Information & Security

Published since 1998

Y. Todorov
vol. 55, no. 2 (2024): 113-132
https://doi.org/10.11610/isij.5509

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

Research Article

# Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region

*Yavor Todorov*

*Ministry of Defense, Sofia, Bulgaria, https://mod.bg/en/index.php*

## ABSTRACT:

The Black Sea region, a vital maritime corridor, faces an escalating wave of cybersecurity threats that endanger both regional and international security. As digital technologies increasingly integrate into maritime operations, vulnerabilities to cyberattacks in the region are exacerbated by ongoing geopolitical tensions, particularly with the involvement of major powers like Russia, China, and Iran. This article offers an analysis of the maritime cybersecurity landscape in the Black Sea, evaluating the capabilities of the littoral states and identifying the key actors responsible for cyber intrusions. Through case studies and examining state-sponsored cyber operations, the research highlights the challenges posed by hybrid warfare in the region. The article also assesses the current policy frameworks and regional cooperation efforts aimed at countering these threats. It concludes by offering actionable recommendations, including the development of robust cybersecurity strategies, enhanced regional collaboration, and the leveraging of emerging technologies to safeguard maritime infrastructure. These measures are essential to preserving stability, protecting global trade routes, and reinforcing NATO's strategic interests in the Black Sea.

ARTICLE INFO:

RECEIVED: 05 SEP 2024
REVISED: 10 OCT 2024
ONLINE: 31 OCT 2024

KEYWORDS:

maritime cybersecurity, Black Sea, cyber threats, geopolitical tensions, national security, regional security

E-mail: yktodorov@mod.bg

## Introduction

At the end of March 2022, occurrences of “dark activity” sharply increased within Russian waters. Engaging in business with Russia led to blacklisting because of the war with Ukraine. As a result, many ships turned off their navigation systems to avoid detection and conduct business with Russians unnoticed.[1,2]

The Black Sea region holds significant strategic importance due to its geographical location, serving as a critical gateway between Europe and Asia. This area is pivotal for international trade routes, energy transportation, and military operations, making it a vital nexus for geopolitical and economic activities. The increasing reliance on digital technologies in maritime operations has revolutionized the industry, enhancing efficiency and communication. However, this digital transformation also introduces new vulnerabilities, particularly in cybersecurity, which can have profound implications for national security and global commerce.

According to the International Maritime Organization (IMO), cybersecurity must be an integral part of onboard safety management systems. The IMO’s Resolution MSC.428(98) mandates that shipping companies implement measures to protect these systems and conduct regular audits to ensure compliance.[3] Furthermore, the European Union Agency for Cybersecurity (ENISA) has emphasized the critical need for cybersecurity in the maritime sector by providing guidelines that help port operators and shipping companies manage cyber risks effectively.[4] These guidelines advocate for a systematic approach to identifying cyber-related assets, evaluating cyber risks, and implementing relevant security measures.[5]

The interconnected nature of modern maritime operations means that a single cyber incident can have cascading effects, disrupting trade, compromising sensitive information, and threatening the stability of critical infrastructure. Therefore, understanding and mitigating cybersecurity risks in the Black Sea maritime domain is not only a regional priority but also a global imperative. This article analyzes the cybersecurity challenges facing the maritime domain of the Black Sea—a region of strategic importance to NATO and the EU. As digital technologies become increasingly integrated into maritime operations, the potential for cyber threats grows exponentially. These threats range from data breaches and ransomware attacks to sophisticated state-sponsored cyber espionage and sabotage, posing serious risks to the security and stability of the region. The main focus of this article is to examine the various characteristics of these cybersecurity challenges, highlighting the vulnerabilities within the maritime infrastructure of EU and NATO Black Sea countries. It explores how these vulnerabilities are exploited by malicious actors, including state-affiliated groups, and also defines the potential impacts of such cyber incidents on national security, economic stability, and international trade.

Furthermore, the article emphasizes the need for robust cybersecurity strategies to address these challenges. This includes not only technological solutions but also comprehensive policy frameworks, regional cooperation, and capacity-building measures. The main thesis of the article is that by implementing proactive and resilient cybersecurity measures, the countries bordering the Black Sea can better safeguard their maritime infrastructure, ensure the smooth operation of trade routes, and maintain regional stability in the face of evolving cyber threats.

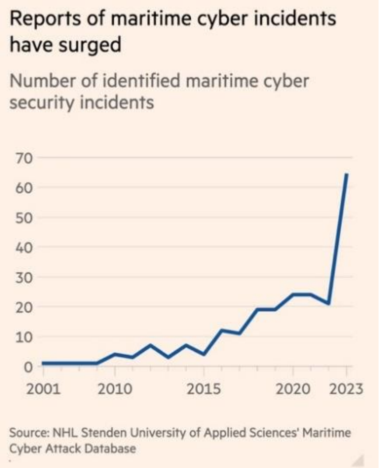

**Figure 1: Rise of the Maritime cyber incidents (IMO Annual Report on Maritime Cybersecurity, 2023).**

The interlined nature of modern maritime operations means that a single cyber incident can have cascading effects, disrupting trade, compromising sensitive information, and threatening the stability of critical infrastructure. Therefore, understanding and mitigating cybersecurity risks in the Black Sea maritime domain is not only a regional priority but also a global imperative. This article analyzes the cybersecurity challenges facing the maritime domain of the Black Sea, a region of strategic importance to NATO and EU. As digital technologies become increasingly integrated into maritime operations, the potential for cyber threats grows exponentially. These threats range from data breaches and ransomware attacks to sophisticated state-sponsored cyber espionage and sabotage, posing serious risks to the security and stability of the region.

The main focus of this article is to examine the various characteristics of these cybersecurity challenges, highlighting the vulnerabilities within the maritime infrastructure of EU and NATO Black Sea countries. It explores how these vulnerabilities are exploited by malicious actors, including state-affiliated groups, and also defines the potential impacts of such cyber incidents on national security, economic stability, and international trade.

Furthermore, the article emphasizes the need for robust cybersecurity strategies to address these challenges. This includes not only technological solutions but also comprehensive policy frameworks, regional cooperation, and capacity-building measures. The main thesis of the article is that by implementing proactive and resilient cybersecurity measures, the countries bordering the Black Sea can better safeguard their maritime infrastructure, ensure the smooth operation of trade routes, and maintain regional stability in the face of evolving cyber threats.

### *Methodology*

This study employs a qualitative research approach to analyze the cybersecurity landscape in the Black Sea maritime sector. The research is based on secondary data, including publicly available reports, government publications, academic papers, and cybersecurity databases. Key data sources include the International Maritime Organization (IMO), the European Union Agency for Cybersecurity (ENISA), and the European Repository of Cyber Incidents (EuRepoC). The study focuses on identifying patterns in cyberattacks, understanding the capabilities of prominent threat actors, and evaluating the cybersecurity policies of littoral states. The research combines case studies of significant cyber incidents with policy analysis to provide a comprehensive view of the regional cybersecurity posture. Limitations regarding data availability and the rapidly evolving threat landscape are acknowledged in the conclusions.

### *Research Question*

The central research question guiding this study is: *How do geopolitical tensions and the increasing integration of digital technologies impact the cybersecurity of maritime infrastructure in the Black Sea region, and what measures can littoral states take to mitigate these risks?*

## Overview of the Types of Cyber Threats Affecting Maritime

The maritime industry, essential for global trade and economic stability, is increasingly susceptible to a wide array of cyber threats. As digital technologies and interconnected systems become integral to maritime operations, the sector faces heightened risks from various cyberattacks.

Notable cyber incidents have included an attack in 2020 on Iran's Rajaee Port, which handled nearly half of the country's foreign trade, and an attack that in 2023 took down the website of the port of Rotterdam, Europe's largest. Danish shipowner AP Møller-Maersk, which controls about 15 percent of the global container shipping capacity, was unable to take customer orders and had to reroute ships after IT systems were taken offline by the NotPetya malware attack, which was attributed to Russia after affecting businesses globally in 2017.

Here is an overview of the predominant types of cyber threats affecting maritime operations worldwide:

*Phishing Attacks*: Phishing remains one of the most common and effective methods for cybercriminals to gain unauthorized access to maritime systems. These attacks typically involve deceptive emails or messages that trick employees into revealing sensitive information or downloading malicious software.

Once inside the network, attackers can move laterally, access critical systems, and steal data.

*Ransomware* attacks have increased in recent years, targeting shipping companies, ports, and other maritime entities. These attacks encrypt essential data, rendering systems inoperable until a ransom is paid. Notable incidents, such as the attack on Maersk in 2017, demonstrated the potential for significant operational disruption and financial loss.[6]

*Data breaches* in the maritime sector can expose sensitive information, including cargo manifests, ship schedules, and proprietary operational data. Cybercriminals can use this information for financial gain, industrial espionage, or to facilitate other attacks.

*Distributed Denial of Service (DDoS) Attacks*: DDoS attacks aim to overwhelm maritime systems with excessive traffic, causing disruptions to communication and navigation systems. These attacks can lead to significant delays and operational challenges, particularly at busy ports and shipping routes.

*Supply chain* attacks target the interconnected systems and software used by maritime companies. By compromising a third-party vendor or software provider, attackers can infiltrate the primary target network. Such attacks can go undetected for extended periods, allowing cybercriminals to conduct espionage or sabotage.

*Advanced Persistent Threats* (APTs) are prolonged and targeted cyber attacks carried out by state-sponsored or highly organized groups. These attackers infiltrate maritime networks to gather intelligence, disrupt operations, or gain strategic advantages. APTs are particularly concerning due to their sophistication and the resources behind them.

*Malware and Virus Infections*: Malware and viruses can infect maritime systems through various vectors, including USB drives, email attachments, and compromised websites. These malicious programs can steal data, disrupt operations, or provide backdoor access to attackers.

*Insider Threats*: Insiders, such as disgruntled employees or contractors with access to sensitive systems, can pose significant cyber risks. Insider threats can be intentional, such as sabotage or data theft, or unintentional, resulting from negligence or a lack of awareness.

*GPS Spoofing and Jamming*: GPS spoofing involves sending false signals to mislead ships about their true location, while GPS jamming disrupts the reception of legitimate GPS signals. Both techniques can have severe implications for navigation and safety at sea.

*Eavesdropping and Interception*: Eavesdropping attacks involve intercepting and monitoring communications within maritime systems. This can include voice, email, and data communications, allowing attackers to gather sensitive information or disrupt operations.

## Specific Characteristics of the Black Sea Cyber Domain

The Black Sea region is a complex geopolitical arena characterized by a blend of strategic interests, historical conflicts, and ongoing tensions among bordering nations. This geopolitical volatility significantly exacerbates cybersecurity risks, particularly in the maritime domain. It is also confirmed by The Atlantic Council's report, "A Security Strategy for the Black Sea," the region's maritime domain is in peril and needs fast and efficient measures to minimize the relevant risks and threats.[7]

Several factors, including the strategic importance of the region, the presence of state and non-state actors, and the continuous evolution of cyber warfare tactics, influence the specific threats in the Black Sea.

*Strategic Importance and Vulnerability:* The Black Sea serves as a critical maritime route for international trade, energy transport, and military operations. Key ports like Odessa, Constanta, Poti, and Varna are vital for the economies of surrounding nations, as well as for the EU and NATO. The strategic importance of these maritime hubs makes them prime targets for cyberattacks aimed at disrupting economic activities and military logistics. Cyber threats targeting these ports can lead to significant operational disruptions, financial losses, and geopolitical instability.

*State-Sponsored Cyber Warfare:* Geopolitical tensions in the Black Sea are heightened by the activities of state-sponsored actors. Russia has been implicated in numerous cyber operations aimed at asserting dominance in the region. Russian cyber units, including APT28 (Fancy Bear) and Sandworm, have been known to conduct sophisticated cyber espionage and sabotage operations. These activities are often aligned with broader geopolitical objectives, such as undermining the stability of neighboring countries and deterring NATO influence.

*Conflict spillover:* The ongoing war between Russia and Ukraine have a potential significant impact on cybersecurity in the Black Sea. Cyberattacks, such as the NotPetya ransomware, initially targeted Ukrainian entities but quickly spread to affect global systems. The proximity and interconnectivity of Black Sea nations mean that cyber incidents in one country can have cascading effects on the entire region. This spillover effect exacerbates the overall cybersecurity risk landscape.

The concept of hybrid warfare, which combines conventional military tactics with cyber operations, is becoming increasingly relevant in the Black Sea. Cyberattacks are used to complement traditional military actions, creating a multi-faceted threat environment. During periods of heightened military tension, cyber operations are deployed to disrupt communications, sabotage critical infrastructure, and spread misinformation. This integrated approach to warfare amplifies the cybersecurity challenges in the region.

*Non-State Actors and Cybercrime:* Apart from state-sponsored threats, the Black Sea region is also vulnerable to cyber activities by non-state actors, including organized crime groups and hacktivists. These actors often exploit geopolitical instability to conduct cyber operations for financial gain, political objectives, or ideological reasons. Such actors add another layer of complexity to the cybersecurity landscape, making it difficult to attribute and respond to cyber incidents effectively.

*Energy Sector Vulnerabilities:* The Black Sea is a key conduit for energy transportation, including oil and gas pipelines. Cyberattacks on energy infrastructure can have far-reaching consequences, affecting not only local economies but also global energy markets. State-sponsored actors may target energy assets to disrupt supply chains, exert economic pressure, or gain strategic advantages. The energy sector's vulnerability to cyber threats is a critical concern for the Black Sea region's security.

*Maritime Operational Risks*: In the Black Sea, the maritime industry relies heavily on digital systems for satellite navigation, cargo management, and communication. Cyberthreats to these systems lead to navigational errors, loss of cargo, and safety hazards at sea. GPS spoofing and jamming can mislead vessels, causing them to veer off course or collide with other ships.

## Potential Consequences

### *Disruption of Maritime Trade*

Cyberattacks can lead to significant disruptions in maritime trade by targeting port operations, shipping logistics, and navigation systems. This can lead to delays, financial losses, and increased shipping costs, all of which can affect the global supply chain.

### *Military Implications*

Cyber capabilities can be used to gather intelligence on naval operations, disrupt military logistics, and potentially sabotage military assets. This poses a direct threat to the security of the Black Sea littoral states and NATO operations in the region.

### *Economic Impact*

The Black Sea region is a critical economic zone for several countries. Cyberattacks on maritime infrastructure can lead to economic instability, affect energy supplies, and undermine investor confidence.

## Capabilities of the Black Sea Countries

Maritime cybersecurity is a critical concern for countries bordering the Black Sea. This analysis explores the maritime cybersecurity capabilities of Bulgaria, Romania, Georgia, Ukraine, and Turkey to tackle the relevant risks and threats. By examining each country's approach, this document highlights the diverse strategies and common hurdles in safeguarding maritime operations from cyber threats.

## *Bulgaria*

Bulgaria adheres to the EU's cybersecurity regulations, which provide a robust framework for protecting digital infrastructure. The National Cybersecurity Strategy and the Cybersecurity Act outline the country's approach to cybersecurity and defense. However, maritime-specific cybersecurity guidelines are limited, and funding for cybersecurity enhancements in this sector is insufficient:[25]

**Table 1. Black Sea Countries Capabilities (EuRepoC: European Repository of Cyber Incidents).**

| Country | Cybersecurity Norms | Cybersecurity Structures | Deficiencies | Challenges |
|---|---|---|---|---|
| Bulgaria | Adheres to EU cybersecurity regulations;<br>National Cybersecurity Strategy | National Cybersecurity Coordination Center;<br>Ministry of e-gov<br>MoD<br>State Agency for National Security<br>MoI | Limited maritime-specific cybersecurity guidelines;<br>Insufficient funding for maritime cybersecurity | Integrating cybersecurity across diverse stakeholders;<br>Enhancing cybersecurity in aging maritime infrastructure |
| Romania | Compliance with EU Network and Information Security (NIS2) Directive;<br>National Cybersecurity Strategy | National Computer Security Incident Response Team (CERT-RO); National Cyber Security Directorate<br>SRI | Limited coordination between maritime authorities;<br>Gaps in maritime-specific cybersecurity policies | Balancing investments in cyber and physical maritime security;<br>Ensuring seamless cooperation between civilian and military maritime sectors |
| Georgia | National Cybersecurity Strategy;<br>Cybersecurity legislation aligned with EU standards | Cyber Security Bureau;<br>Ministry of Defence | Limited maritime cybersecurity expertise;<br>Insufficient infrastructure for cyber defense and cybersecurity | Developing comprehensive maritime cybersecurity regulations;<br>Addressing the growing cyber threats in the maritime sector |
| Ukraine | National Cybersecurity Strategy;<br>Cybersecurity Law | State Service of Special Communications and Information Protection;<br>Cyber Police Department | Limited maritime cybersecurity framework.<br>Resource constraints for cybersecurity enhancements | Combatting cyber threats amid ongoing war;<br>Coordinating cybersecurity efforts across different maritime sectors |
| Turkey | National Cybersecurity Strategy;<br>Cybersecurity Regulations | National Cyber Incident Response Center (USOM);<br>Ministry of Transport and Infrastructure | Maritime-specific cybersecurity needs refinement;<br>Need for better integration of maritime cyber defenses | Ensuring cybersecurity in a geopolitically sensitive area; Managing the balance between civil and military maritime operations |

## *Romania*

Romania complies with the EU Network and Information Security (NIS2) Directive, ensuring a high standard of cybersecurity. The National Cybersecurity

Strategy and the National Cyber Security Directorate play key roles in the country's cyber defense framework. Nevertheless, coordination between maritime authorities is limited, leading to gaps in maritime-specific cybersecurity policies.[26]

### Georgia

Georgia's National Cybersecurity Strategy and aligned legislation reflect the country's commitment to cybersecurity, supported by structures like the Data Exchange Agency, the Cyber Security Bureau, and the Ministry of Defence. Despite these efforts, Georgia faces a shortage of maritime cybersecurity expertise and infrastructure.[27]

### Ukraine

Ukraine has established a National Cybersecurity Strategy and a Cybersecurity Law to safeguard its digital environment. Key organizations include the State Service of Special Communications and Information Protection and the Cyber Police Department. However, the maritime cybersecurity framework remains incomplete, and there are resource constraints for enhancements.[28]

### Turkey

Turkey's Turkey's National Cybersecurity Strategy and regulations provide a robust foundation for cyber defense, supported by the National Cyber Incident Response Center (TR-CERT) and the Ministry of Transport and Infrastructure. However, maritime-specific cybersecurity requires further refinement and integration to address the unique challenges in the sector. A notable example of this need occurred in August 2023, when AKBASOGLU HOLDING Trans KA, a Turkish company, fell victim to a Knight ransomware attack. The attackers infiltrated the company's network, stealing sensitive data, including financial documents, logistics information, personal details, insurance records, and confidential information. The stolen data is set to be made publicly available within three days, posing a significant threat to the company's customers.[29]

Knight ransomware, an evolution of Cyclops ransomware, operates as a Ransomware-as-a-Service (RaaS) platform. This type of cybercrime tool allows cybercriminals to "rent" ransomware software, making it easier to execute attacks on enterprises and organizations using the Server Message Block (SMB) protocol. RaaS has been widely documented as a growing concern in cybersecurity, especially due to its accessibility to even low-skilled hackers.[30] This attack underscores the critical importance of implementing multi-layered security measures, comprehensive employee education, strong password policies, multi-factor authentication, regular system updates, and robust backup and disaster recovery plans.[31]

## Analysis of Cybersecurity Threats to Maritime Transport

### *Common Sectors Targeted*

The sectors frequently targeted by cyberattacks across the analyzed countries are:

- Transportation
- Energy
- Telecommunications
- Finance
- Defence industry
- Research.

These sectors represent critical infrastructure in the Black Sea region and are highly vulnerable to cyberattacks, particularly from state-sponsored and non-state actors who exploit vulnerabilities for financial gain, espionage, or sabotage.

## Analysis of the Cyberattacks in the Black Sea Region

The following table presents an analysis of cyberattacks in the Black Sea region, highlighting the frequency and types of attacks across the countries examined. This analysis underscores the significant threats posed to maritime and national infrastructure across the region.[13]

**Table 2. Black Sea Countries Threat Map (EuRepoC: European Repository of Cyber Incidents).**

| Country | Data Theft | Ransomware | DDoS/Defacement | Wiper Attacks |
|---|---|---|---|---|
| Romania | High frequency | Moderate frequency | Moderate frequency | N/A |
| Bulgaria | Moderate frequency | Moderate frequency | High frequency | N/A |
| Georgia | High frequency | N/A | Moderate frequency | N/A |
| Ukraine | High frequency | High frequency | Moderate frequency | Moderate frequency |
| Turkey | High frequency | Moderate frequency | Moderate frequency | Moderate frequency |

## Techniques used by threat actors

Across the analyzed countries, the common techniques used for initial access include:

- Phishing: deceiving individuals to reveal confidential information.
- Exploiting Public-Facing Applications: Leveraging software vulnerabilities.
- Drive-By Compromise: Embedding malicious code in frequently visited websites.
- Supply Chain Compromise: Attacking third-party vendors to infiltrate target systems.

## Prominent cyber threat actors and their state affiliations

Table 3 outlines the most prominent cyber threat actors operating in the Black Sea region, detailing their affiliations and typical activities, which highlight the complexity of attribution in cyber operations.

**Table 3. Black Sea Countries Prominent Threat Actors (EuRepoC: European Repository of Cyber Incidents)**

| Threat Actor | Type | Activities | State Affiliation |
|---|---|---|---|
| Killnet | Non-State Actor | DDoS and defacement attacks | None explicitly mentioned |
| TA558 | Non-State Actor | Data theft via drive-by compromise | None explicitly mentioned |
| UNC4841 | Non-State Actor | Data theft and phishing | None explicitly mentioned |
| Inception Frame-work/Cloud Atlas | Unknown | Data theft with unknown initial access | Suspected state-affiliated |
| MuddyWater/ TEMP.Zagros | State-Affiliated | Data theft and phishing | Iran |
| Sandworm (VOODOO Bear) | State-Affiliated | Wiper malware and public-facing app exploits | Russia |
| Fancy Bear (APT28) | State-Affiliated | Data theft and public-facing app exploits | Russia |
| Gamaredon (Shuckworm) | State-Affiliated | Phishing and data theft | Russia |
| Red Stinger/Bad Magic | Unknown | Data theft with unknown initial access | Suspected state-affiliated |
| Lazarus Group/Labyrinth Chollima | State-Affiliated | Data theft and public-facing app exploits | North Korea |

| | | | |
|---|---|---|---|
| DeftTorero/Volatile Cedar | State-Affiliated | Data theft using public-facing applications | Lebanon |
| MoleRATs/Extreme Jackal | Non-State Actor | Data theft with unknown initial access | None explicitly mentioned |

Other findings include a growing vulnerability in OT systems, which manage critical physical assets like sensors and safety mechanisms, due to increased connectivity. Despite heightened awareness following high-profile incidents such as the NotPetya attack on Maersk, the industry still focuses predominantly on IT security, leaving OT systems exposed. A gap between the industry cybersecurity maturity and new stringent regulations also presents challenges.

## Capabilities of the threat actors

This chapter provides a detailed analysis of the cyber capabilities of key threat actors, focusing on nations that pose significant risks in the Black Sea region. The analysis includes an overview of the strategic cyber doctrines of these countries and highlights the offensive cyber units and advanced persistent threat (APT) groups that form the backbone of their cyber operations.

### *Russian Federation*

Russia's cybersecurity strategy is integrated into its broader national security and information warfare doctrines.[19] Key strategic documents include:

**Table 5. Russia capabilities (EuRepoC: European Repository of Cyber Incidents)**

| Document | Overview | Key Points |
|---|---|---|
| National Security Strategy (2021) | Emphasizes defending national interests, including cyber capabilities. | Focus on offensive cyber capabilities and economic stability |
| Information Security Doctrine (2016) | Focuses on protecting Russia's information space and enhancing cybersecurity. | Emphasizes international cooperation and critical infrastructure protection |
| Military Doctrine (2014) | Integrates cyber operations into broader military strategies. | Emphasizes offensive and defensive cyber operations, particularly in hybrid warfare |

Russia's cyber operations in the Black Sea region are particularly concerning due to its geopolitical interests and proximity. Russian APTs, such as APT28 and APT29, have a history of targeting critical infrastructure, including maritime systems. For instance, the NotPetya attack, which initially targeted Ukrainian companies, quickly spread globally, affecting numerous sectors, including shipping.

The ability to disrupt port operations, logistics, and navigation systems can severely impact maritime trade and military logistics in the Black Sea.

### *Iran*

Iranian cyber capabilities, while often regionally focused, pose a growing threat due to their increasing sophistication. Iranian APTs, such as APT33 and MuddyWater, have engaged in cyber espionage and attacks on critical infrastructure. Although their operations have primarily targeted regional adversaries and Western interests, the potential for spillover into the Black Sea maritime domain exists, especially if Iranian interests align with broader geopolitical conflicts involving Russia or NATO member states.

**Table 6. Iran capabilities (EuRepoC: European Repository of Cyber Incidents)**

| Document | Overview | Key Points |
|---|---|---|
| National Security Strategy (2021) | Emphasizes defending national interests, including cyber capabilities | Focus on offensive cyber capabilities and economic stability |
| Information Security Doctrine (2016) | Focuses on protecting Russia's information space and enhancing cybersecurity | Emphasizes international cooperation and critical infrastructure protection |
| Military Doctrine (2014) | Integrates cyber operations into broader military strategies | Emphasizes offensive and defensive cyber operations, particularly in hybrid warfare |

### *China*

China's cyber operations are heavily focused on economic espionage and gathering geopolitical intelligence. APT groups like APT1 and APT41 have been implicated in widespread cyber espionage campaigns targeting various sectors, including maritime industries. China's interest in the Belt and Road Initiative, which includes significant maritime components, suggests that Chinese cyber activities could increasingly target maritime infrastructure in strategic locations such as the Black Sea to gain economic and strategic advantages.

### *North Korea*

North Korea's approach to cybersecurity is heavily influenced by its broader national security priorities, focusing on both defensive and offensive cyber capabilities as tools of state policy.[20]

1.Juche Cyber Strategy (2018):

Overview: Reflects North Korea's self-reliance principle (Juche), emphasizing the development of indigenous cyber capabilities.

Key Points:

Enhance cyber defense mechanisms to protect against foreign threats.

**Table 7. China's capabilities (EuRepoC: European Repository of Cyber Incidents)**

| Document | Overview | Key Points |
|---|---|---|
| Defensive Posture and Retaliation | Focuses on defending against cyber threats from Western nation. | Retaliation and offensive cyber capabilities for deterrence |
| Cyber Espionage and Sabotage | Engages in cyber espionage and attacks on critical infrastructure | Targets energy sectors, gathers intelligence for strategic advantages |
| State-Sponsored Cyber Units | Iran's cyber operations are conducted through state-sponsored groups like APT33 | Focuses on critical industries and regional influence |

Develop offensive cyber tools for strategic advantage and information warfare (The Diplomat)

2.National Military Strategy (2015):

Overview: Integrates cyber operations within the broader context of military strategy, emphasizing cyber warfare as a component of asymmetrical warfare.

Key Points:

Use cyber operations to disrupt enemy infrastructure.

Leverage cyber tools for intelligence gathering and strategic disruptions (Council on Foreign Relations).

3.Cyber Operations Doctrine (2017):

Overview: A specific doctrine describing the deployment and use of cyber tools for both defense and offense.

Key Points:

Focus on cyber-espionage and intellectual property theft.

Develop capabilities to conduct cyber attacks on critical infrastructure of adversaries (CSIS)

### *Lebanon*

Key Points:

Strengthen cybersecurity infrastructure and capabilities.

Promote public-private partnerships for enhanced cyber resilience.

Enhance legal and regulatory frameworks for cybersecurity (ITU)

2.Critical Infrastructure Protection Plan (2019):

Overview: Focuses on securing Lebanon's critical infrastructure against cyber threats.

Key Points:

Implement robust protection measures for key sectors such as energy, telecommunications, and finance.

Develop response and recovery plans for cyber incidents (Arab Regional Cybersecurity Center) Lebanon's cybersecurity strategy is evolving, driven by both national security concerns and the need to protect critical infrastructure from increasing cyber threats.[19]

1.National Cybersecurity Strategy (2020):

Overview: Framework outlining Lebanon's approach to improving national cybersecurity posture.

3.Information Security Doctrine (2018):

Overview: Outlines Lebanon's policies and practices for protecting information assets and ensuring cybersecurity.

Key Points:

Enhance information security awareness and training.

Promote international cooperation in cybersecurity efforts (Lebanon National Cyber Security Authority)

The following figure illustrates the rise in maritime cyber incidents, as reported by the IMO's Annual Report on Maritime Cybersecurity in 2023. It demonstrates the increasing trend of cyberattacks targeting the maritime sector, highlighting the urgency of addressing these threats in the Black Sea region

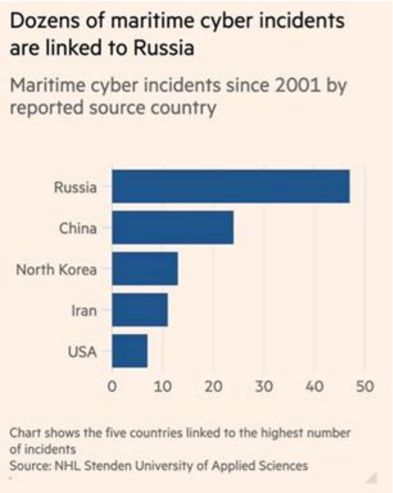

**Figure 2: Maritime Cyber incidents by threat actor**
**(Source: IMO Annual Report on Maritime Cybersecurity 2023)**

As shown in Figure 1, maritime cyber incidents have increased significantly over the past few years. This rise can be attributed to the growing reliance on digital technologies in maritime operations and the increasing sophistication of cyber threats. The data emphasizes the need for robust cybersecurity measures to protect maritime infrastructure and maintain the stability of global trade routes.

## Recomendations

To address the significant cybersecurity challenges in the Black Sea region, it is essential to adopt a multi-faceted approach that encompasses technological advancements, comprehensive policy frameworks, regional cooperation, and capacity-building measures.

Enhancing the cybersecurity infrastructure is crucial. This involves investing in state-of-the-art cybersecurity technologies such as intrusion detection systems, firewalls, and encryption to protect maritime operations. Regular cybersecurity audits and vulnerability assessments should be conducted frequently to identify and mitigate potential threats.

Strengthening policy frameworks is another critical step. Adhering to International Maritime Organization (IMO) cybersecurity guidelines and incorporating them into national regulations is essential. Additionally, developing tailored cybersecurity policies that address the unique challenges of the maritime sector, including navigation and communication systems, is necessary.

Promoting regional cooperation is vital for effective cybersecurity. Establishing regional platforms for sharing cybersecurity threat intelligence and best practices among Black Sea countries can enhance collective defense. Conducting joint cybersecurity drills and exercises will improve coordination and response capabilities among regional stakeholders.

Building cybersecurity capacity involves implementing comprehensive training programs for maritime industry personnel to enhance their cybersecurity awareness and skills. Fostering collaborations between governments, private sector entities, and academic institutions can help develop innovative cybersecurity solutions.

Enhancing NATO's presence in the Black Sea is also recommended. Strengthening NATO's naval presence in the region can deter potential cyber threats and enable swift responses to incidents. Increasing collaboration between NATO and Black Sea countries on cyber defense initiatives is crucial.

Promoting energy independence is another important aspect. Encouraging the diversification of energy sources and routes can reduce reliance on vulnerable infrastructure. Implementing robust cybersecurity measures to safeguard critical energy infrastructure from cyberattacks is necessary.

Countering hybrid threats requires developing strategies that integrate conventional and cyber defense mechanisms effectively. Public awareness campaigns should be launched to educate stakeholders about the risks and preventive measures associated with hybrid warfare.

By implementing these recommendations, Black Sea countries can enhance their cybersecurity posture, protect critical maritime infrastructure, and maintain regional stability in the face of evolving cyber threats.

## Conclusion

The Black Sea region, a crucial maritime gateway between Europe and Asia, faces significant cybersecurity challenges due to geopolitical tensions and the increasing digitization of maritime operations. The rise in "dark activity" in Russian waters amidst the Ukraine conflict highlights the complexities of maintaining cybersecurity in such a volatile environment.

Digital technologies have revolutionized maritime operations, enhancing efficiency and communication. However, they have also introduced new vulnerabilities that malicious actors, both state-sponsored and non-state groups, can exploit. The potential disruptions in maritime trade, military logistics, and economic stability necessitate a comprehensive and proactive approach to cybersecurity.

NATO/EU countries bordering the Black Sea, including Bulgaria, Romania, Georgia, Ukraine, and Turkey, show varying degrees of preparedness in addressing maritime cybersecurity threats. While compliance with international and EU regulations is evident, gaps remain in maritime-specific guidelines, coordination, expertise, and resource allocation.

The urgent need for robust cybersecurity strategies is clear. These strategies must include technological advancements, policy frameworks, regional cooperation, and capacity-building measures. Strengthening NATO's presence, enhancing intelligence sharing, promoting energy independence, and countering hybrid threats through public-private partnerships are essential steps to safeguard the region's maritime infrastructure.

## Limitations

This study presents a comprehensive analysis of maritime cybersecurity in the Black Sea region, but several limitations should be noted. First, the research is based largely on publicly available data and incident reports, which may not fully capture the extent of state-sponsored cyber activities, particularly in classified or covert operations. The lack of transparency surrounding cybersecurity incidents, especially in military and defense sectors, can limit the accuracy of assessments. Furthermore, the rapidly evolving nature of cyber threats presents another challenge. As threat actors continually develop new tools and techniques, the findings of this study may become outdated relatively quickly, especially in the context of emerging technologies.

Additionally, the geopolitical complexities of the Black Sea region add another layer of uncertainty. The region's shifting alliances, conflicts, and diplomatic relations can influence cyber activities and impact the applicability of the study's findings over time. While the analysis focuses on several prominent state and non-state actors, it does not encompass all potential cyber actors that may have interests in the region, particularly lesser-known or emerging groups. Finally, the study primarily addresses technological aspects of cybersecurity and operational capabilities. It does not delve as deeply into socio-political factors, such as public opinion, regulatory responses, or the influence of international organizations, which also play critical roles in shaping the region's cybersecurity landscape.

## References

[1] K. Oanh, “Russian Tankers Going Dark Raises Flags on Sanctions Evasion,” *Claims Journal*, 29 March 2022, https://www.claimsjournal.com/news/international/2022/03/29/309507.htm.

[2] “The Hack That Should Have Been Impossible,” *Bloomberg.Com*, accessed 27 August 2024, https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/.

[3] International Maritime Organization (IMO), “IMO Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems,” IMO Resolution, June 16, 2017, https://mlaus.org/wp-content/uploads/bp-attachments/10110/OVSC-Spring-2021-Cyber.pdf.

[4] European Union Agency for Cybersecurity (ENISA), “Cybersecurity for Ports and Maritime Entities: Guidelines for Managing Cyber Risks,” January 2023, https://www.enisa.europa.eu/publications/maritime-cybersecurity-guidelines.

[5] European Union Agency for Cybersecurity (ENISA), *Guidelines for Enhancing Maritime Cybersecurity*, 2023, https://www.enisa.europa.eu/publications.

[6] “BSMCySec Conference,” accessed 27 August 2024, https://conference.blacksea cybersecurity.net/.

[7] NATO Defense College, “NDC-Research,” NDC, accessed 27 August 2024, https://www.ndc.nato.int/research/https:www.ndc.nato.int/research/research.php ?icode=704.

[8] Basil Germond, “Op-Ed: The Geopolitics of Maritime Cybersecurity,” *Marine Log*, 10 July 2023, https://www.marinelog.com/views/op-eds/op-ed-the-geopolitics-of-maritime-cybersecurity/.

[9] “Cyber-Attack on ShipManager Servers – Update,” DNV, 23 January 2023, https://www.dnv.com/news/cyber-attack-on-shipmanager-servers-update-237931/.

[10] Sam Fenwick, “Cyber-Attacks on Port of Los Angeles Have Doubled since Pandemic,” *BBC World Service*, 22 July 2022, https://www.bbc.com/news/business-62260272.

[11] “Cybercrime Intelligence Fight Cyber Threats,” *Intel471*, accessed 27 August 2024, https://intel471.com/.

[12] “Cybersecurity in Maritime: Navigating the Digital Seas Safely,” *MarineLink*, 9 August 2024, https://www.marinelink.com/articles/maritime/cybersecurity-in-maritime-navigating-the-digital-seas-safely-101609.

[13] “Defining Insider Threats,” CISA, accessed 27 August 2024, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats.

[14] Anastasia Dimakopoulou and Konstantinos Rantos, “Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0,” *Journal of Marine Science and Engineering* 12, no. 6 (2024): 919, https://doi.org/10.3390/jmse12060919.

[15] Directoratul Național de Securitate Cibernetică (DNSC), accessed 27 August 2024, https://dnsc.ro/.

[16] EuRepoC: European Repository of Cyber Incidents, accessed 27 August 2024, https://eurepoc.eu/.

[17] "Jump in AIS Gaps Mask Russian Maritime Activity," Lloyd"s List Intelligence, accessed 27 August 2024, https://www.lloydslistintelligence.com/knowledge-hub/data-storytelling/jump-in-ais-gaps-mask-russian-maritime-activity.

[18] Atlantic Council, "A Security Strategy for the Black Sea," *Atlantic Council Task Force on Black Sea Security* (blog), 15 December 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-security-strategy-for-the-black-sea/.

[19] Sevan Araz, "Lebanon's Cybersecurity Strategy Emerges," Middle East Institute, accessed 27 August 2024, https://mei.edu/publications/lebanons-cybersecurity-strategy-emerges.

[20] MCAD Maritime Cyber Attack Database, accessed 27 August 2024, https://maritime cybersecurity.nl/.

[21] Nima Khorrami, "Navigating Cybersecurity and Surveillance: Iran's Dual Strategy for National Security," The Washington Institute, Mar 29, 2024, www.washington institute.org/policy-analysis/navigating-cybersecurity-and-surveillance-irans-dual-strategy-national-security.

[22] Arms Control Association, "Russia"s Military Doctrine," accessed 27 August 2024, https://www.armscontrol.org/act/2000-05/russias-military-doctrine.

[23] Hideshi Takesada, "Interpreting North Korea's Military Strategy," International Symposium on Security Affairs 2010, National Institute for Defense Studies, December 2, 2010.

[24] T.C. Ulaştırma ve Altyapı Bakanlığı, accessed 27 August 2024, https://www.uab.gov.tr/.

[25] "National Cybersecurity Strategy: Cyber Resilient Bulgaria 2023," Republic of Bulgaria, Sofia: Council of Ministers, 2021.

[26] European Union Agency for Cybersecurity (ENISA), *Cybersecurity in the Maritime Sector: NIS2 Directive Compliance,* 2023.

[27] Georgian Ministry of Defence, *Cyber Security Bureau Annual Report*, 2023.

[28] State Service of Special Communications and Information Protection of Ukraine, *National Cybersecurity Strategy of Ukraine*, 2022.

[29] "Knight Ransomware Attack on AKBASOGLU HOLDING Trans KA," *Intel471,* accessed August 27, 2024, https://intel471.com/knight-ransomware-attack-trans-ka.

[30] Catalin Cimpanu, "Ransomware-as-a-Service (RaaS): The Growing Cybercrime Threat," *ZDNet*, August 3, 2023, https://www.zdnet.com/article/ransomware-as-a-service-the-growing-cybercrime-threat/.

[31] CISA, "Cybersecurity Measures for SMBs: Protecting Against Ransomware," accessed August 27, 2024, https://www.cisa.gov/cyber-measures-for-smbs.

[32] "The Cost of a Malware Infection? For Maersk, $300 Million," *Digital Guardian*, accessed 27 August 2024, https://www.digitalguardian.com/blog/cost-malware-infection-maersk-300-million.

[33] "The Kremlin Sees Bulgaria and Romania as a Threat to Its Security in The Black Sea," *Radio Bulgaria*, 18 July 2024, https://avimbulten.org/en/Bulten/THE-KREMLIN-SEES-BULGARIA-AND-ROMANIA-AS-A-THREAT-TO-ITS-SECURITY-IN-THE-BLACK-SEA.

[34] "China Publishes First National Cybersecurity Strategy," *USITO*, accessed 27 August 2024, https://usito.org/news/china-publishes-first-national-cybersecurity-strategy.

[35] Boyan Mednikarov et al., "Cyber Hygiene Issues in the Naval Security Environment," *Information & Security: An International Journal* 53, no. 2 (2022): 205-218, https://doi.org/10.11610/isij.5314.

[36] Boyan Mednikarov et al., "Analysis of Cybersecurity Issues in the Maritime Industry," *Information & Security: An International Journal* 47, no. 1, (2020): 27-43, https://doi.org/10.11610/isij.4702.

## About the Author

Yavor **Todorov**, PhD, is a cybersecurity expert with over 20 years of experience in security, defense, and cybersecurity. He advises Bulgaria's Ministry of Defense on cyber defense and cyber risk management. He holds a Master's in Strategic Studies and a PhD degree in Maritime Cybersecurity and. Dr. Todorov has led key cybersecurity initiatives at Bulgaria's State Agency for National Security. He represents Bulgaria in high-level international forums and is a frequent speaker at the Marshall European Center for Security Studies.
https://orcid.org/0000-0002-2279-2075