding of threats to be addressed in connection with the operations of the Norwegian energy sector and infrastructure, this quantitative examination presents how these issues are present in the official threat assessments. This is done in the following way. First, terms related to infrastructure and energy sector are identified and searches in the set of official documents are conducted to map the interest in these issues as represented in this set of official threat assessments. Second, terms describing threats that can be posed to infrastructure and energy sector are identified and searches for these terms conducted. Third, we map what actors are identified in this set of threat assessments as posing the most serious challenge to Norway's security interests, focusing on the perceptions of Russia and China in this security context.

This section focuses on the quantitative and qualitative examination of official PST threat[32] and NSM risk assessments[33] as the most important documents dealing with these questions in the

[32] The whole set of PST threat assessments is available here: https://pst.no/alle-artikler/?FilterByValues=8&v=1640709241297&PageNumber=1

[33] NSM risk assessments are available here: https://nsm.no/regelverk-og-hjelp/rapporter/

national context, but in the quantitative presentation (**Figure 1**) we also add how these issues are dealt with in the NIS threat assessments[34] in this period.

Already in 2020, two years before the Russian full-scale invasion of Ukraine, PST published a brief assessment of threats to the Norwegian petroleum sector posed by the activity of foreign intelligence organisations.[35] According to this document the Norwegian petroleum sector was at that time exposed to intelligence activity. The targets included both public and private companies, technology environments at universities and research institutes, and Norwegian authorities. Intelligence services from Russia, China and other countries were supposed to collect information about the Norwegian petroleum sector, including about petroleum technology, Norwegian authorities' strategies and positions, and economic conditions. There were several types of threats actors in the Norwegian petroleum sector had to be aware of. First, people working with or having contacts within oil and gas policy, could be approached and attempted to be recruited by other countries' intelligence services at conferences and trade fairs or in connection with foreign travel or stationing abroad. Second, the Norwegian petroleum sector was also exposed to network operations – for instance in 2014, more than 50 Norwegian oil and gas companies, as well as the Ministry of Petroleum and Energy and Oil Directorate, were exposed to a major network attack. Third, other countries' intelligence services were also involved in mapping petroleum infrastructure in Norway, including undersea oil and gas pipelines, onshore facilities (e.g. processing plants or refineries), landfall sites and other petroleum installations.

The operations conducted by foreign intelligence services against the Norwegian petroleum sector before the outbreak of the war in 2022 could improve the military capabilities of other countries and weaken Norway's resilience. In addition, this could also have negative economic implications for Norway and undermine the Norwegian companies' ability to compete with other actors. In the worst-case scenario such an activity could also facilitate conducting sabotage operations against this most important sector of the country's economy.

In its 2022 threat assessment PST listed several technologies that can be interesting for foreign intelligence actors to get better access to. Examples of technology areas that may be exposed

---

[34] NIS threat assessments are available here: https://www.etterretningstjenesten.no/publikasjoner/fokus

[35] PST. (2020). Etterretningstrusselen mot norsk petroleumssektor https://www.pst.no/globalassets/eldre/2020/etterretningstrusselen-mot-norsk-petroleumssektor.pdf.

to covert and overt procurement activities included in this assessment sensor and detection technology, marine and underwater technology, oil and gas technology, semiconductor technology, space and satellite technology, drone technology, laboratory and manufacturing technology and communications technology

According to the 2022 assessment several countries were seeking access to information about Norwegian decision-making processes. Businesses that work with Norwegian foreign, defence and security policy were identified as particularly vulnerable to network operations. The same applied to companies and research environments within defence, health and maritime technology. The petroleum and space sectors should also be prepared for unauthorized parties to attempt to steal information from their computer networks.

The 2023 PST threat assessment repeated to a very large extent these warnings. It argued that attempts at getting access to sensitive information through procurement of assets could cover a number of fields of technology, including sensor and detection technology, maritime technology, semi-conductor technology, space and satellite technology, as well as drone and communication technology. In 2023 PST argued that it was unlikely that Russia would carry out a sabotage operation on Norwegian territory in 2023. However, acts of sabotage could become a more relevant scenario if Russia's willingness to escalate the conflict with NATO and the West were to increase. In 2023 PST considered the petroleum sector to be a particularly vulnerable target but other critical functions could also be targeted, including infrastructure associated with the power sector or the e-communications sector.

The 2024 PST threat assessment singled out businesses related to Norwegian oil and gas activities as particularly vulnerable because Norway had become a more central energy supplier to Europe after the war of aggression against Ukraine. It was also underlined that Russia considered the use of energy-related instruments as a central element of sowing discord in the West. The same document described activities related to Norwegian gas exports or military contributions to Ukraine to be most vulnerable to possible sabotage actions. The purpose of such actions against targets related to Norwegian gas exports could trigger or intensify an energy crisis in Europe. Russia's overall objective in such a case may be to create a reduced willingness to continue military support for Ukraine.

This document listed also organisations most exposed to cyber threats, including organisations operating in finance, health, research and education, space, technology, telecommunications, logistics and transport, energy and the maritime sectors.

NSM 2022 mentions infrastructure 7 times. It describes data centers and telecommunications infrastructure, which are dependent on power, to be the key elements of national digital infrastructure. It also adds that any failures in value chains, including digital ones, can have consequences for both societal security and national security, for example if civilian services or deliveries to the Armed Forces were to cease. It also underlines that these important functions must be available in peace, crisis and war (p.9).

This document lists power supply, telecommunications infrastructure, healthcare and food supply as sectors that can be exposed to digital blackmail and sabotage. It also mentions other types of threats related to infrastructure, such as cyber-attacks, acquisitions, influence operations or the use of ships for mapping Norway's undersea infrastructure (p.17-19).

NSM 2023 report on risks was the first one published after the outbreak of the full-scale war against Ukraine. This was also reflected clearly in the assessment of risks that the Norwegian society could face in this changing situation. The document mentioned infrastructure 16 times and warned that threat actors use a variety of tools to advance their interests. Sabotage against the Nord Stream pipelines in the Baltic Sea was mentioned as an example, but references were also made to high levels of reconnaissance activity aimed at critical Norwegian infrastructure, and several cases of serious insider trading as other examples (p.9).

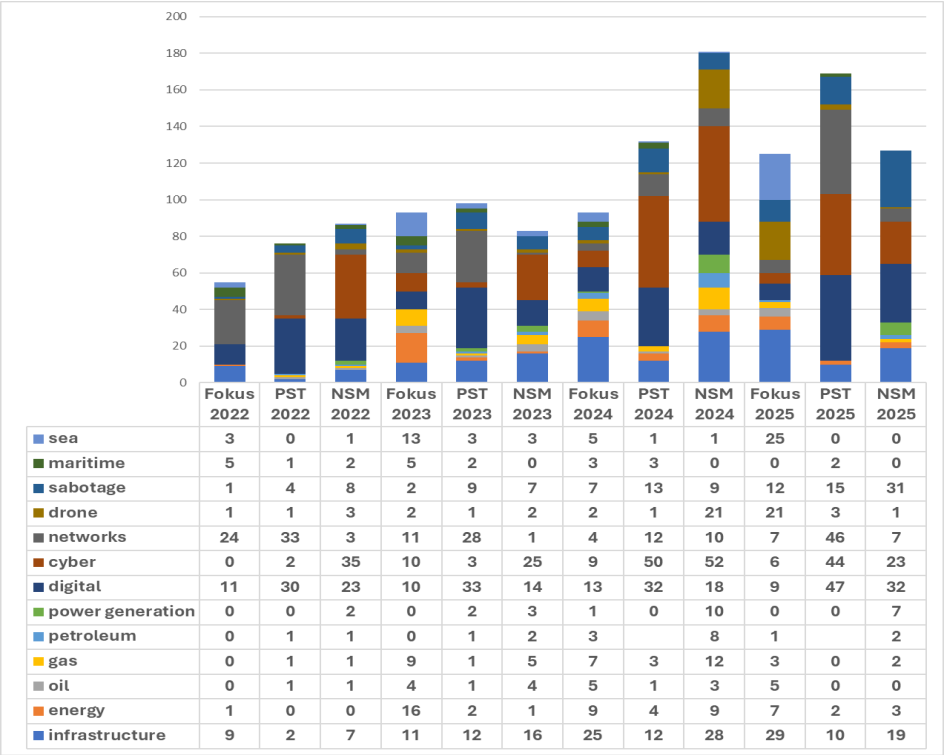
This document stated that the importance of the fundamental national functions was constantly changing. In a situation when disruptions to Norwegian oil and gas exports to Europe could increase, an acceptable level of security in the sector must be established in light of this. This was also one of the reasons why in 2022 the Armed Forces were deployed to secure civilian infrastructure. Fighter aircraft and Navy vessels were sent to patrol and demonstrate their presence around oil and gas installations, while Home Guard soldiers assisted with guarding onshore facilities in a situation when the need for protection increased because of the Russian aggressive policy (p.11). Describing the changing security situation in Europe this document also underlined the increased role Norwegian gas supplies played in securing access of European customers to needed energy in a situation when Russian gas supplies were no longer available. According to this risk assessment Norwegian gas infrastructure could be therefore

exposed to various types of risks and threats (p.11). This document paid also increased attention to the need to protect sensitive information related to oil sector and various types of technology and elements of critical infrastructure (p.36).

NSM 2024 report mentioned infrastructure-related issues 28 times and called for paying greater attention to questions related to protection of various elements of critical infrastructure. The document argued that critical infrastructure must be shielded from scrutiny and influence. It described both foreign acquisitions and investments in Norwegian companies and procurements as posing a risk to national security. It mentioned that imported technology may be equipped with hidden backdoors or vulnerabilities that can be exploited and that this could have serious consequences for national security. The overall national dependence on countries that pose a security threat to Norway is a significant vulnerability for national security interests (p.8). This document identified several risks to critical infrastructure, including risks related to insiders who could have access to sensitive information (p.26-27), drones (p.29) or cyber-attacks (31-32).

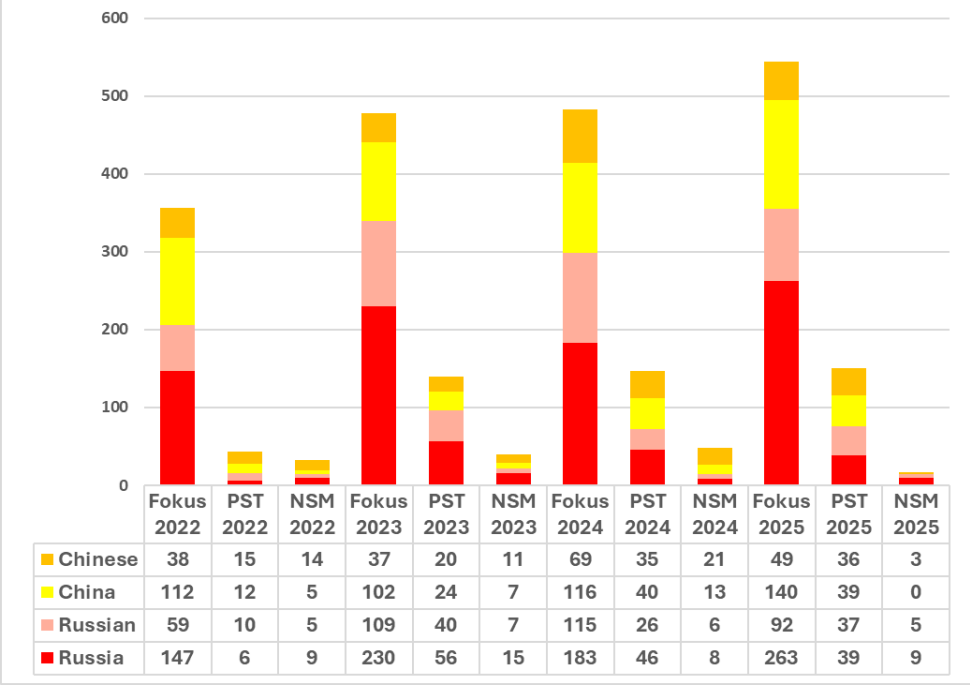
Petroleum sector is mentioned in this document 8 times. The importance of the Norwegian oil and gas sector is linked to the conflict developing in the Middle East that had made the Norwegian supplies of energy to Europe even more important (p.10). It also defined the possible exposure of the Norwegian petroleum sector (oil and gas) to cyber-attacks as a serious risk (p.31). In general, more attention was paid to the situation in the Norwegian gas sector as gas and risks related to gas sector were mentioned in this document 12 times.

Figure 1. Evolution of the official threat landscape in Norway 2022-2025 – number of mentions of terms in official threat assessments.



	Fokus 2022	PST 2022	NSM 2022	Fokus 2023	PST 2023	NSM 2023	Fokus 2024	PST 2024	NSM 2024	Fokus 2025	PST 2025	NSM 2025
sea	3	0	1	13	3	3	5	1	1	25	0	0
maritime	5	1	2	5	2	0	3	3	0	0	2	0
sabotage	1	4	8	2	9	7	7	13	9	12	15	31
drone	1	1	3	2	1	2	2	1	21	21	3	1
networks	24	33	3	11	28	1	4	12	10	7	46	7
cyber	0	2	35	10	3	25	9	50	52	6	44	23
digital	11	30	23	10	33	14	13	32	18	9	47	32
power generation	0	0	2	0	2	3	1	0	10	0	0	7
petroleum	0	1	1	0	1	2	3		8	1		2
gas	0	1	1	9	1	5	7	3	12	3	0	2
oil	0	1	1	4	1	4	5	1	3	5	0	0
energy	1	0	0	16	2	1	9	4	9	7	2	3
infrastructure	9	2	7	11	12	16	25	12	28	29	10	19

Figure 2. Mentions of Russia and China in Norwegian threat assessments 2022-2025



	Fokus 2022	PST 2022	NSM 2022	Fokus 2023	PST 2023	NSM 2023	Fokus 2024	PST 2024	NSM 2024	Fokus 2025	PST 2025	NSM 2025
Chinese	38	15	14	37	20	11	69	35	21	49	36	3
China	112	12	5	102	24	7	116	40	13	140	39	0
Russian	59	10	5	109	40	7	115	26	6	92	37	5
Russia	147	6	9	230	56	15	183	46	8	263	39	9

What this brief examination of the official Norwegian threat assessments focusing on the role of infrastructure and energy in this context can tell us about official interest and perceptions? What is obvious is the growing focus on questions related to infrastructure that have over the past four years received more attention in all official threat assessments as demonstrated in Figure 1. It is also obvious that questions related to challenges in the digital and cyber space are high on the Norwegian threat agenda as those are among the most often mentioned issues in all threat assessments. What is however still relatively surprising is the relatively low interest in questions related to energy sector, which is the most important sector not only of the country's economy, but also in the broader European context because of the growing dependence of Europe on energy – and especially gas – supplies from Norway. National power supply, transport of gas in pipes to Europe, control of petroleum extraction on the Norwegian continental shelf as well as ensuring that the Armed Forces and pre-designated critical users have access to sufficient fuel supplies are defined by the National Security Authority NSM as basic national functions[36], and one should therefore expect more attention to be paid to issues related to protection of various elements of critical energy infrastructure.

While the qualitative examination of the evolution of the threat landscape in Norway poses several practical challenges, the picture of who is considered to pose the most serious challenge in this context is relatively clear as both Russia and China are named as actors causing the most trouble in the evolving threat landscape as demonstrated in Figure 2.

6. Conclusion

The aim of this brief study was to map actual and potential risks, challenges and threats to maritime security in the Black Sea region where the situation is strongly influenced by the ongoing conflict in Ukraine. Russian aggression against Ukraine that started in 2014 and escalated in 2022 has changed many security parameters in the region. The situation of all actors operating in the region has been influenced negatively by the ongoing conflict, creating a situation characterized by the high level of unpredictability and insecurity. At the same time there are some plans to develop new energy projects in the region and there was therefore a burning need to present a realistic assessment of what types of risks, challenges and threats those who

[36] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/grunnleggende-nasjonale-funksjoner/oversikt-over-innmeldte-grunnleggende-nasjonale-funksjoner/

consider embarking on such offshore energy projects will have to deal with. This study aimed to provide some informed answers to these questions by examining how questions related to protection of the existing – and future – infrastructure are addressed in the national threat assessments in the region. In addition, this study also presents how questions related to protection of infrastructure, including maritime energy infrastructure, are dealt with in Norway that has a long experience from addressing this type of challenges not only in the peace time, but also during the ongoing conflict in Ukraine in which Norway has taken a clear stance showing solidarity with Ukraine.

After having examined these important questions, the authors of this study want also to present some policy-relevant conclusions on how the approach to those questions can be improved at both national and international levels. We argue that the following steps should be taken:

- Situational awareness is crucial for efficient policy- and decision-making. Good situational awareness is necessary for authorities and enterprises to be able to meet future security challenges with adequate security measures. The key element is sufficient knowledge of the current threat landscape in the international environment in which security policies are developed and implemented. A good understanding of what must be protected against various types of malign influence and identification of own vulnerabilities that can be exploited by various types of threat actors are of crucial importance.

- Because all countries must address risks, challenges and threats stemming from both external and internal arenas, a better situational awareness can be achieved by strengthening international cooperation on these issues, especially within institutions that play a crucial part in shaping security in Europe. Cooperation within NATO and the EU – and between those two – should be therefore promoted as the best way of addressing various types risks, challenges and threats all member states must deal with.

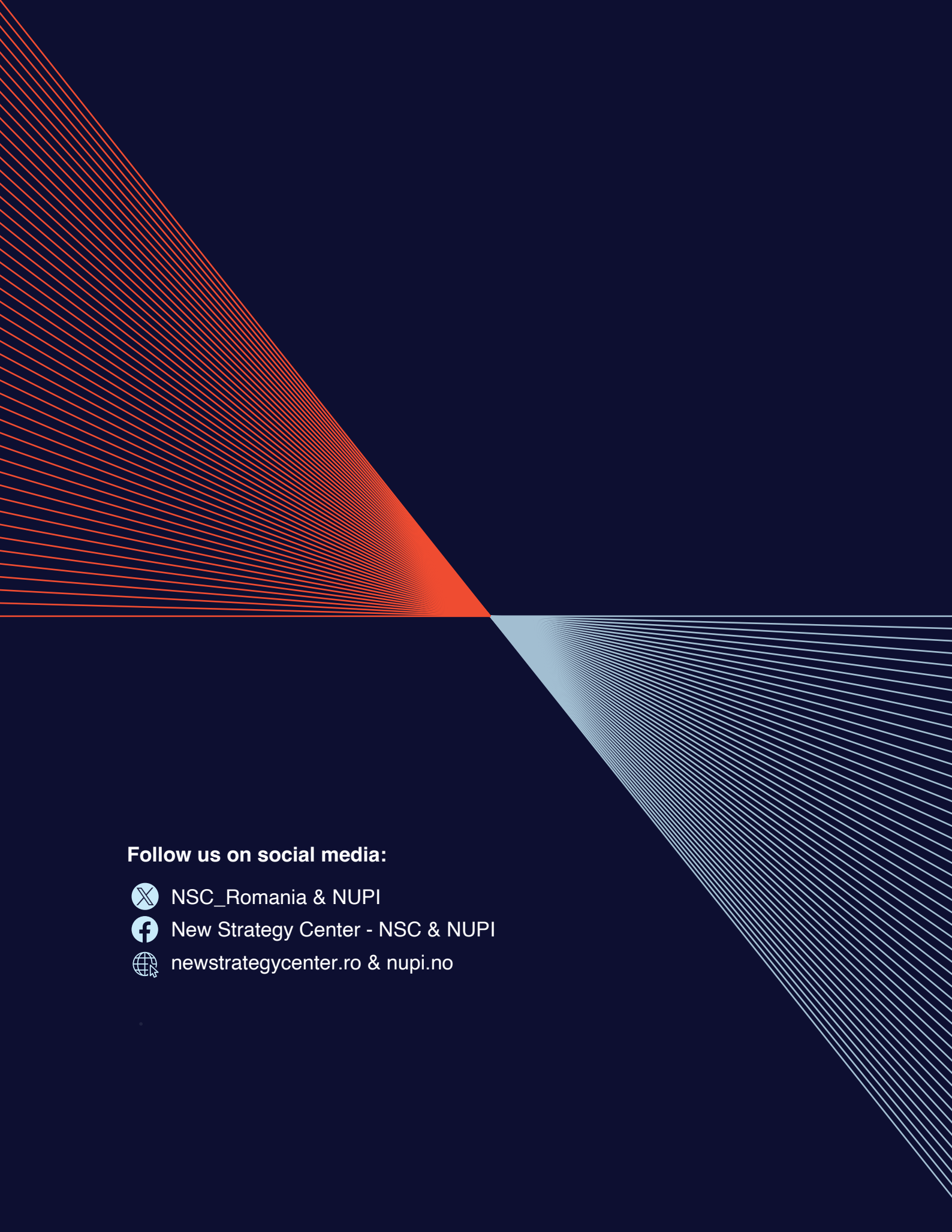
- At the national level it is crucial to improve situational awareness by regularly producing open national threat assessments that would make policymakers and societies better prepared to meet security risks, challenges and threats identified by specialized national authorities.

- There is an obvious need to strengthen regional cooperation on protection of critical infrastructure: in the Black Sea region expanding Turkish-Romanian-Bulgarian cooperation on protection of critical infrastructure situated in EEZ should be promoted, but other forms of regional cooperation, based on the same model as the newly established cooperation in the North Sea region could also be considered.

- Question of maintaining freedom of navigation in the Black Sea should be considered a top priority once the kinetic phase of the conflict in Ukraine is over. It is important to strengthen cooperation on these questions involving NATO, the EU, the UK, the USA and countries from the region to limit negative Chinese, Russian and Iranian influence.

- Securing stability in the Black Sea region through improving protection of critical infrastructure will contribute to the reconstruction of Ukraine by enabling the exploitation of resources, which will most probably imply construction of additional elements of critical infrastructure to be protected in the region.

- Cooperation between North, Baltic and Black Sea Allies should be strengthened to make all of them better prepared to tackle various risks and threats along the Eastern EU and NATO flank. Special attention should be given to what Russia could try to achieve by implementing various types of measures from its hybrid repertoire after the end of the kinetic phase of the conflict in Ukraine.



Follow us on social media:

NSC_Romania & NUPI

New Strategy Center - NSC & NUPI

newstrategycenter.ro & nupi.no