Information & Security

N. Dimitrov & K. Karakolev
vol. 55, no. 2 (2024): 133-148
https://doi.org/10.11610/isij.5566

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Seabed Critical Infrastructures

Nedko Dimitrov (✉) ***and Kalin Karakolev***

Nikola Vaptsarov Naval Academy, Varna, Bulgaria,
http://naval-acad.bg

ABSTRACT:

The article presents a study in the area of critical infrastructure protection based on the fact that maritime areas include critical assets which functionality appears to be very important in the modern security environment. The objective of the study is to recognise such seabed critical infrastructures in the scope of Bulgarian territorial waters and to analyse their security having legal, procedural, and technological considerations for the security system and identifying the rapidly evolving threats in the Black Sea region.

The article is structured in the same logical way, resulting in multifactor analysis and classification. The main findings are based on the understanding that critical infrastructures resilience is achieved by continuity of operation and their physical security, and both of them can be controlled properly by applying a risk management approach in line with the national particularities. The specifics in the maritime domain determine a specific security environment that can be used successfully for offensive and defensive actions.

ARTICLE INFO:

RECEIVED: 05 SEP 2024
REVISED: 18 OCT 2024
ONLINE: 31 OCT 2024

KEYWORDS:

seabed critical infrastructures, protection, security measures, surveillance systems, autonomous systems

Introduction

Globalization has significantly expanded maritime trade, which has consequently increased the importance of critical maritime infrastructures. These infrastructures, particularly those located on the seabed, have become increasingly attractive targets for disruption. The strategic relevance of seabed infrastructures became especially clear during World War II when the United Kingdom gained a significant advantage by cutting off Nazi Germany's submarine communications. More recently, the attacks on the Nord Stream gas pipeline in

✉ E-mail: n.dimitrov@nvna.eu

September 2022 brought global attention to the vulnerabilities of seabed critical infrastructure.

In this sense, Seabed Critical Infrastructure (SCI) refers to essential structures and systems situated on or beneath the ocean floor that are crucial for a variety of operations, including communication, energy production, transportation, and defence. These infrastructures are vital to the functioning of modern society and the global economy. Key components of seabed infrastructure include submarine cables, which transmit approximately 99 % of international communications, making them indispensable for global connectivity. Additionally, power cables are used to transmit electricity across water bodies, connecting electrical networks between countries. Other critical elements include oil and gas pipelines and offshore renewable energy installations (e.g., wind farms and tidal systems), representing an important part of the global energy supply chain, especially in regions such as the North Sea, the Gulf of Mexico, and the Persian Gulf and marine research and defence facilities, such as underwater surveillance systems and underwater communication systems and transport infrastructure, including underwater tunnels and bridge reinforcement.

The rapid proliferation of underwater technologies, such as autonomous and remotely operated devices capable of complex operations at extreme depths, has transformed seabed activities. While these technologies offer enhanced defensive capabilities, they also introduce vulnerabilities that could be exploited by malicious actors. The concept of "War on the seabed" is no longer a distant concept: it poses an immediate and legitimate threat to the Allies.[1] In light of these emerging threats, developing a robust protection system for seabed critical infrastructures is essential. Such a system must encompass a comprehensive approach to prevention, early warning, and effective countermeasures to neutralize the impact of risks and threats.

Methods

This study employs a multifaceted methodological framework, beginning with a complex systems approach, which has been successfully applied in prior analyses of critical infrastructures at the Naval Academy and has proven to be the best one when it comes to the national security system.[2] This approach facilitates a holistic examination of the various factors influencing the infrastructure and emphasizes system classification and organization of the analyzed objects and their interrelations.

Specific methods used in this analysis include:

- detailed description and classification – a comprehensive description and classification of the elements within the critical infrastructure system, identifying key components for further analysis.
- selection of typical elements – selection of representative elements from the defined system for a more focused and in-depth analysis.

- synthesis – the synthesis of data gathered from multiple sources to derive new insights into the protection and security of seabed critical infrastructures.

These methods are applied in accordance with the steps outlined in the ISO 31000 risk management process, ensuring a standardized approach to the identification, evaluation, and mitigation of risks. The selection of methodologies is informed by analogous studies in the field of critical infrastructure security, ensuring the applicability and relevance of the chosen techniques.

1. Seabed Critical Infrastructure Elements

To construct an effective protection system for seabed critical infrastructure, it is imperative to analyze the physical characteristics of the infrastructure, define its legal framework, conduct a thorough risk assessment, and propose preventive measures. For the purposes of this study, the object of analysis is a critical infrastructure component within the Bulgarian coastline: a natural gas platform and its associated pipeline.

1.1. Physical Characteristics

The physical characteristics of seabed infrastructure are diverse and include elements such as seabed topography, geology, bathymetry, hydrodynamic conditions, and biological factors. These characteristics play a crucial role in the design, installation, and operation of critical infrastructures like offshore wind farms, oil and gas platforms, undersea cables, and pipelines.

The case study focuses on the Galata Gas Platform, a natural gas production facility located approximately 20 to 25 kilometers off the Bulgarian coast in the Black Sea. This platform operates in shallow waters, with depths ranging from 30 to 40 meters, and is connected to a network of underwater pipelines that transport natural gas to onshore facilities. The platform itself is a fixed offshore installation, anchored to the seabed and equipped with various safety systems to ensure the protection of both personnel and the environment.

The subsea pipeline, stretching approximately 23 kilometers, is made of corrosion-resistant carbon steel and designed to withstand the challenging conditions of the marine environment, including pressure, temperature fluctuations, and potential physical impacts. Both the platform and the pipeline adhere to strict environmental regulations to mitigate their impact on marine ecosystems.

The seabed near the Galata Gas Platform is generally flat or has gentle slopes and includes features such as sand waves, ripples, and sediment drifts formed by underwater currents. The hydrodynamic conditions are characterized by moderate currents and wave activity with minimal tidal effects. The bathymetry of the area shows a shallow to moderate depth suitable for offshore gas extraction activities. The geology is shaped by both regional and local geological processes and characterized by thick sedimentary sequences, primarily composed of clay, silt, and sand layers.[3]

These characteristics provide an overview of the physical attributes of the Galata Gas Platform and its associated pipeline, which are integral components of Bulgaria's offshore gas production infrastructure.

1.2. The Legal Status of the Seabed and Its Resources

The legal framework governing seabed resources is complex and varies depending on whether the activities occur within a coastal state's Exclusive Economic Zone (EEZ) or in international waters, often referred to as 'the Area,' which lies beyond national jurisdictions. Seabed mining in international waters is regulated by the United Nations Convention on the Law of the Sea (UNCLOS),[4] specifically through the Mining Codes and the International Seabed Authority (ISA). Conversely, seabed activities within a country's EEZ are governed by that country's domestic law. The international seabed area, or 'the Area,' covers approximately 260 million square kilometres, while 85 million square kilometres of the ocean falls within EEZs. Under UNCLOS, coastal states have sovereign rights over the exploration and exploitation of natural resources within their EEZs, which typically extend 200 nautical miles (370 km) from shore. Maritime boundaries between states are generally established through bilateral negotiations or, in some cases, with the assistance of independent judicial bodies. UNCLOS confers coastal states with a broad range of rights and responsibilities within their EEZs, including the management of living resources, enforcement of fisheries management, and exploitation of non-living resources, such as hydrocarbons and minerals. Additionally, it regulates marine scientific research, the protection and preservation of the marine environment, and the production of energy from currents and winds. This includes the seabed, subsoil and water column.[5]

The Galata Gas Platform and its associated pipeline are located within Bulgarian territorial waters and the contiguous zone of the Black Sea. The legal regime governing such installations is shaped by a combination of international agreements, European Union (EU) directives, and Bulgarian national legislation.

In accordance with International Legal Framework, Bulgaria's rights to explore and exploit marine resources are derived primarily from UNCLOS, which provides the legal foundation for Bulgaria's activities in the Black Sea. Additionally, the International Maritime Organization (IMO), a specialized United Nations agency, plays a crucial role in regulating shipping and ensuring that offshore platforms meet international safety and environmental standards. Notable IMO conventions relevant to offshore platforms include the MARPOL Convention, which focuses on preventing pollution from ships and other maritime installations.

As a member state of the European Union, Bulgaria is required to comply with a range of EU directives that pertain to offshore oil and gas operations. Directive 2013/30/EU on Safety of Offshore Oil and Gas Operations [21] seeks to reduce the risk of major accidents related to offshore oil and gas activities by establishing minimum safety requirements and limiting their consequences for human health and the environment. Marine Strategy Framework Directive

2008/56/EC mandates that EU member states work to achieve good environmental status in their marine waters [6] and Environmental Impact Assessment Directive 2014/52/EU requires member states to assess the environmental impacts of certain public and private projects, including offshore installations like the Galata Gas Platform.[7]

Bulgaria's national legislation has provided specific rules and regulations and has implemented a comprehensive legal framework to govern the exploration, development, and exploitation of its offshore oil and gas resources. The Energy Act is a fundamental piece of legislation governing energy policy in Bulgaria, including provisions related to the exploration and extraction of natural gas and other hydrocarbons. It establishes the licensing regime for such activities and the roles of different state agencies.

The Subsurface Resources Act regulates the prospecting, exploration, extraction, and conservation of subsurface resources, including natural gas. It defines the legal regime for concessions, sets out environmental and safety standards, and outlines the rights and obligations of operators.

The Environmental Protection Act provides the legal framework for environmental protection in Bulgaria, including requirements for environmental impact assessments (EIAs) for projects like the Galata Gas Platform. Operators must ensure compliance with national environmental standards and regulations.

Maritime Spaces, Inland Waterways, and Ports Act governs the use and management of Bulgaria's maritime spaces and ports, providing regulations relevant to offshore installations and ensuring that activities comply with maritime spatial planning. Several Bulgarian authorities oversee the regulation of offshore oil and gas activities:

- Ministry of Energy is responsible for policy development, issuing exploration and production licenses, and overall energy strategy;
- Ministry of Environment and Water ensures compliance with environmental legislation, including EIAs and environmental permits;
- Executive Agency for Exploration and Maintenance of the Danube River is involved in regulating maritime navigation and safety;
- Bulgarian Maritime Administration oversees maritime safety and security, including the regulation of offshore platforms.

In conclusion, the legal framework surrounding the Galata Gas Platform is composed of multiple layers of governance, combining international, European, and national regulations. This comprehensive framework ensures the safe, environmentally responsible, and economically efficient operation of offshore gas production. By complying with UNCLOS, EU directives, and national legislation, the platform benefits from robust legal protections while minimizing its environmental impact and ensuring the security of the infrastructure.

2. Model of Seabed Critical Infrastructure Elements Protection

Seabed critical infrastructure includes vital underwater installations and assets such as subsea cables, oil and gas pipelines, data transmission systems, offshore

drilling platforms, and subsea sensors. These infrastructures are integral to global communications, energy supply, and national security. However, they face a range of threats, from natural disasters to deliberate attacks, with potentially significant geopolitical, economic, and environmental consequences. Seabed critical infrastructure vulnerabilities can be categorized into two main types – intentional and unintentional. Unintentional threats to seabed infrastructure are pervasive and arise from both natural and human sources. Natural events like earthquakes, tsunamis, landslides, and volcanic activity are unpredictable but have the potential for widespread disruption, while human activities, particularly fishing, shipping, and offshore development, represent more localized yet frequent risks. While unintentional threats to seabed infrastructure often dominate the conversation, intentional threats — including sabotage, espionage, and cyberattacks — are emerging as critical concerns for governments and industries alike. Intentional attacks on seabed infrastructure can disrupt global communication, energy supplies, and even military operations, making them attractive targets for state and non-state actors. In addition, increasing digital control over subsea infrastructure, such as remotely operated vehicles (ROVs) and automated monitoring systems, exposes these assets to cyber-attacks. Malicious actors can exploit vulnerabilities in control systems to manipulate or shut down operations.

To effectively safeguard seabed critical infrastructure, a comprehensive protection system must be established. This system should encompass early detection, threat prevention, and countermeasures application against potential risks. Protection should be organized to ensure safety from both intentional and unintentional threats. Key elements of this protection model include:

The model protection of the physical part of the seabed critical infrastructure object is organized in order to ensure safety and security from the impact of intentional and unintentional attacks and is achieved by solving the following tasks:

- timely detection and notification of the danger – the system must provide timely detection of threats or security breaches, coupled with a reliable notification mechanism to alert relevant authorities;
- apprehending or neutralization of threat actors – identified security violators should be swiftly apprehended or neutralized to prevent further damage to critical infrastructure;
- preventing intruder penetration – measures must be in place to prevent unauthorized access to protected areas and to mitigate the effectiveness of any breaches that do occur;
- mitigating consequences – the system should also include strategies for minimizing the impact of attacks or accidents and ensuring a quick return to normal operations.

The construction of an effective defence system for seabed critical infrastructure is guided by the following principles: [8]

- Zonal, Zonal-Object, and Object Protection – protection strategies should be layered, ensuring that each zone or object within the critical infrastructure system is adequately secured.
- Distribution of Responsibilities – the responsibilities for protection should be distributed among operators of maritime critical infrastructure and the authorities responsible for safeguarding national sovereignty.
- Interaction of Forces – a coordinated approach between infrastructure operators and national security forces is essential for comprehensive protection.
- Centralized Management – the protection system must be managed centrally, with clear communication and coordination between local, regional, and national authorities.

2.1. Key Aspects of Protecting a Seabed Critical Infrastructure Object

The protection of seabed critical infrastructure (SCI), such as the Galata Gas Platform and its associated pipeline, requires a comprehensive approach that integrates physical security measures, advanced technological systems, and stringent operational protocols. These protective strategies must be designed to mitigate threats arising from natural hazards, accidental damage, and deliberate actions.

The Layered Defence Approach is a multi-tiered strategy designed to protect seabed critical infrastructure by integrating different protective measures at various levels—physical, technological, operational, and legal. This approach provides resilience by addressing both external and internal threats through a combination of prevention, detection, response, and recovery strategies. Each layer works independently while reinforcing the others, ensuring that no single failure leads to a catastrophic outcome.

2.1.1. Physical Protection Layer

The physical protection layer involves the design and engineering of infrastructure to prevent damage from both natural and human-induced threats. This includes:

- Burial and Trenching – burying cables and pipelines beneath the seabed is one of the most effective ways to protect them from accidental damage (e.g., fishing trawlers, anchors) and some natural disasters. Research by Alcatel Submarine Networks (ASN) suggests that cables buried to a depth of 1.5 to 3 meters have significantly reduced the number of incidents involving fishing trawlers and anchors.[9]
- Protective sheathing and materials – applying protective coatings or sheathing to cables and pipelines provides an additional layer of defence. Sheathing materials such as polyethylene or polyurethane are used to protect cables from corrosion and abrasion, while metal armouring can provide resistance to physical impact. Pipelines are often coated with anti-cor-

rosion materials (e.g. pipeline of the Galata Gas Platform, is made of corrosion-resistant carbon steel [3] and concrete weight coatings that help stabilize them on the seabed and prevent mechanical damage.

- Rock dumping and Concrete mattering - perimeter fencing and barriers around sensitive areas on the object in order to prevent unauthorized access. In highly dynamic areas, such as the Strait of Gibraltar, rock dumping has been utilized to create a durable protective layer over critical pipelines and cables.[10]

2.1.2. Technological Protection Layer

This layer focuses on advanced technology to monitor, detect, and respond to threats, both physical and cyber-related.

- Monitoring and Surveillance Systems – constant monitoring of infrastructure is critical to detect potential threats or damages before they escalate. There are a variety of assets that can include Autonomous Underwater Vehicles (AUVs) performing regular patrols and visual and acoustic inspections,[11] Unmanned Surface Vehicles (USVs) providing surface monitoring and detecting nearby vessels or activities that may endanger the infrastructure, Subsea Sensors detecting abnormal activities such as pressure changes, physical impacts, or nearby vessel movements [12] and Satellite Surveillance (e.g. Synthetic Aperture Radar) monitoring vast ocean areas, detecting ships and large-scale events such as oil spills or explosions.
- Cybersecurity for Control Systems – many subsea infrastructures, particularly pipelines and energy platforms, are monitored and controlled remotely through Supervisory Control and Data Acquisition (SCADA) systems.[13] Sensitive data exchanged between control systems and operational sites should be encrypted to prevent interception or tampering. Intrusion Detection Systems (IDS) monitor network traffic for suspicious activities, issuing alerts if potential breaches are detected. Critical control systems should be isolated from general IT networks using firewalls and network segmentation to prevent attackers from accessing operational controls. Artificial intelligence (AI) can be deployed to detect anomalies in system behaviour that could indicate a potential cyberattack, enabling proactive responses.
- Predictive Maintenance and AI Systems use AI and machine learning algorithms to monitor the condition of infrastructure and predict failures before they occur, ensuring timely maintenance. Sensors embedded in pipelines and cables collect data on pressure, vibration, temperature, and movement. AI algorithms are applied to analyse this data to predict failures or vulnerabilities.[14]

2.1.3. Operational and Procedural Layer

This layer emphasizes efficient procedures, coordination, and response mechanisms to protect seabed infrastructure and ensure swift recovery in case of an

incident. Operational protocols include development of variety of procedures that legalize all protection activity and establish organization and preparation of all assets involved in protection system.

- Incident Response Protocols – establishment of a robust framework for responding to any threat or damage to seabed infrastructure and consist of:
  - Real-time Alerts – monitoring systems are integrated with early warning systems that notify operators of any unusual activity or damage in real-time;
  - Response Teams – trained rapid-response teams (involving divers, ROVs, and specialized repair vessels) are dispatched to assess and repair damaged infrastructure;
  - Naval and Coast Guard Support – governments can deploy naval and coast guard resources to assist in securing the area if a threat is detected, ensuring the safety of the infrastructure and repair crews.

Multi-agency collaboration, combining governmental, military, and private sector capabilities, is critical for the immediate deployment of rapid-response teams when infrastructure is threatened. Case studies from Norway's oil and gas sector demonstrate effective coordination between public and private actors to respond swiftly to infrastructure breaches.[15]

- Redundant Systems and Contingency Planning [16] – redundancy is critical to ensuring the continuity of service even if part of the infrastructure is damaged. Seabed communication networks often have multiple parallel cables so that data can be rerouted in case one is damaged. Redundancy reduces the risk of widespread service outages. Comprehensive contingency plans ensure that there are pre-established procedures for rerouting communication traffic or energy supplies in case of infrastructure failure. Backup power and control systems should be in place for critical offshore platforms.

2.1.4. Legal, Regulatory, and International Cooperation Layer

This final layer addresses the need for a strong legal and cooperative framework to protect seabed infrastructure, which often crosses national boundaries and involves multiple stakeholders.

- *International Legal Framework*. International laws provide the foundation for protecting seabed infrastructure, particularly in international waters. The United Nations Convention on the Law of the Sea (UNCLOS) [22] establishes rules for the placement of infrastructure in international waters and defines countries' responsibilities for maintaining and protecting it.[4] International Maritime Organization (IMO) provides guidelines to prevent accidental damage to seabed infrastructure, particularly from ships and maritime activities.
- *National Legislation and Policies*. National governments are responsible for protecting critical infrastructure within their exclusive economic zones

(EEZs) and ensuring compliance with international regulations. Many nations have adopted Maritime Domain Awareness (MDA) policies that combine intelligence, surveillance, and reconnaissance to protect their maritime interests, including seabed infrastructure. Governments implement laws regulating ship movements, fishing activities, and anchoring practices in areas where subsea cables and pipelines are laid to prevent accidental damage. For example, the United Kingdom's 2020 Maritime Security Strategy integrates intelligence sharing, public-private partnerships, and enforcement measures to protect vital seabed infrastructure in the North Sea, where offshore energy and communication cables are particularly vulnerable.[17]

- *International Cooperation and Information Sharing*. Many seabed cables and pipelines traverse international boundaries, requiring cooperation between nations to ensure their protection and include:
  - cross-border agreements - countries sharing maritime regions (e.g., the North Sea or Mediterranean) often sign agreements to collectively protect and maintain shared infrastructure;
  - shared surveillance systems - neighbouring countries might collaborate on deploying shared satellite or radar surveillance systems to monitor seabed infrastructure for suspicious activities or threats.

A 2019 report by NATO's Centre of Excellence for Operations in Confined and Shallow Waters highlights the growing role of international cooperation in protecting shared infrastructure. Information-sharing initiatives, such as NATO's Multinational Submarine Cable Protection Initiative, promote cross-border surveillance and rapid response capabilities.[18]

As key advantages of the Layered Defence Approach can be defined:

- resilience and redundancy - by combining multiple layers of defence, the system can withstand failures in one area (e.g., physical damage) without causing total system failure. For example, if a cable is damaged, traffic can be rerouted while repairs are made;
- comprehensive protection – each layer addresses different threat vectors (physical, cyber, operational, and legal), ensuring that all potential risks are accounted for and mitigated.
- scalability - the model can be scaled and adapted based on the complexity and geographical scope of the seabed infrastructure, from regional energy pipelines to global communication networks.
- continuous monitoring and improvement - with technologies like AI and real-time monitoring, the system can constantly evolve to adapt to new threats, ensuring infrastructure is always protected.

In conclusion, the layered defence approach provides a robust, scalable, and comprehensive strategy to safeguard seabed critical infrastructure. By integrating physical protections, advanced monitoring, cybersecurity, and international

cooperation, this model ensures resilience against a wide range of threats. Each layer acts as a safety net, ensuring that even if one line of defence is breached, others remain in place to protect the infrastructure.

2.2. Key Technologies for Critical Maritime Infrastructure Protection

The integration of emerging technologies into the protection of critical maritime infrastructure is paramount in addressing current and future security challenges. These technologies aim to close existing capability gaps and enhance the resilience of seabed critical infrastructure. Key technological solutions encompass advanced sensors, autonomous systems, specialized sonar systems, and cybersecurity measures, which together form an integrated defence mechanism for critical maritime infrastructure.[1]

2.2.1. Sensors

Sensors form the backbone of maritime security by providing critical information for monitoring, detecting, and responding to potential threats.[12] They refer to a wide range of devices, both acoustic and non-acoustic, that detect biological agents or provide all-weather imaging systems [1] and should respond to the following requirements:

- High-power, wide-band, efficient low-frequency acoustic transducers enabling the detection of underwater threats over long distances, even in challenging environmental conditions;
- Low size, weight, and power open-architecture unmanned undersea vehicle payloads;
- Undersea positioning systems enhancing the ability to monitor infrastructure such as pipelines, cables, and platforms;
- Underwater acoustic communications ensuring continuous oversight and control of underwater infrastructure.
- Advanced algorithms for target detection and classification identifying real threats and filtering out false alarms.
- All-Weather imaging systems – non-acoustic sensors, such as infrared or radar-based systems, provide continuous monitoring in adverse weather conditions, including fog or heavy rainfall, ensuring that threats can be detected in all environments.
- High-frequency hardware technology and processing.

The deployment of sensors along the Nord Stream gas pipeline, for example, represents a model approach to the protection of seabed critical infrastructure. By utilizing a combination of acoustic, seismic, hydrostatic, optical, and cyber sensors, Nord Stream operators are able to maintain continuous surveillance, detect emerging threats early, and respond quickly to any anomalies. This case study underscores the importance of investing in sensor technology as a cornerstone of maritime infrastructure security, with wide applications for other critical installations across the globe.

2.2.2. Autonomous Systems

Autonomous systems, including both unmanned vehicles and autonomous platforms, are increasingly used in the protection and maintenance of critical maritime infrastructure. These systems provide capabilities that extend beyond human limitations, enabling continuous monitoring and rapid response. These systems are now a common and vital aspect of a wide range of maritime activities, especially conducting surveillance, maintaining situational awareness, and providing a capability for mine and antisubmarine warfare, communication nodes, early warning, rapid response, and search and rescue.[1]

- Unmanned Surface Vehicles (USVs) patrol the surface of the water around key maritime infrastructure equipped with cameras, radar, and communication systems. They are capable of identifying unauthorized vessels and acting as the first line of defence against potential threats. USVs can be equipped with non-lethal deterrence mechanisms such as water cannons or sound-based deterrence to keep intruders at a safe distance.[11]
- Unmanned Underwater Vehicles (UUVs) are highly versatile, capable of inspecting subsea pipelines, cables, and infrastructure. UUVs are equipped with sonar, cameras, and other monitoring devices that allow them to operate at depths and in environments that are unsafe or inaccessible to humans. UUVs can carry out tasks like leak detection, corrosion assessment, and repairs, making them invaluable for both maintenance and security.[11]
- Autonomous Submersibles, including Autonomous Underwater Vehicles (AUVs), are increasingly used for deep-sea surveillance. These submersibles are capable of long-duration missions, mapping the seabed, monitoring pipelines, and detecting foreign objects or vessels that may pose a threat. AUVs are equipped with high-resolution sonar, allowing them to perform detailed seabed surveys and infrastructure inspections.[11]
- Drones and Aerial Systems. Drones are used to monitor surface activity and inspect structures such as offshore platforms and wind farms. Equipped with cameras and sensors, they provide an aerial perspective, helping detect intruders or anomalies on the surface. Advanced drones can be equipped with infrared and thermal imaging sensors to detect heat signatures from unauthorized vessels or personnel, even in low-visibility conditions.

2.2.3. Sonar and Detection Systems

Sonar systems are critical for detecting and tracking underwater threats. These systems use sound waves to create a picture of the underwater environment, identifying both natural and man-made objects.[19]

- Passive Sonar Systems detects sounds produced by submarines, underwater drones, and other moving vessels. These systems listen for mechanical noise and propeller signatures, which helps identify the presence of vessels that might otherwise go undetected. They are useful for monitoring in a

stealth mode potential adversaries, who may be attempting to avoid detection.

- Active Sonar Systems emit sound pulses and measure their reflection off objects. This technology is effective for mapping the seabed, inspecting infrastructure, and identifying objects or vessels in the water. High-frequency active sonar is particularly effective in shallow waters where detailed imaging is necessary, such as around offshore platforms or near subsea cables.
- Synthetic Aperture Sonar (SAS). This advanced form of sonar provides higher-resolution images of the seabed, allowing for detailed inspections of underwater infrastructure. SAS is especially useful for identifying minute anomalies in pipelines or cables that might indicate damage or tampering.
- Sub-Bottom Profiling Sonar. This technology enables the detection of objects buried beneath the seabed, which is critical for protecting cables and pipelines that are buried for added security. Sub-bottom profiling can identify shifts in the seabed that may expose these structures to damage or intentional interference.

2.2.4. Communication and Command Systems

Effective command and control are essential for responding to threats to critical seabed infrastructure. Robust and secure communication systems enable real-time data sharing and coordination of defence measures across different platforms and control centers.[20]

- Satellite Communication Systems. Offshore and remote installations often rely on satellite communication to maintain links with control centres on land. This system ensures continuous communication with unmanned systems and provides a secure data pipeline for transmitting surveillance information in real-time.
- Underwater Acoustic Communications. These communication systems enable secure data exchange between submerged assets and surface platforms. Acoustic modems transmit information, allowing for the coordination of UUVs and the real-time transmission of sonar data back to monitoring centres.
- Automated Command and Control (C2) Systems. C2 systems integrate data from multiple sensors, unmanned vehicles, and surveillance platforms. These systems use algorithms to prioritize threats and optimize response times, ensuring that human operators have the most relevant information when making security decisions.

In summary, the integration of these advanced technologies into critical infrastructure protection systems significantly enhances the ability to detect, deter, and respond to potential threats. By combining sensors, autonomous systems, sonar technologies, and robust cybersecurity measures, critical maritime assets can be secured against a range of physical and cyber threats, ensuring

their resilience and operational integrity in an increasingly complex global security environment.

Conclusions

The seabed critical infrastructure is defined as a part of the national set of "critical infrastructures." It operates in an underwater environment with specific physical characteristics that require specific protective measures, both technical and procedural. The legal framework in the domain is robust and is composed of international agreements, EU directives, and national legislation, all directed toward the resilience of the infrastructure, safe, environmentally responsible, and economically efficient operations. The process of seabed critical infrastructure protection is organised at three levels – national, regional, and local- and involves many actors with safety and security responsibilities. It is increasingly recognized as a pivotal aspect of national security, economic stability, and environmental sustainability. The vital role that seabed infrastructures, such as subsea cables, pipelines, and offshore platforms, play in global communications, energy distribution, and defence underscores the necessity of developing robust and multifaceted protection strategies.

As this study has demonstrated, the integration of advanced technologies is essential for securing seabed infrastructure against a wide range of threats. Sensor technologies, autonomous systems, and cybersecurity frameworks form the backbone of a comprehensive security system. These technologies offer continuous monitoring, early threat warning, and the ability to mitigate risks before they escalate into full-blown crises. The growing dependence on seabed infrastructure for energy, communication, and defence means that these assets will remain high-value targets for adversaries and face increasing threats from natural disasters and cyber-attacks. Therefore, long-term strategies must focus on:

- resilience – building redundancy into systems to ensure that critical operations can continue even in the event of a failure or attack. For example, backup communication lines and diversified energy routes can prevent catastrophic disruptions;
- sustainability – ensuring that the protection measures employed are environmentally sustainable. This includes minimizing the impact of monitoring technologies on marine life and ensuring that the deployment of sensors, cables, or autonomous systems does not degrade ecosystems;
- innovation – the technological landscape is rapidly evolving, and continual investment in research and development will be essential. Countries and industries must remain at the forefront of technological innovation to maintain the security and integrity of their seabed infrastructures.

It could be summarized that protecting seabed critical infrastructure requires a holistic approach that incorporates cutting-edge technologies, a robust legal framework, international cooperation, and continuous innovation. As the global economy becomes more intertwined with the seabed for communication and energy, the security of these infrastructures will only grow in importance. By

adopting a forward-looking and adaptable approach, stakeholders can ensure the resilience, security, and sustainability of seabed critical infrastructures in the face of evolving global challenges. Further analysis is needed in order principles to be implemented in an effective protection system.

References

1. Njall Trausti Fridbertsson, "Protecting Critical Maritime Infrastructure – the Role of Technology," General Report, Science and Technology Committee, NATO Parliamentary Assembly, 07 October 2023, https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc.
2. Nedko Dimitrov and Valentin Najdenov, "National security in Bulgaria – is it really a system?" *Scientific technical union of mechanical engineering industry-4.0*: Year 3, 1, no. 5 (2019): 70-73.
3. Gergana Meracheva, Efrosima Zaneva-Dobranova, and Nikolay Hristov, "Seismic characterization analyses of Bulgarian Black Sea shelf for assessment of reservoir properties," *Geologica Balcanica* 51, no. 3 (2022): 29–42, https://www.geologica-balcanica.eu/sites/default/files/articles/Meracheva_Geol_Balc_51-3_2022.pdf.
4. M. Bourrel and J. Rochette, "The role of the United Nations Convention on the Law of the Sea (UNCLOS) in protecting marine biodiversity," *Marine Policy 104*, no. 1 (2019): 97-107.
5. Catherine Banet, *The Law of the Seabed: access, uses, and protection of seabed resources*, Series: Publications on ocean development, 0924–1922, vol. 90 (Boston: Brill, 2020).
6. "Directive 2008/56/EC of the European Parliament and of the Council of 17 June 2008 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive)," The European Parliament and The Council of the European Union, 17 June 2008.
7. "Directive 2014/52/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2011/92/EU on the assessment of the effects of certain public and private projects on the environment," The European Parliament and The Council of the European Union, 16 April 2014.
8. Nedko Dimitrov, "Critical infrastructures Zone," in *Functional Zoning of the National Maritime Spaces for Creating an Information System for Management of the Shore Zones* (Varna: Bulgarian Naval Academy, 2018), 168-187. – in Bulgarian
9. Lionel Carter, Douglas Burnett, Stephen Drew, Graham Marle, Lonnie Hagadorn, Deborah Bartlett-McNeil, and Nigel Irvine, "Submarine cables and the oceans-connecting the world," *UNEP-WCMC Biodiversity Series 31* (2009), ICPC/UNEP/GRID-Arendal.
10. J. Brouwers and J. H. Vreeburg, "Subsea pipeline stabilization with rock dumping: Evaluating stability in high-flow environments," *Marine Structures* 71, *no.* 2 (2020): 102-115.

11. G. Ferri, Y. Murakami, and T. Eckstein, "Advances in autonomous underwater vehicles for seabed infrastructure monitoring," *IEEE Journal of Oceanic Engineering 45, no.* 5 (2020): 1103-1115.

12. G. Smith and M. Warner, "AI-based predictive systems for subsea infrastructure: Enhancing maintenance protocols," *Journal of Ocean Technology* 35, no. 2 (2019): 76-91.

13. M. Khalid and N. Javaid, "Cybersecurity for SCADA Systems: A Multi-layered Defense Strategy," *IEEE Transactions on Industrial Informatics 16, no.* 5 (2020): 3443-3452.

14. Z. He, R. Johnson, and P. Anderson, "Predictive Maintenance for Subsea Pipelines Using Machine Learning Algorithms," *Reliability Engineering & System Safety 198* (2020): 106920.

15. O. Lange, H. Bjørnsen, and M.Olsen, "Coordinated Response Strategies for Offshore Infrastructure Protection: Lessons from Norway's Oil and Gas Sector," *Journal of Maritime Operations and Logistics 9, no.* 3 (2017): 145-162.

16. M. Rodríguez and S. Shenoi, "Redundant Networks for Resilient Subsea Communication Systems," *International Journal of Critical Infrastructure Protection* 17, no*.* 4 (2017): 32-45.

17. N. Pidgeon, D. Clarke, and S. Evans, "Legal Frameworks for Protecting Marine Infrastructure in the United Kingdom: Bridging the Regulatory Gap," *Ocean and Coastal Management* 185, *no.* 4 (2020): 1048-1063.

18. H. Fink, P. Brown, and S. Walsh, "NATO and the Protection of Critical Submarine Cables: Multinational Initiatives in Shallow Waters," *NATO Centre of Excellence for Operations in Confined and Shallow Waters*, 2019.

19. A.S. Maddox and J. P. Smith, "Subsea Cable Protection and Surveillance: A Technological Review," *Journal of Maritime Technology* 45, no. 2 (2020): 215–230.

20. N. Klein, "Security of Offshore Oil and Gas Platforms: Legal and Technological Perspectives," *Journal of Energy Law & Policy* 39, no. 1 (2018): 87–102.

21. "Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on Safety of Offshore Oil and Gas Operations and Amending Directive 2004/35/EC," The European Parliament and The Council Of The European Union, 12 June 2013.

22. "United Nation Convention on the Law of the Sea," Articles 56 and 60 of UNCLOS, 1982.

About the Authors

Prof. Nedko Dimitrov, PhD, is a Captain (BUL Navy) and Dean of the Naviation Faculty of the Bulgarian Naval Academy. https://orcid.org/0000-0003-1174-6783

Kalin Karakolev is an officer in the Bulgarian Navy, pursuing a PhD degree in the Bulgarian Naval Academy. https://orcid.org/0009-0005-7652-5465