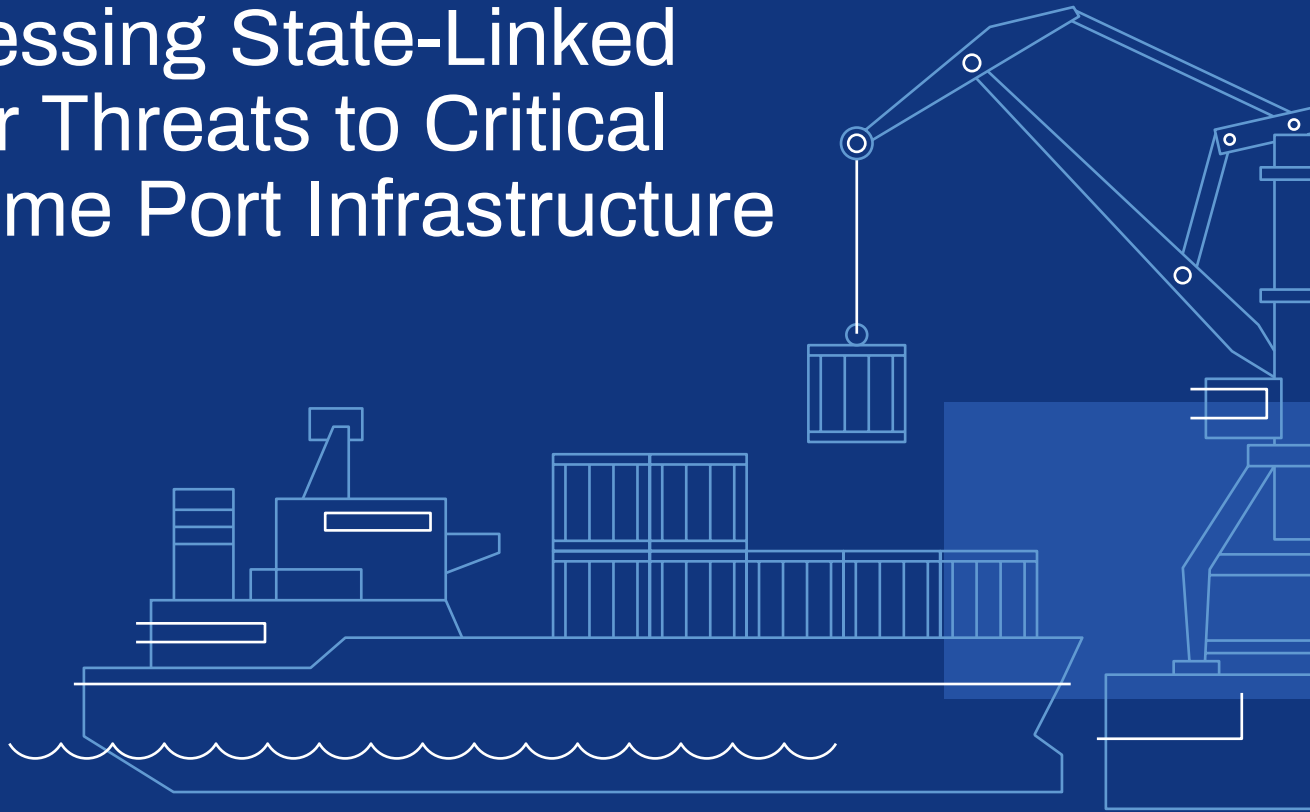




Policy Brief

Addressing State-Linked Cyber Threats to Critical Maritime Port Infrastructure



Executive Summary

Maritime ports handle 80% of global trade and serve as critical nodes in NATO's defence logistics network, yet they face unprecedented cybersecurity threats from state-linked actors. Recent intelligence shows a high frequency of cyber attacks affecting port facilities across Europe and the Mediterranean, with a significant proportion of these attacks traced back to threat actors originating from Russia, Iran, and China.¹ This trend highlights the pressing need for coordinated policy and security responses. Our analysis reveals that nearly all surveyed countries have experienced cyber attacks within the past five years, with access control systems and vessel traffic management systems identified as the main reported risks.²

The blurring of responsibilities between national and international, public and private entities particularly challenges current NATO civil-military coordination mechanisms, as most critical port infrastructure remains under civilian control while serving essential military logistics functions. The current NATO Alliance Maritime Strategy lacks formalised frameworks for engagement with commercial port operators, despite their critical role in maritime security and NATO logistics operations.

Information and communication technology (ICT) and operational technology (OT) underpin all land and sea-based maritime operations. Maritime port cybersecurity requires immediate policy intervention to establish sector-specific intelligence sharing networks, coordination mechanisms, and resilience standards. The recommendations outlined in this brief provide a framework for strengthening NATO's maritime cyber defence while preserving the commercial efficiency that makes the ports economically vital. The cost of inaction far exceeds the investment required for comprehensive maritime cybersecurity.

¹ The Cyber Threat Intelligence (CTI) companies EclecticIQ and Silobreaker have kindly provided us data and threat reports during this research period.
² During the research, NATO CCDCOE conducted a cybersecurity survey of maritime port infrastructure amongst NATO and partner countries in the period 29.11.24 - 14.02.25. The goal was to assess the current security postures, challenges, and best practices. This survey collected responses from 9 countries out of 30 countries representing military and government entities operating maritime ports across multiple geographical regions.

Authors

James Austin (OPS, CCDCOE)
Maj. Andrii Davydiuk (P&C, CCDCOE)
Adam Dollimore (STRAT, CCDCOE)
Aleksi Kajander (LAW, CCDCOE)
Erik Kursetgjerde (STRAT, CCDCOE)

Contributors

Gen. Valerii Zaluzhnyi — Ambassador Extraordinary and Plenipotentiary of Ukraine to the UK of Great Britain and Northern Ireland; Permanent Representative of Ukraine to the IMO.
Maj. Gen. Volodymyr Koval — Deputy Chief, GS of the AFU (Aug 2021 – Feb 2024); PhD (Mil.Sci.), Sr. Research Fellow; Military Expert, NGO Center for Military Strategy and Technologies.
Brig. Gen. Oleksandr Potii — Head of State Service of Special Communications and Information Protection of Ukraine (SSSCIP); Doctor of Technical Sciences, Professor.
Cdr. Mike Widmann (USN) — NATO Allied Maritime Command (MARCOM)

Introduction

Maritime port facilities represent cornerstone assets for national economic stability, energy security, and NATO's operational logistics framework. With ports facilitating approximately 80% of international trade, their strategic importance extends beyond commercial considerations to serve as vital nodes in national defence strategies and crisis response capabilities.³ The strategic value of maritime facilities as hybrid warfare targets was demonstrated when Russia initiated a naval blockade of Ukraine's Black Sea ports. Occurring two weeks prior to its full-scale invasion on 24th February 2022, the blockade disrupted global supply chains and contributed to rising food prices worldwide.⁴

Traditional risks continue to play a major role in maritime port infrastructure security, but rapid digitalisation has created cybersecurity vulnerabilities that both state-sponsored and state-linked adversaries are actively exploiting. The maritime industry is facing rapid digital transformation, with ports at the forefront of this evolution. The complexity of today's modern port operations has increased significantly, with the number of integrated and interconnected systems increasing, driven by the need for improved efficiency, real-time monitoring, and optimised operations.⁵

This digital transformation has created a multitude of challenges. The convergence of IT with OT has become essential for improving efficiency, security, and sustainability, yet this integration represents significant challenges due to differences in system architecture, security requirements, and operational priorities.

The Challenge of Digitalisation

The maritime sector encompasses many stakeholders and integrated systems that require a delicate balance between operational efficiency and risk management. The convergence of IT and OT represents a multifaceted transformation in modern operations and demands meticulous coordination between the traditional industrial control systems (ICS) and contemporary digital solutions, ensuring that operational continuity and data security remain uncompromised.

Historically, port operations have relied on legacy OT systems, such as Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems, designed primarily for operational reliability rather than cybersecurity. Many ports operate with legacy OT systems that were not originally designed for internet connectivity. Integrating them with modern ICT networks introduces significant vulnerabilities and new threat vectors.

The 2017 NotPetya cyber attack exemplifies this risk through its spillover effect on Maersk. The global shipping company suffered a \$300 million loss when malware spread rapidly across ICT and OT domains due to poor network segmentation. Port operations were also disrupted in major hubs such as Rotterdam and Los Angeles, demonstrating how cybersecurity incidents can cascade across maritime infrastructure networks.⁶ NotPetya was publicly attributed to Russian state-sponsored actors by the UK, US, and Australia in 2018.⁷

NotPetya demonstrates that even if maritime infrastructure is not the original intended target, the spillover effect becomes inevitable due to increased connectivity. As such, critical maritime infrastructure cannot afford to lag behind in cybersecurity, as threats are capable of impacting even unintended targets. Therefore, considering that maritime infrastructure is crucial from a financial and military perspective, it is a magnet for all types of malicious cyber attacks.

3 UNCTAD. (2023). "Review of Maritime Transport 2023: Towards a Green and Just Transition." Review of Maritime Transport.
4 The Guardian. (June 9, 2022). "The Black Sea Blockade: Mapping the Impact of War in Ukraine on the World's Food Supply."
5 Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis – How to reduce threats? Transactions on Maritime Science, 8(1)
6 Greenberg, A. (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired.
7 UK Foreign, Commonwealth & Development Office. (February 15, 2018). "Foreign Office Minister Condemns Russia for NotPetya Attacks." GOV.UK.

Threat Landscape

Maritime port facilities face a range of threats from state-sponsored advanced persistent threats (APTs), financially motivated cybercriminals, and politically driven hacktivists. These threats are remarkably consistent regardless of geographical location, and the tactics, techniques, and procedures (TTPs) are the same if not identical across Europe, the Americas, and the Asia Pacific regions. The CCDCOE survey that was conducted with member and partner countries demonstrates that the most common attacks against maritime facilities include denial-of-service attacks and significant data breaches, followed by phishing or malware delivery and ransomware.

State-Sponsored Cyber Attacks

Since Russia's full-scale invasion of Ukraine in 2022, Moscow has expanded its use of unconventional attacks, including sabotage, disruption, and support for extremist groups. These attacks often target critical infrastructure with the dual aims of disrupting services and undermining trust in democratic institutions. In May 2025, multiple NATO and European nations published a joint cybersecurity advisory stating that APT28 (Fancy Bear) - attributed to the Russian military intelligence service (GRU) - had targeted Western logistics entities and technology companies across virtually all transport modes.⁸ According to the Nordic Maritime Cyber Resilience Centre (NORMA Cyber), Fancy Bear has targeted maritime organisations, logistics providers, and air traffic control systems in at least 11 countries.⁹

Iranian APTs operating under the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS) have orchestrated sophisticated campaigns targeting critical ports and shipping facilities as part of a broader geopolitical objective to disrupt adversaries and assert regional influence. Groups such as Yellow Lideric (Imperial Kitten), APT35 (Charming Kitten), MuddyWater, and the IRGC-affiliated cyber persona, Cyber Aveng3rs, have systematically targeted ports in Israel, Egypt, and the broader Eastern Mediterranean.¹⁰ Attacks have targeted major Israeli maritime ports including Ashdod and Haifa (the latter of which handles 88% of Israel's maritime logistics), Israeli oil refinery BAZAN Group, and Egypt's Port Said, all representing critical nodes in global supply chains.¹¹

In February 2024, Australia, Canada, New Zealand, the UK, and the US publicly stated, "*China state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure*".¹² This includes the maritime transportation sector. In April 2024, CISCO TALOS identified that a state-sponsored actor - dubbed ArcaneDoor

- used custom malware leveraging known vulnerabilities to collect maritime and financial intelligence.^{13, 14} Consisting of significant ICT infrastructure, the campaign spread across coastal facilities in numerous countries that were identified as strategically important to China.¹⁵ Additionally, the China-linked actor Mustang Panda has been found targeting maritime transportation companies using various attack vectors, including infected USB drives.¹⁶

State-sponsored cyber attacks highlight the need for both preparation and effective responses against states infringing international law through cyber means. This need is elevated in the case of critical infrastructure such as port facilities, as cyber operations against ports can not only cause financial losses but disrupt military logistics. As a result, the need for collective responses through lawful means, such as retorsion in the form of economic sanctions, will be critical in deterring state-sponsored cyber attacks. The Cyber Diplomacy Toolbox has filled this role for the EU and has enabled targeted "cyber sanctions" as a response to significant cyber attacks.¹⁷ Consequently, a similar arrangement to the Cyber Diplomacy Toolbox could provide deterrence against cyber attacks against NATO's critical maritime infrastructure for NATO member states.

Financially-Motivated Cybercriminals

The lack of clarity between state-sponsored actors and cybercriminal groups presents particular challenges for attribution and response. In January 2022, ransomware attacks unfolded over several days, targeting at least 17 major oil port terminals in Belgium, the Netherlands, and Germany. These attacks affected some of the largest ports in the region, such as Hamburg, Ghent, Antwerp-Zeebrugge, and Rotterdam. European prosecutors and cybersecurity officials investigating these attacks found that ransomware forced oil suppliers to reroute their products, disrupting operations. Further, this could disrupt and delay military operations in the region. Investigations by Antwerp public prosecutors' office highlighted the complexity of attributing such cyberattacks.^{18, 19} According to Germany's Federal Office for Information Security (BSI), the state-linked BlackCat ransomware group was responsible for these attacks.²⁰ Meanwhile, the now-defunct state-linked Conti ransomware group was identified as responsible for the cyber attack on Ghent-based international terminal operator Sea-Invest.²¹

According to NORMA Cyber, at least 45 maritime organizations were attacked with ransomware in 2024, with the actual number likely to be much higher.²² These incidents highlight the ongoing and significant threat ransomware poses to critical infrastructure. Moreover, in the case of cybercriminals disrupting maritime

8 U.S. Department of Defence & NSA. (May 21, 2025). "Russian GRU Targeting Logistics Infrastructure." Cybersecurity Advisory.

9 Norma Cyber. (2024). "Annual Threat Assessment." Norma Cyber.

10 EclecticIQ. (2024). "Advanced Persistent Threat Activities Targeting Middle Eastern Maritime Ports: Focus on Islamic Republic of Iran Linked Groups." EclecticIQ Threat Research.

11 CISA. (December 1, 2023). "Cybersecurity Advisory AA23-335A." CISA.

12 CISA. (February 7, 2024). "Cybersecurity Advisory AA24-038A." CISA.

13 Cisco Talos Intelligence. (April 24, 2024). "ArcaneDoor: New Espionage-Focused Campaign Found Targeting Perimeter Network Devices." Talos Intelligence Blog.

14 Censys. (2024). "Analysis of ArcaneDoor Threat Infrastructure Suggests Potential Ties to Chinese-Based Actor." Censys Blog.

15 The Hacker News. (June 5, 2024). "China-Linked Hackers Suspected in ArcaneDoor Cyberattacks Targeting Network Devices."

16 ESET. (2024). "ESET Research APT Report: Russian Cyberattacks in Ukraine Intensify - Sandworm Unleashes New Destructive Wiper." ESET Research.

17 Council of the European Union. (2024). "Sanctions Against Cyber Attacks." European Council.

18 Reuters. (February 1, 2022). "Shell Re-Routes Oil Supplies After Cyberattack on German Firm." Reuters.

19 The Record. (2022). "String of Cyberattacks on European Oil and Chemical Sectors Likely Not Coordinated, Officials Say." The Record.

20 ZDNet. (2022). "BlackCat Ransomware Implicated in Attack on German Oil Companies." ZDNet.

21 eSentire. (2022). "Conti Ransomware Gang Claims 50 New Victims Including Oil Terminal Operator Sea-Invest." eSentire Security Advisory.

22 Norma Cyber. (2024). "Annual Threat Assessment." Norma Cyber.

critical infrastructure, the effective cooperation of both civilian and military entities is essential. The need for clear responsibilities and efficient cooperation between law enforcement agencies, the civilian operators of critical infrastructure, and the military is crucial in responding to and deterring the actions of cybercriminals. As a result, the national frameworks of NATO nations must be capable of fostering the necessary cooperation to respond to and fight cybercrime.

Politically-Motivated Hacktivists

In addition to espionage and financially-driven threats, maritime organisations regularly face the threat of disruption of services by politically-motivated groups. One of the most prominent groups threatening maritime infrastructure is the pro-Russian hacktivist group NoName057.

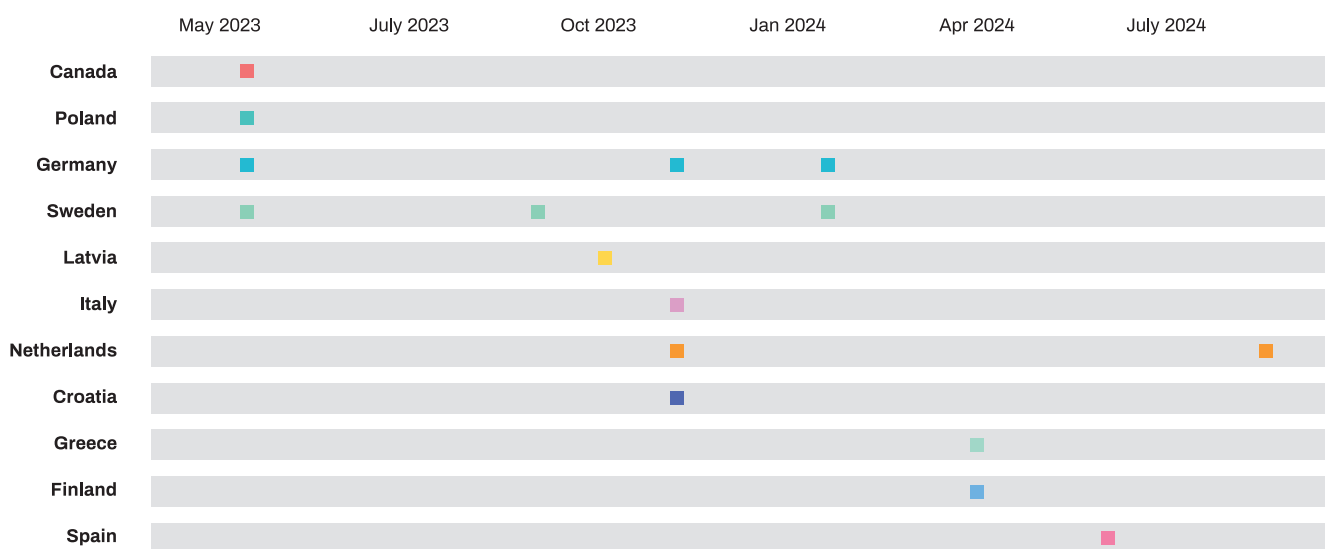
NoName057 represents one of the most active pro-Russian hacktivist groups. They focus on using distributed denial-of-service (DDoS) attacks, often forming alliances with other groups such as People’s Cyber Army, Z-Pentest, and Jus0t Evil Hacker Group. These groups target countries and organisations perceived as Russia’s adversaries, with particular focus on Ukraine, countries supporting Ukraine, and NATO/EU member countries. The group’s primary tool for DDoS attacks is a crowdsourced botnet project called DDoSia. NoName057 often relies on politically motivated hacktivists willing to install a bot on their computers to participate in the attacks, potentially with financial incentives for successful operations. According to the public Telegram channel of the pro-Russian hacktivist group, several critical port facilities across Western Europe have been targeted. On June 11 2023, the Port of Rotterdam, Europe’s busiest port, suffered a DDoS attack attributed to NoName057, disrupting the port’s main website, leading to a short-term operational disruption.²³

In addition to NoName057, various other pro-Russian groups have attempted to disrupt maritime port infrastructure through DDoS attacks. On August 16, 2023, Poland’s Port of Gdynia was targeted by a pro-Russian hacktivist group, Net Worker Alliance, through a DDoS attack. This attack aimed to disrupt the port facility’s digital systems, including maritime traffic management and cargo handling, potentially resulting in delays and economic losses due to interrupted supply chains. On August 6 2024, the Cyber Army of Russia, a group closely aligned with NoName057, was reportedly responsible for DDoS attacks on both the Port of Felixstowe and the Port of Tyne in the UK. The Port of Felixstowe, the UK’s largest container port, serves as a hub for ships connecting the UK with global markets, while the Port of Tyne, located in North East England, is one of the country’s significant deep-sea ports, playing a vital role as a trading gateway to worldwide markets. According to the BBC, a port spokesman confirmed that OT had not been affected, and that all website accessibility was restored quickly, with the port working with all relevant parties to investigate the source of the attack.²⁴

The actions of NoName057 demonstrate that political hacktivist groups represent a credible threat to the functioning of port facilities. Similar to financially-motivated cybercriminals, the efficient cooperation of law enforcement, civilian operators of maritime infrastructure, and the military is crucial in responding to the actions of political hacktivists. Moreover, frameworks such as the EU’s Cyber Diplomacy Toolbox represent a key means of deterrence against the actions of private individuals, such as hacktivists or cybercriminals, through targeted individual restrictive measures. Without real consequences for the individuals conducting cyber attacks, either for political or financial reasons, deterrence will not be effective.

FIGURE 1 - TARGETED PORT FACILITIES IN DDOS ATTACKS.

DDoS Attacks by NoName057(16) Against Port Facilities (2023-2024)



23 Silobreaker. (2025). "Russian Actors Targeting CI. Internal report." Silobreaker Threat Intelligence.
 24 BBC News. (2024). "Port of Tyne Website Hit by Cyber Attack." BBC News.

Policy Gaps in Current Frameworks

NATO Alliance Maritime Strategy Limitations

The NATO Alliance Maritime Strategy is from 2011 and identifies maritime security as one of its four foundational pillars, yet it requires updating to comprehensively address emerging threats, particularly cyber threats to maritime infrastructure.²⁵ The current strategy lacks formalised frameworks for engagement with commercial port operators, despite their critical role in maritime security and NATO logistics operations. The traditional distinction between civilian and military maritime security becomes increasingly problematic when state adversaries systematically target commercial ports that handle military logistics. The blurring of responsibilities particularly challenges current NATO civil-military coordination mechanisms, as most critical port infrastructure remains under civilian control while serving essential military logistics functions.

Combining physical and cyber operations against maritime infrastructure, the hybrid warfare approach exposes gaps in the current NATO Alliance Maritime Strategy frameworks. These frameworks were developed before the emergence of sophisticated state-linked cyber campaigns targeting allied ports, necessitating comprehensive updates to address the convergence of cyber and physical domain threats. The strategy's current focus on traditional maritime threats requires expansion to encompass the full spectrum of contemporary threats facing maritime infrastructure.

The maritime sector remains a high-risk cyber environment requiring a comprehensive understanding of the maritime ICT and OT ecosystem.²⁶ Ports represent some of the most prominent examples of critical infrastructure where physical and digital domains converge, particularly through their dependence on energy systems. This interdependence means that not only can ports themselves be targeted by cyber attacks, but so too can the power generation and distribution facilities that enable their operation. Such attacks could result in cascading effects, impacting both

military and civilian logistics chains. As a result, port cybersecurity cannot be treated in isolation; it must be addressed as a complex, multi-layered challenge that includes the resilience of supporting energy infrastructure.²⁷ This underscores the need for dedicated strategic attention to port cybersecurity within NATO's broader maritime posture.

Existing Cybersecurity Framework Limitations

Unlike traditional security risk management, addressing cybersecurity risks presents unique and complex challenges for port operators and their maritime facilities. Many lack the internal cybersecurity expertise, established organisational structures, standardised processes, and dedicated resources to assess and mitigate cyber threats effectively. Risk perception among port operators surveyed by NATO CCDCOE reveals a consensus concerning challenges for maritime infrastructure cybersecurity. When asked to assess their current cybersecurity risk level, most respondents classified it as moderate, indicating awareness of risk elements present. The consistency in risk assessment can suggest a shared understanding of the cybersecurity challenges across different geographical regions and operational levels.

Current cybersecurity frameworks, while comprehensive, face implementation challenges specific to the maritime environment. The International Ship and Port Facility Security Code focuses primarily on the physical security of ports and vessels, providing guidance on planning and assessing security at ships and ports, but lacks comprehensive cybersecurity provisions. The International Association of Ports and Harbors Cybersecurity Guidelines offer cybersecurity guidance on identifying and assessing port risks during operations, yet implementation remains inconsistent across different jurisdictions and port authorities.

Recommendations

Revision of the NATO Alliance Maritime Strategy

The NATO Alliance Maritime Strategy, last updated in 2011, requires revision to integrate cybersecurity as a fundamental component of maritime security. This revision should formalise frameworks for engagement with commercial port operators, acknowledging their critical role in maritime security and NATO logistics operations. The strategy should also address the blurred boundaries between civilian and military maritime security. Further, the strategy should establish protocols for NATO engagement during significant cyber incidents affecting maritime infrastructure, including coordination mechanisms between military commands and civilian port authorities. The revised strategy should reflect the strategic importance of cyber resilience in modern port operations and logistics chains.

Establish and Actively Participate in Structured Threat Intelligence-Sharing Networks

Develop and activate a formal threat intelligence-sharing platform (e.g., MISP) specifically for maritime cyber threats, building on existing frameworks while addressing the unique requirements of maritime cybersecurity. The platform should facilitate not only threat intelligence sharing but also best practices, lessons learned, and coordinated response planning among maritime stakeholders. The network could build on successful models like Norma Cyber, ReCAAP ISC, and NMIO Global Maritime Community of Interest.

25 North Atlantic Treaty Organization. (2011). Alliance Maritime Strategy. Brussels: NATO.

26 Halisdemir, E., et al. (2023). Cyber Threat Intelligence: Mitigating Risks to Maritime Security. Cooperative Cyber Defence Centre of Excellence (CCDCOE)

27 Zaluzhnyi, V. (2025). Ensuring the energy resilience of Ukrainian seaports under current conditions of armed conflict. In Proceedings of the 2nd Scientific and Practical Conference "Resilience of Dynamic Systems" (pp. 5–9).

Establish Dedicated Liaison Roles and Coordination

Mechanisms

NATO should establish a dedicated liaison role between NATO Maritime Command (MARCOM) and national port cybersecurity authorities, developing comprehensive playbooks for coordinated responses (e.g., the EU Cyber Diplomacy Toolbox) to significant cyber incidents in port infrastructure. The liaison function should facilitate regular information exchange and look into incorporating port cybersecurity scenarios into broader NATO maritime exercises such as Dynamic Mongoose and Trident Juncture.

Develop Maritime Cybersecurity Working Groups

Industry stakeholders should establish international working groups under the International Maritime Organization's auspices to develop maritime-specific security standards and ensure consistency across the Alliance. These working groups should bring together port operators, shipping companies, government agencies, and cybersecurity experts to develop comprehensive standards that address the challenges of maritime cybersecurity. The groups should additionally focus on developing practical guidance for implementing existing cybersecurity frameworks in maritime environments, addressing the specific challenges of OT and IT convergence in port operations. This includes developing sector-specific implementations of frameworks such as the NIST Cybersecurity Framework and NIS2.

Way forward

Cyber threats targeting critical maritime infrastructure have created an urgent imperative for action. The recommendations outlined in this brief provide a framework for addressing current vulnerabilities while building resilience for the future.

As the security climate hardens, more destructive measures are anticipated to target critical infrastructure. China's increasing targeting of US critical infrastructure – for example, Volt Typhoon pre-positioning in US CNI - has been linked with increased tensions over Taiwan, which is also expected to continue to rise.²⁸ Russian and Iranian state-sponsored attacks illustrate the highly developed nature of threats facing port facilities, while the ransomware and hacktivist groups have demonstrated how non-state actors can have as significant an impact as state-sponsored actors.

The motivation for the threat actors aligns with the broader geopolitical objectives, using cyber attacks as a tool for statecraft to gather intelligence, disrupt operations, and project influence. Protecting high-risk port infrastructure presents serious challenges that directly impact the safety, efficiency, and reliability of maritime operations. Nations must recognise these evolving threats to their critical maritime infrastructure and develop comprehensive strategies to enhance resilience while enabling continued modernisation and digital transformation of port operations.

This requires prioritisation of cybersecurity in maritime strategy, conducting regular joint exercises that simulate cyber scenarios, and creating mechanisms for threat intelligence sharing across national boundaries. The NATO Alliance Maritime Strategy requires a revision to fully integrate cybersecurity, recognizing that protecting allied maritime capabilities extends beyond physical assets, where adversaries increasingly target critical infrastructure through cyber means.

NATO CCDCOE offers exercises that serve as platforms to practise defending critical infrastructure and strengthen collaboration between civilian and military stakeholders. The Locked Shields exercise, the world's largest international live-fire cyber defence exercise, focuses on defending national ICT systems and critical infrastructure under real-time attacks in a competitive environment. These exercises emphasise a comprehensive national defence approach, recognising that protecting a country's critical infrastructure requires coordinated responses across all sectors that underpin economic and security resilience. The exercise's emphasis on realistic scenarios, cutting-edge technologies, and the complexity of massive cyber incidents - including strategic decision-making and legal and strategic communications aspects - makes it an ideal platform for training civilian and military personnel in coordinated cyber defence.

The rapid digitalisation of critical infrastructure has increased the attack surface of maritime port facilities, which requires approaches that take these developments into account to protect this infrastructure more successfully. Success will depend on integrating cybersecurity considerations into the Alliance Maritime Strategy, which should emphasize the effective coordination between civilian and military stakeholders. The interconnected nature of modern port operations makes them a tempting target for adversaries and vulnerable to unintended effects due to the spillover effect (e.g., NotPetya). Therefore, a comprehensive transformation of maritime cybersecurity governance is not just recommended, but essential for preserving Allied maritime operational capacity.

Acknowledgments

This brief is based on NATO CCDCOE research and recent threat intelligence analysis supported by the CTI companies EclecticIQ and Silobreaker, which have informed our understanding of the evolving maritime cyber threat landscape in developing these policy recommendations. We also acknowledge the valuable insights from Cdr. Mike Widmann and NATO Allied Maritime Command (MARCOM), whose expertise contributed to shaping the maritime military logistic dimension of this brief.

About NATO CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia is the leading dedicated hub for NATO allies and like-minded nations to jointly raise their cyber defence capabilities. The NATO-accredited Centre provides valuable expertise on cyber defence across strategic, legal, operational, and technical realms. Today, 39 Allied and Partner countries are contributing to the work of the Centre.

Disclaimer. This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). The expressions reflected are those of the author(s) alone; publication by the Centre should not be interpreted as endorsement thereof by the Centre, its Sponsoring Nations or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation. Please contact industry@ccdcoe.org with any further queries.