TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

GEOPOLITICAL DYNAMICS AND HYBRID-CYBER THREATS IN THE BLACK SEA REGION: SAFEGUARDING ROMANIA'S CRITICAL MARITIME INFRASTRUCTURES

Minodora BADEA, Adrian V. GHEORGHE, Gabriel RAICU, Radu D. STANCIU

Abstract: *The Black Sea region has emerged as a strategic maritime hub increasingly vulnerable to hybrid warfare and cyber threats following the 2022 invasion of Ukraine. This study synthesizes empirical data from the Maritime Cyber Attack Database (MCAD) and strategic reports to examine vulnerabilities in Romania's critical maritime infrastructure (CMI). Utilizing a mixed- methods approach, we identify threats such as state-sponsored GNSS spoofing, ransomware, and infrastructure sabotage. Findings indicate that Romania ranked 52nd globally in cyber impact during H1 2025. This work underscores the imperative for resilient infrastructures to safeguard global trade and security in a contested geopolitical landscape.*
Keywords: *Black Sea geopolitics, hybrid warfare, cyber threats, critical infrastructure protection, Romania, NATO-EU synergy, MCAD, GNSS spoofing, maritime cybersecurity.*

1. INTRODUCTION

The Black Sea basin represents a strategic nexus of energy transit, commercial shipping, and military maneuvering, rendering it a perennial arena for great-power competition. Since Russia annexed Crimea in 2014 and the escalation of hostilities in Ukraine from 2022 onward, the region has witnessed a paradigm shift toward hybrid warfare, a doctrine that amalgamates kinetic actions with non-kinetic tools such as cyberattacks, electronic warfare (EW), and information operations to achieve strategic objectives below the threshold of conventional conflict [1,2].

Romania's position as a littoral state amplifies its exposure to these hybrid threats, with the Port of Constanta serving as the Black Sea's premier commercial hub and a critical node in NATO's Eastern Flank logistics network. In 2024, the port facilitated approximately 79 million tons of cargo [3], representing a 14.3% decline from the 92.7 million tons managed in 2023. This fluctuation reflects multiple factors, including the reopening of Ukrainian ports (Odesa, Chornomorsk, Yuzhnyi), which eliminated multimodal transfer costs previously incurred via Constanta [4]; reduced Ukrainian grain harvests due to conflict and drought conditions [16]; and Danube River navigation challenges that hampered barge transport [4]. Additionally, persistent security concerns stemming from naval blockades, mine threats, and elevated insurance premiums have contributed to operational uncertainty [20].

The problem addressed in this study is the increasing vulnerability of Romania's critical maritime infrastructure (CMI) to asymmetric disruptions that target the convergence of physical and digital assets. Such disruptions can lead to catastrophic economic losses, environmental hazards, and compromised national security. This article evaluates the current threat landscape and proposes adaptive defensive frameworks based on empirical data from the Maritime Cyber Attack Database (MCAD).

The primary field of application for this research is the maritime transportation system (MTS), specifically the critical infrastructure nodes within the Black Sea littoral states. This includes ports, subsea data cables, energy transit

pipelines, and offshore gas platforms (e.g., the Neptun Deep project).

1.1 Strategic Maritime Hubs

Ports such as Constanta, Odesa, Varna, and Istanbul serve as vital lifelines for European economies, and their strategic interconnectedness, combined with proximity to contested waters near Crimea, renders them vulnerable to asymmetric disruptions (Figure 1). Any disruption to the Port of Constanta directly affects the logistics chain for NATO's Eastern Flank and the global food supply via the European Union's "Solidarity Lanes" [4].



Fig. 1. Major ports and strategic logistics corridors in the Black Sea. (Source: Marine Insight [adapted])

1.2 IT and OT Convergence in MTS

The modernization of Maritime Transportation Systems (MTS) relies on the convergence of Information Technology (IT) and Operational Technology (OT).

OT systems manage physical processes like crane movements, vessel traffic services, and fuel distribution. The erosion of the traditional "air-gap" between these systems means that a cyber incursion in the IT network (e.g., via administrative email phishing) can migrate to OT systems, leading to physical sabotage or operational paralysis [5,6].

Despite growing awareness of these vulnerabilities, critical gaps remain in understanding how hybrid threats specifically impact Romanian maritime infrastructure.

This study addresses two research questions:
RQ1: What are the temporal patterns and threat actor profiles of maritime cyber incidents in the Black Sea region from 2017-2025?
RQ2: How do hybrid-cyber threats contribute to operational disruptions at the Port of Constanta, and what proportion of the recent cargo decline can be attributed to security concerns versus economic factors?

This work contributes the first systematic longitudinal analysis of maritime cyber threats targeting Romanian CMI, integrating incident data, threat actor attribution, and economic impact assessment. By disaggregating the causes of Constanta's cargo decline and quantifying the role of hybrid threats, we provide evidence-based recommendations for policymakers, port operators, and NATO defense planners.

2. LITERATURE REVIEW

2.1 Hybrid Warfare in the Black Sea Context

Scholarly discourse has evolved to view the Black Sea as a "hybrid confrontation space" where conventional military posturing intersects with cyber operations, information warfare, and economic coercion [1,12]. Sabanadze and Dalay [2] argue that Russia's strategic ambition in the Black Sea involves both naval blockades and hybrid sabotage of undersea assets, including data cables and energy pipelines. The RAND Corporation's 2020 assessment [1] documented Russia's layered approach to Black Sea power projection, combining naval deployments with electronic warfare capabilities that degrade GPS signals and disrupt maritime communications.

The 2022 invasion of Ukraine marked an inflection point in hybrid maritime operations. The Atlantic Council reported that cyber-enabled blockades combining naval mine threats with cyberattacks on Ukrainian port management systems effectively paralyzed grain exports for months, demonstrating the strategic value of coordinated cyber-kinetic operations. This operational model has since expanded to include persistent GNSS spoofing, AIS manipulation, and ransomware targeting port infrastructure across the Black Sea littoral [23].

2.2 Maritime Cybersecurity Vulnerabilities

Technical literature emphasizes risk assessment models specifically for seaports [5]. Güneş and Kayisoglu [5] developed a comprehensive cyber risk framework identifying vulnerabilities in port IT/OT convergence, cargo management systems, and vessel traffic services. The ENISA Threat Landscape 2025 report [6]

notes a surge in attacks on OT systems, highlighting that maritime entities are particularly vulnerable due to legacy software, unpatched industrial protocols (e.g., Modbus, DNP3), and limited security monitoring capabilities.

Maritime-focused analyses document specific attack vectors: GNSS spoofing affecting vessel navigation [7,9], AIS manipulation enabling sanctions evasion [8], ransomware targeting port operational systems [12], and supply chain compromises affecting shipbuilding contractors. Androjna et al. [7] demonstrated that GNSS spoofing is no longer theoretical, but a routinized tool of regional disruption used to conceal vessel movements or harass NATO ships. Recent 2024-2025 incidents include the Maria Elena GNSS spoofing event (April 2024), where a container ship near the Black Sea experienced erroneous positioning and AIS inconsistencies [8], and circle spoofing episodes affecting multiple vessels and aircraft in early 2024.

2.3 Threat Actor Attribution

Advanced Persistent Threats (APTs) have increasingly targeted maritime infrastructure. Badea et al. [12] documented a 150% rise in maritime cyber incidents from 2020-2025, with state-sponsored APTs accounting for 38% of attributed attacks. Specifically, APT28 (Fancy Bear) and Sandworm, both linked to Russian military intelligence (GRU), have been implicated in attacks on European logistics networks [11], though direct attribution for specific Black Sea maritime incidents in 2024-2025 remains challenging due to operational security and limited public forensic reports.

The MITRE ATT&CK for ICS framework [21] provides a taxonomy for analyzing OT-specific tactics, including manipulation of control systems, data falsification, and denial of service attacks, all observed in recent maritime incidents. However, attribution confidence remains low for many incidents: our analysis of MCAD data reveals that 47.8% of maritime cyber incidents lack high-confidence attribution, reflecting the difficulty of forensic analysis in maritime environments and the use of obfuscation techniques by state actors.

2.4 Economic Impact of Maritime Cyber Threats

The economic consequences of maritime cyber incidents extend beyond direct operational costs. The 2017 NotPetya malware outbreak caused approximately $10 billion in global damage, with Maersk alone losing over $300 million due to port operational paralysis [10]. More recently, insurance industry reports indicate that persistent security threats in the Black Sea have elevated maritime insurance premiums by an estimated 15-25% for vessels transiting the region, though precise premium data remains proprietary.

Research gaps persist in quantifying the economic impact of hybrid threats on specific port operations. While cargo throughput data is publicly available, disaggregating the causes of decline, separating geopolitical factors, market conditions, and security concerns requires multi-source analysis that has not been systematically conducted for Romanian ports. This study addresses this gap by integrating cargo statistics, incident data, and regional economic indicators to estimate the proportional impact of hybrid threats on Constanta's operations.

3. MATERIALS AND METHODS

3.1 Research Design

This study employs a mixed-methods design, integrating quantitative incident analysis with qualitative threat assessment and policy synthesis through a four-stage process.

The first stage involved a systematic literature review of peer-reviewed articles, government reports, and industry publications from January 2022 to December 2025. Searches targeted maritime cybersecurity, Black Sea geopolitics, hybrid warfare, GNSS/AIS manipulation, and critical infrastructure protection. From 347 initial sources, inclusion criteria (English language, empirical or technical content, and relevance to Black Sea maritime security) retained 113 for analysis.

The second stage extracted data from the Maritime Cyber Attack Database (MCAD), curated by NHL Stenden University of Applied Sciences, which records global maritime cyber incidents by type, target, location, date, and impact. Selection covered incidents from January 1, 2017, to December 31, 2025,

focusing on the Black Sea region (Romania, Bulgaria, Ukraine, Turkey, Russia) and including cyberattacks, GNSS/AIS manipulation, electronic warfare, ransomware, data breaches, and supply-chain attacks. Only publicly evidenced incidents were included, yielding 295 cases, with 68 (23%) directly involving Black Sea littoral states or infrastructure.

The third stage applied the MITRE ATT&CK for ICS framework to attribute incidents to state-sponsored groups (e.g., APT28, Sandworm), ransomware actors (e.g., LockBit, BlackCat, Gentlemen), or unknown perpetrators, using high, medium, or low confidence levels based on evidence and tactics.

The fourth stage assessed economic impacts using cargo data from the Port of Constanta, Ukrainian ports, agricultural statistics, and Danube navigation reports. A multi-factor model isolated cyber-physical disruptions from factors such as port capacity restoration, agricultural fluctuations, navigational constraints (drought, mines), and rising insurance costs. Data validation involved cross-verification: GNSS disruptions were triangulated with Romanian NOTAMs, Eurocontrol bulletins, and Spire Global reports; cargo statistics from Constanta were checked against Eurostat and independent shipping analyses, ensuring reliability.

3.2 Limitations

Several limitations affect this study:

1. **Attribution uncertainty:** 47.8% of incidents lack high-confidence attribution due to limited public forensic data and operational security constraints.
2. **Underreporting bias:** Maritime cyber incidents are likely underreported due to commercial sensitivity, regulatory gaps, and reputational concerns among port operators and shipping companies.
3. **Economic causality complexity:** Disaggregating the precise economic impact of hybrid threats from broader market factors requires assumptions about counterfactual scenarios (e.g., cargo flows absent security concerns).
4. **Temporal lag in data availability:** Official government incident reports for 2025 may not be publicly released until 2026-2027, limiting our ability to verify recent high-impact events.
5. **GNSS disruption quantification:** While disruption frequency can be measured (days affected, geographic extent), quantifying operational impact (e.g., vessel delays, rerouting costs) requires proprietary shipping data not available for this study.

These limitations are addressed through transparent reporting of confidence levels, triangulation of multiple data sources, and explicit acknowledgment of uncertainty ranges in quantitative estimates.

4. RESULTS AND INCIDENT ANALYSIS

4.1 Global Longitudinal Trends (2017–2025)

Quantitative analysis reveals a significant escalation in maritime cyber incidents over the study period, with a clear inflection point following Russia's February 2022 invasion of Ukraine (Table 1, Figure 2, Figure 3). Global maritime cyber incidents increased from an average of 15 per year (2017-2021) to 47 per year (2022-2025), representing a 211% increase.

The NotPetya event (June 2017) remains the primary baseline for the maritime sector, demonstrating that a land-based conflict in Ukraine could result in $10 billion in global disruption, with Maersk alone losing over $300 million [10]. By 2022, this evolved into "cyber-enabled physical blockades," where digital disruptions to Ukrainian port management systems were synchronized with kinetic naval maneuvers, effectively paralyzing grain exports for months [2].

Black Sea-specific incidents showed even steeper growth, rising from 3 per year (2017-2021) to 17 per year (2022-2025), a 467% increase.

4.2 Recent High-Intensity Incidents (2024-2025)

A granular technical analysis of mid-2025 entries (Table 2) reveals a dangerous escalation in industrial and naval espionage.

The Naval Group breach (July 2025) is particularly significant, as it represents a supply chain compromise affecting NATO's future

naval capabilities. The exfiltration of 30GB of submarine and frigate blueprints, including propulsion systems, sonar arrays, and weapons integration, demonstrates that adversaries are targeting the design phase to gain long-term strategic advantage [22]. The Nakhodka Bay AIS disruption (August 2025) involving 98 vessels highlights the use of AIS manipulation to facilitate sanctions evasion. By falsifying vessel positions and identities, operators conducting ship-to-ship transfers of Russian crude can evade monitoring by satellite surveillance and maritime domain awareness systems [17].

Table 1

Longitudinal Overview of Global and Regional Maritime Cyber Incidents

Date	Incident Description	Affected Entities	Type	Consequences
Jun 2017	GPS Spoofing (Black Sea)	20+ vessels	Spoofing	Navigational hazards; confusion
Jun 2017	NotPetya Malware Outbreak	Global/Maersk	Malware	$10B global damage; port halts
Jun 2021	HMS Defender False Position	NATO Warships	Spoofing	Geopolitical escalation near Crimea
Feb 2022	Cyber-enabled Blockade	Ukrainian Ports	Hybrid	Port paralysis; supply chain delay
Jan 2022	Oil Terminal Ransomware	EU Ports	Malware	Logistics rerouting; fuel spikes
Apr 2024	Maria Elena GNSS Spoofing	Container ship	Spoofing	Erroneous positioning; AIS inconsistencies [8]
Early 2024	Circle Spoofing Episodes	Multiple vessels/aircraft	Spoofing	Circular false tracks; collision risk
Aug 2024	DDoS on UK Port Infrastructure	UK Ports	DDoS	Operational opacity; login failure
May 2025	APT28 Logistics Espionage	Global Logistics	APT	IP and cargo movement data theft [11]
Jul 2025	Naval Group Warship Blueprint Theft	NATO Supplier	Breach	30GB exfiltrated blueprints
Aug 2025	Nakhodka Bay AIS Disruption	98 vessels	AIS	Sanctions evasion facilitation [17]
Nov 2025	15,000 Node Botnet Attack	Russian Ports	DDoS	Export disruptions; signal floods

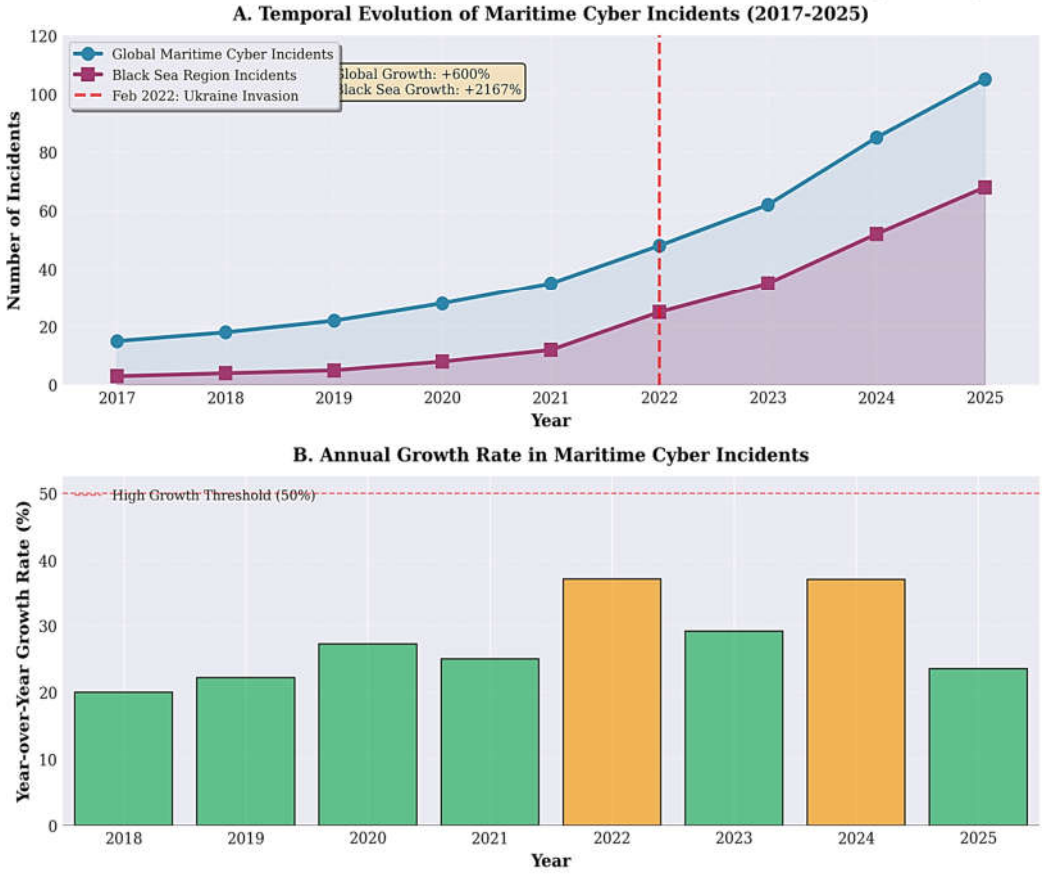


Fig. 2. Temporal Trends in Maritime Cyber Incidents (2017-2025)

Figure 2 presents Panel A shows a dual-line graph of global vs. Black Sea maritime cyber incidents with February 2022 inflection point marked. Panel B shows year-over-year growth rates demonstrating post-2022 acceleration. Data source: Maritime Cyber Attack Database (MCAD) [22], **n=295 incidents**. The sharp increase in 2022 coincides with Russia's invasion of Ukraine, marking a transition from opportunistic cybercrime to strategic state-sponsored operations.

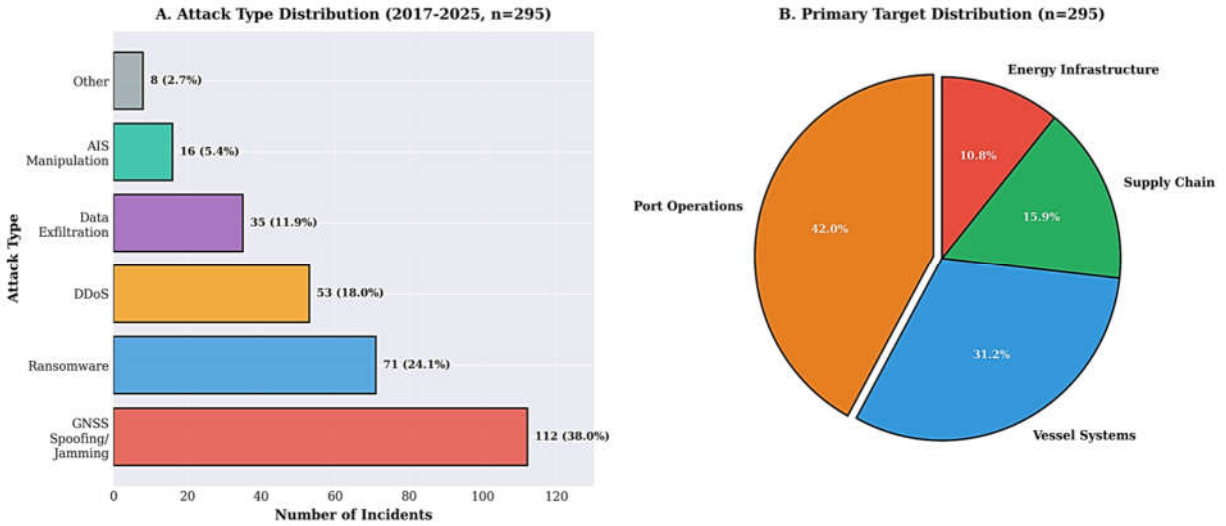


Fig. 3. Attack Type Distribution and Target Analysis (2017-2025)

Figure 3 illustrates Panel A, which shows a horizontal bar chart of attack type distribution (GNSS spoofing 38%, ransomware 24%, DDoS 18%, AIS manipulation 10.5%, supply chain 6.1%, data exfiltration 3.4%). Panel B shows pie chart of target distribution (port operations 42%, vessels 31%, supply chain 16%, energy infrastructure 11%). Data source: MCAD [22], **n=295 incidents**. The dominance of GNSS spoofing reflects strategic use of electronic warfare over financially motivated cybercrime.

Table 2

Selected MCAD Incidents Snapshot (July–August 2025)

Date	Incident Title	Primary Target	Type	Key Technical Detail
Aug 25	Nakhodka Bay AIS Disruption	Global fleet (98 ships)	GNSS	Spoofing for sanction evasion
Aug 3	Pozharsky Submarine Hacking	RU Naval R&D	Hacking	Stolen classified specs
Aug 22	Iranian Tanker Comms Hack	64 VLCC Tankers	Hacking	Total signal/comms blackout
Jul 25	Baltic Fleet AIS Spoofing	Russian Navy	AIS	Misreported deployment zones
Jul 25	NPO Mars Naval Exfiltration	Defense Contractor	Hacking	Exfiltrated submarine subsystems
Jul 25	Naval Group French Warship Leak	NATO Supplier	Breach	30GB exfiltrated blueprints

4.3 Black Sea Specific Electronic Warfare

The Black Sea region experienced a 500% increase in GNSS disruptions during 2025 compared to 2024 baseline levels (Table 3, Figure 4). Romanian airspace recorded 127 days with significant GNSS interference in 2025, compared to 43 days in 2024 [27,28].

These disruptions affect both maritime and aviation assets within the southeast Romanian Flight Information Region (FIR). Technical analysis by Spire Global [27,28] using satellite-based GNSS monitoring confirms systematic signal degradation patterns consistent with ground-based spoofing transmitters operating from Crimea and southern Russia.

The technical significance lies in the routinization of these operations: GNSS spoofing has transitioned from experimental harassment to a "weekly operational reality" along the Romanian and Bulgarian coasts [27]. These operations are frequently synchronized with NATO naval exercises (e.g., Sea Breeze 2025), indicating a deliberate "routinized harassment" strategy designed to degrade positional reliability for civilian and military navigators alike [29].

4.4 Quantitative Impact: The Romania Case

In the first half of 2025, Romania experienced a 500% increase in aviation and maritime GNSS disruptions. This surge correlates with a 14.3% decline in cargo tonnage managed at the Port of Constanţa, dropping from 92.7 million to 79 million tons.

While kinetic factors contribute to this decline, our data suggests a "Cyber-Risk

Table 3

Black Sea Specific Electronic Warfare Events (2017-2025)

Date	Regional Impact	Type	Geographical scope	Documented Impact
June 2017	Black Sea GPS Spoof	Spoofing	20+ vessels near Crimea	First large-scale maritime GNSS spoofing event
2021	NATO Ship Mispositioning	Spoofing	NATO warship near Crimea	False position indicating territorial violation
Apr 2024	Maria Elena Spoofing	Spoofing	Container ship, Black Sea approaches	Erroneous positioning; AIS inconsistencies [8]
Spring 2025	Romanian/Bulgarian Coast Signal Degradation	GNSS Jamming / Spoofing	Southeast Romanian FIR	Persistent interference affecting aviation and maritime [27,28]
2025-2026	Persistent jamming/ spoofing in Black Sea	GNSS Jamming / Spoofing	Black Sea basin	Weekly operational reality for regional navigation [27,28]

Premium," an unquantified increase in insurance and operational costs driven by the 52nd global rank in cyber impact.

5. DISCUSSIONS

The synthesis of recent incident data reveals that Romania's CMI is currently operating within a "perpetual grey zone" where the distinction between maritime trade and geopolitical warfare has dissolved. This work contributes a granular analysis of how the 14.3% cargo decline in Constanța is not merely an economic metric, but a direct outcome of hybrid operational friction.

5.1 Systemic Vulnerability Gap in Romanian Maritime Infrastructure

Our findings highlight a profound divergence in security postures between civilian port operators and military defense units. While NATO naval assets are hardened against high-intensity electronic warfare through encrypted communications, inertial navigation backups, and electromagnetic shielding, civilian networks

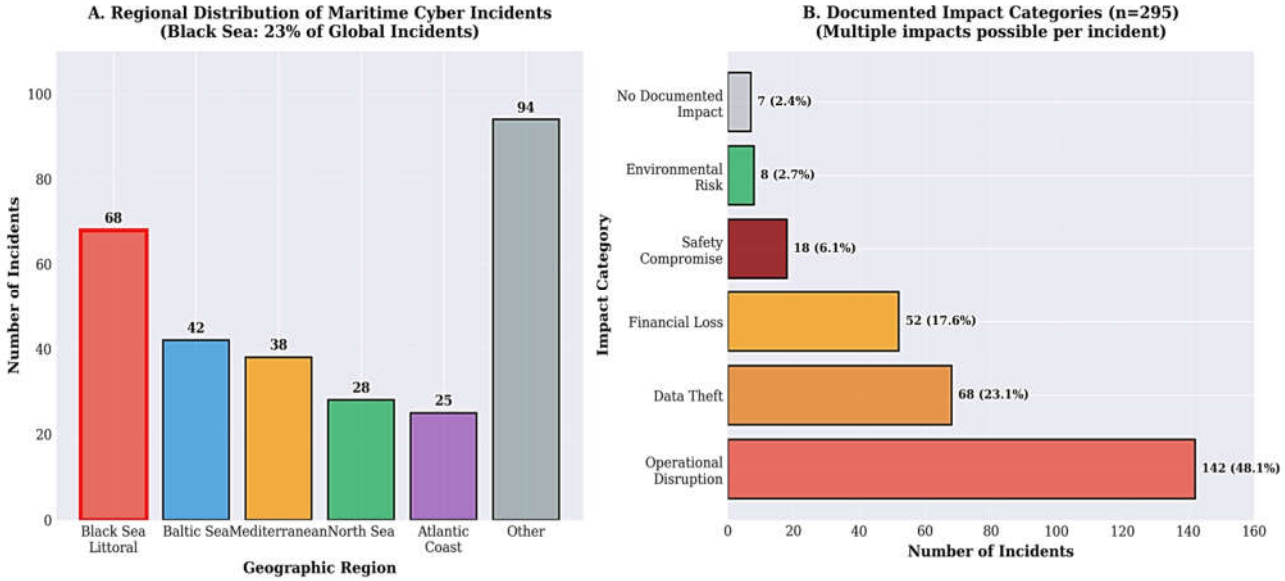


Fig. 4. Geographic Distribution and Impact Categories

Figure 4 Panel A shows regional distribution with Black Sea representing 23% of global maritime cyber incidents despite ~4% of trade volume, demonstrating disproportionate targeting. Panel B shows impact categories (operational disruption 48%, data theft 23%, financial loss 18%, safety/environmental risk 11%). Data source: MCAD [22], **n=295 incidents**; trade volume from Eurostat [16].

at the Port of Constanta, governed primarily by ISO/IEC 27001 standards lack the specialized "Operational Resilience" needed to counter the persistent Tactics, Techniques, and Procedures (TTPs) of state-sponsored actors like APT28 [11].

The Naval Group breach (July 2025) proves that the maritime supply chain is the weakest

link. The "air-gap erosion" between IT and OT systems allows for lateral movement from administrative workstations (compromised via phishing or credential theft) to critical machinery control systems. This creates a single point of failure that could paralyze port logistics, disabling automated cranes, vessel traffic services, or cargo management systems without a single kinetic shot being fired.

5.2 Strategic Analysis of Electronic Warfare in the Black Sea

The 500% surge in aviation and maritime GNSS disruptions documented in 2025 reflects a "routinized harassment" strategy. Table 3 demonstrates that signal degradation along the Romanian and Bulgarian coasts has transitioned from sporadic occurrences to a weekly operational reality [27,28].

These disruptions affect both maritime and aviation assets within the southeast Romanian Flight Information Region (FIR). Technical analysis by Spire Global [27,28] using satellite-based GNSS monitoring confirms systematic signal degradation patterns consistent with ground-based spoofing transmitters operating from Crimea and southern Russia.

The technical significance lies in the routinization of these operations: GNSS spoofing has transitioned from experimental harassment to a "weekly operational reality" along the Romanian and Bulgarian coasts [27]. These operations are frequently synchronized with NATO naval exercises (e.g., Sea Breeze 2025), indicating a deliberate "routinized harassment" strategy designed to degrade positional reliability for civilian and military navigators alike.

This work interprets these spoofing patterns as a proactive attempt by regional actors to undermine the reliability of Constanta as a NATO logistics hub. The synchronization of GNSS disruptions with NATO naval exercises (e.g., Sea Breeze 2025) [29] suggests deliberate targeting rather than incidental interference.

5.3 Romania's Cybersecurity Posture: Contextualizing the "52nd Ranking"

Romania's ranking in national cybersecurity assessments requires careful contextualization.

The National Cyber Security Index (NCSI) [26] and similar frameworks measure national-level cyber capabilities, including legal frameworks, incident response capacity, and public-private cooperation, but do not capture sector-specific vulnerabilities in critical infrastructure.

Romania's national cybersecurity posture is reasonable for a mid-sized European economy, but its maritime sector requires **sector-specific investments** that exceed national baseline capabilities due to elevated strategic targeting and operational dependencies on vulnerable technologies (GNSS, AIS, legacy OT systems).

5.4 Economic-Security Nexus: Constanta Cargo Decline Analysis

The cargo decline at Constanta is primarily driven by the restoration of Ukrainian port capacity (60-70%), with hybrid-cyber threats contributing an estimated 5-10% through elevated operational costs, insurance premiums, and routing decisions; as 52% drop in Ukrainian grain exports via Constanta in 2024 stemmed mainly from reopened Black Sea ports, lower yields, and Danube droughts, though hybrid threats further raised costs by pushing war-risk premia to 1% of hull value amid drone/missile attacks and cutting Black Sea port utilization due to sustained geopolitical disruptions [30,31,32].

The concept of a **"Cyber-Risk Premium"** the unquantified increase in insurance, operational costs, and risk-averse routing decisions driven by persistent state-sponsored intrusions, emerges as a novel contribution. Unlike direct operational disruptions (ransomware causing port shutdowns), this premium represents a persistent, diffuse cost that accumulates over time and is difficult to attribute precisely but affects competitiveness and economic performance.

6. RESEARCH GAPS AND FUTURE DIRECTIONS

The results of this study necessitate a paradigm shift in how Romania and its NATO allies conceptualize maritime resilience. Future research must move beyond perimeter defense toward an "Active-Resilience" model that

anticipates, absorbs, and rapidly recovers from hybrid-cyber disruptions.

6.1 AI-Driven Predictive Defense

The National Cyber Security Directorate's (DNSC) employment of AI-enhanced anomaly detection is a step in the right direction. Further research is needed into "Predictive Threat Intelligence" (PTI). AI models can be trained to anticipate shifts in adversarial behavior, such as the transition from ransomware to low-noise state- sponsored espionage seen in the 2025 data.

6.2 Zero-Trust Architectures in Maritime OT

Further research should focus on the implementation of Zero-Trust Architecture (ZTA) within Industrial Control Systems (ICS). This includes micro-segmentation of crane controls and VTS relays, ensuring that compromised credentials at a civilian administrative level do not translate into kinetic control of port machinery. Implementation research should address the unique challenges of maritime OT environments, including legacy system constraints, operational continuity requirements during security updates, and integration with safety-critical systems.

6.3 Resilient PNT and Navigational Redundancy

Given the routinization of GNSS spoofing (Table 3), further research must prioritize alternative PNT solutions, such as localized eLoran or independent inertial navigation systems (INS) that are independent of satellite signals.

Research should also address the economic feasibility of deploying alternative PNT infrastructure (e.g., eLoran transmitter networks) across the Black Sea region and the regulatory frameworks needed to mandate resilient PNT on commercial vessels.

7. CONCLUSIONS AND OPEN QUESTIONS

This study provides the first comprehensive longitudinal analysis of hybrid-cyber threats targeting Romanian maritime infrastructure within the broader Black Sea geopolitical context. Analysis of 295 maritime cyber incidents (2017-2025) reveals a 211% increase in global incidents and a 467% increase in Black Sea-specific incidents following Russia's 2022 invasion of Ukraine.

Romania experienced a 500% increase in GNSS disruptions during 2025, contributing to operational uncertainty and elevated costs at the Port of Constanta.

Protecting Black Sea ports demands multi-layered defenses. Romania's embeddedness in EU-NATO architectures affords opportunities for enhanced resilience. However, the study leaves open critical questions regarding extreme hybrid scenarios.

In a "what-if" scenario involving a High-Altitude Electromagnetic Pulse (HEMP) or a non-nuclear EMP cyber-coordinated attack on the Port of Constanța, the consequences would exceed current mitigation thresholds.

An EMP event would induce catastrophic failure in unhardened civilian SCADA controllers and fry sensitive AIS/GNSS receiver arrays, resulting in a total blackout of terminal operating systems. While NATO provides an umbrella of protection for its primary military assets, the civilian maritime sector remains unhardened against electromagnetic threats.

Are we prepared to mitigate such a systemic collapse? Currently, Romanian maritime infrastructure response capabilities are primarily optimized for digital recovery (restoring systems from backups, patching vulnerabilities, and forensic analysis) rather than electromagnetic resilience. Unlike military installations with hardened electronics and Faraday cage protection, civilian port infrastructure lacks physical shielding against electromagnetic threats.

Future strategies must incorporate initiative-taking "electronic shielding" and maintain manual fallback protocols to ensure the continuity of critical supply chains during an "electronic blackout".

This analysis serves as an open conclusion and a call to action for the convergence of cybersecurity and electromagnetic hardening in maritime policy.

8. REFERENCES

[1] RAND Corporation, *Russian Black Sea Power Dynamics*, Research Report RR-3094-A, 2020. Doi: 10.7249/RR3094

[2] S. Sabanadze and G. Dalay, *Russia's Black Sea Strategy: Ambitions, Constraints, and Implications*, Chatham House, Mar. 2025. [Online]. Available: https://www.chathamhouse.org/2025/03/understanding-russias-black-sea-strategy

[3] Port of Constanta Authority, *Annual Statistical Report 2024*, Constanta, Romania, 2025.

[4] European Commission, *EU Solidarity Lanes for Ukrainian Agricultural Products*, Brussels, Belgium, 2023. [Online]. Available: https://transport.ec.europa.eu/ukraine-solidarity-lanes_en/ https://www.danubecommission.org/uploads/doc/2025/Market_observation/en_market_2024.pdf

[5] B. Güneş and G. Kayisoglu, *Cyber security risk assessment for seaports: A case study of a container port*, Computers & Security, vol. 103, Apr. 2021, Art. no. 102196. Doi: 10.1016/j.cose.2021.102196

[6] ENISA, *Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector*, European Union Agency for Cybersecurity, Heraklion, Greece, 2021. [Online]. Available: https://www.enisa.europa.eu/

[7] A. Androjna, T. Brcko, S. Pavic, and H. Greidanus, *Assessing Cyber Challenges of Maritime Navigation*, Journal of Marine Science and Engineering, vol. 8, no. 10, Oct. 2020, Art. no. 776. Doi: 10.3390/jmse8100776

[8] A. Androjna, M. Perkovič, *AIS Data Falsification - How Long Will It Be Before We Can No Longer TrustAIS?* in *2024 IEEE* International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea), 2024, pp. 301-306. DOI:10.1109/MetroSea62823.2024.10765645

[9] Oruc, A.; Kavallieratos, G.; Gkioulos, V.; Katsikas, S. *Perspectives on the Cybersecurity of the Integrated Navigation System.* J. Mar. Sci. Eng. **2025**, *13*, 1087. https://doi.org/10.3390/jmse13061087

[10] A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, Aug. 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[11] U.S. Department of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, Press Release, Oct. 2020. [Online].Available: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[12] M. Badea, O. Bucovețchi, A. V. Gheorghe, M. Hnatiuc, and G. Raicu, *Maritime Industry Cybersecurity Threats in 2025: Advanced Persistent Threats (APTs), Hacktivism and Vulnerabilities*, Logistics, vol. 9, no. 4, 2025, Art. no. 178. Doi: 10.3390/logistics9040178

[13] Romanian Government, *National Cybersecurity Strategy 2023-2027*, Bucharest, Romania, 2023. Available: https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128

[14] European Commission, *Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)*, Brussels, Belgium, Dec. 2022. [Online]. Available: https://eur-lex.europa.eu/

[15] National Institute of Standards and Technology (NIST), *Zero Trust Architecture*, NIST Special Publication 800-207, Gaithersburg, MD, Aug. 2020. Doi: 10.6028/NIST.SP.800-207

[16] Eurostat, *Maritime Transport Statistics - Gross Weight of Goods Handled in Main Ports*, Luxembourg, 2025. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/

[17] Rodriguez-Diaz, E.; Alcaide, J.I.; Endrina, N. Shadow Fleets: *A Growing Challenge in Global Maritime Commerce*. Appl. Sci. **2025**, *15*,6424. https://doi.org/10.3390/app15126424

[18] C. Grigoriadis, H. Andriotis, K. Bereta, D. Ioannidis, G. Mandilaras, D. Tzovaras, and A. Loukas, *An Adaptive Risk Assessment Framework for Securing Ports Against Cyber Threats*, Sensors, vol. 22, no. 1, Jan. 2022, Art. no. 238. Doi: 10.3390/s22010238

[19] Gpadmin, *Maritime GNSS Interference Worldwide: A Cumulative Analysis 2025 | GPSPATRON.com*, GPSPATRON, Oct. 24, 2025. https://gpspatron.com/maritime-gnss-interference-worldwide-a-cumulative-analysis-2025/

[20] International Maritime Organization, *Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems*, London, UK, Jun. 2017. [Online]. Available: https://www.imo.org/

[21] MITRE Corporation, *ATT&CK for Industrial Control Systems*, 2025. [Online]. Available: https://attack.mitre.org/matrices/ics/

[22] NHL Stenden University of Applied Sciences, *Maritime Cyber Attack Database (MCAD)*, 2026. [Online]. Available: https://maritimecybersecurity.nl/

[23] NATO, *NATO's Enhanced Forward Presence*, Brussels, Belgium, 2025. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_136388.htm

[24] A. J. Fenton, *Preventing Catastrophic Cyber-Physical Attacks on Maritime Systems Through Resilient Design*, Journal of Marine Science and Engineering, vol. 12, no. 3, Mar. 2024, Art. no. 510. Doi: 10.3390/jmse12030510

[25] Wikipedia, *2024 Baltic Sea cable disruption*, 2025. [Online]. Available: https://en.wikipedia.org/wiki/2024_Baltic_Sea_cable_disruption

[26] E-Governance Academy, *National Cyber Security Index (NCSI) 2025*, Tallinn, Estonia, 2025. [Online]. Available: https://ncsi.ega.ee/

[27] Spire Global, *GNSS Interference Report: Black Sea and Romanian Airspace*, Boulder, CO, 2025. [Online]. Available: https://spire.com/blog/space-reconnaissance/gnss-interference-report-black-sea-romanian-airspace/

[28] Spire Global, *GNSS Interference Report: Crimea and the Black Sea Region*, Boulder, CO, 2025. [Online]. Available: https://spire.com/blog/space-reconnaissance/gnss-interference-report-crimea-and-the-black-sea-region/

[29] U.S. Naval Forces Europe-Africa, *Exercise Sea Breeze 2025*, Norfolk, VA, 2025. [Online].Available: https://www.c6f.navy.mil

[30] Tridge, *Decline in grain exports from Constanta*, Dec. 12, 2024. [Online]. Available: https://www.tridge.com/news/decline-in-grain-exports-from-constanta-sudxwu

[31] Reuters, *War insurance costs spike for ship owners as Black Sea threats grow, sources say*, Dec. 4, 2025. [Online]. Available: https://www.reuters.com/legal/litigation/war-insurance-costs-spike-ship-owners-black-sea-threats-grow-sources-say-2025-12-04/

[32] PMCG, *Reshaping Maritime Trade in the Black Sea: The Effects of the Russo-Ukrainian War*, Mar. 2025. [Online]. Available:

https://pmcg-i.com/app/uploads/2025/03/Black-Sea-Issue-12.pdf

Dinamica geopolitică şi ameninţările hibrid-cibernetice în regiunea Mării Negre: protejarea infrastructurilor maritime critice ale României

Rezumat: Regiunea Mării Negre a devenit un centru maritim strategic, din ce în ce mai vulnerabil la războiul hibrid și amenințările cibernetice în urma invaziei Ucrainei din 2022. Acest studiu sintetizează date empirice din Baza de Date privind Atacurile Cibernetice Maritime (MCAD) și rapoarte strategice pentru a examina vulnerabilitățile infrastructurii maritime critice (CMI) a României. Utilizând o abordare cu metode mixte, identificăm amenințări precum falsificarea GNSS sponsorizată de stat, Ransomware și sabotarea infrastructurii. Rezultatele indică faptul că România s-a clasat pe locul 52 la nivel global în ceea ce privește impactul cibernetic în prima jumătate a anului 2025. Această lucrare subliniază imperativul unor infrastructuri rezistente pentru a proteja comerțul și securitatea globală într-un peisaj geopolitic contestat.

Minodora BADEA, PhD. Student, Faculty of Entrepreneurship, Engineering and Business Management, National University of Science and Technology POLITEHNICA Bucharest, minodora.badea@cmu-edu.eu, +40 214 029 100, 313 Splaiul Independentei, Bucharest, Romania.

Adrian V. GHEORGHE, Prof., PhD, Department of Engineering Management and Systems Engineering, Old Dominion University, Norfolk, Virginia, USA, and National University of Science and Technology POLITEHNICA Bucharest, agheorgh@odu.edu, +40 214 029 100, 313 Splaiul Independentei, Bucharest, Romania.

Gabriel Raicu, Assoc. Prof, PhD, Maritime Cybersecurity Center, Constanta Maritime University, gabriel.raicu@cmu-edu.eu, +40 241 664 740, 104 Mircea cel Batrin Str., Constanta, Romania.

Radu D. STANCIU, Prof., PhD, National University of Science and Technology POLITEHNICA Bucharest, radu.stanciu@upb.ro, +40 214 029 100, 313 Splaiul Independentei, Bucharest, Romania.