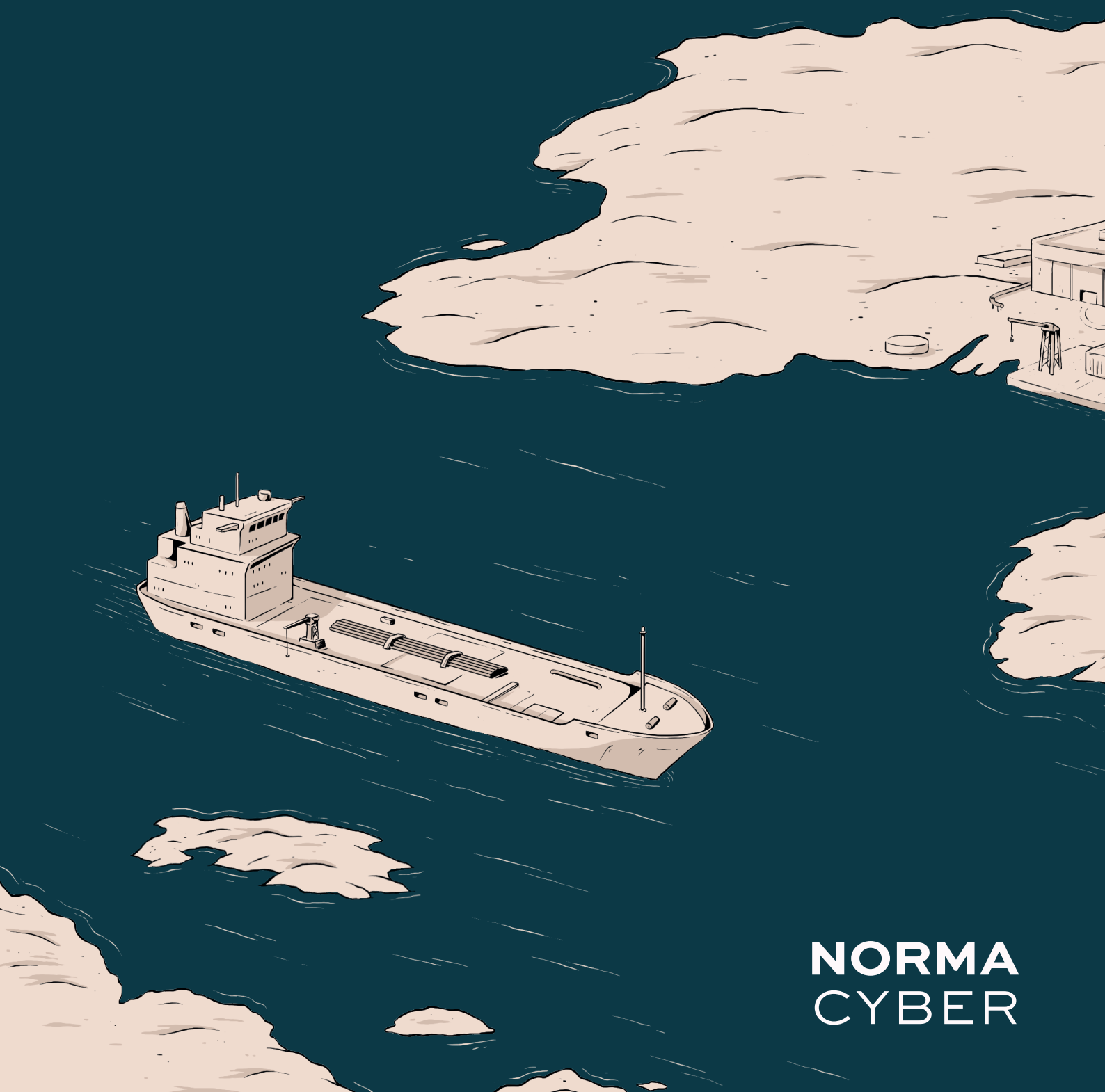
The Nordic Maritime Cyber Resilience Centre

Annual Threat Assessment 2025

normacyber.no



NORMA CYBER

The Nordic Maritime Cyber Resilience Centre, NORMA Cyber, is the leading hub for operational cyber security efforts within the Nordic maritime industry. The centre has been operational since 2021 and was initiated as a joint effort between The Norwegian Shipowners' Mutual War Risks Insurance Association (DNK) and the Norwegian Shipowners' Association. Originally focusing on the Norwegian maritime sector, NORMA Cyber expanded to the Nordics in the Spring of 2024.

NORMA Cyber operates as a non-profit, and the members are organisations within the maritime sector in the Nordics. The centre offers affiliate and vendor memberships to international organisations and maritime vendors.

NORMA Cyber currently has 123 members, representing more than 2 600 vessels and offshore units.

The centre delivers a centralised cyber security function for its members to pool together resources and be more effective and resilient than if the companies were to establish similar resources independently. The centre therefore spends significant time on developing new solutions that take advantage of new technology and ensures efficient and cost-effective cyber security for our members.

The services include threat intelligence, a system for timely information sharing among members, crisis response support and similar functions.

Since 2024 NORMA Cyber has been the operational arm of the sectorial response function for cyber security within the Norwegian maritime sector, led by the Norwegian Coastal Administration.

Our experts work closely with security and emergency preparedness professionals in DNK and the Norwegian Shipowners' Association. In Oslo, our three organisations have established the Norwegian Shipping Security and Resilience Centre. This is a joint centre to support common members with complex operations when both physical and cyber threats are prominent.

ADMINISTRATIVE QUERIES:
contact@normacyber.no
Phone: 22 22 00 50

Emergency number: +47 90 98 97 37

Contents

Dear Reader,
Welcome to this edition of the NORMA Cyber Annual Threat Assessment.

We find ourselves at a time of uncertainty on many levels. Increased competition and tension between major nations together with several regional conflicts is the new normal. Security authorities in the Nordics warn of a likely threat of hybrid attacks and sabotage against Nordic countries. The maritime industry is by nature global and with complex and intertwined supply chains making us vulnerable to these conflicts and threats.

The technological development and digitalisation of the industry continues. The connectivity onboard vessels increase, and we see a growing interest to connect vessels, ports and other parts of the maritime industry with each other and with adjacent industries. Operational Technology (OT) is increasingly connected to IT and the outer world. Great efficiency gains are possible, but the development does not come without increased vulnerabilities and potential negative impact should an attack take place. Through the latest member survey of the Norwegian Shipowners Association, C-levels at Shipowners express that cyber security is the type of security threat they are most concerned with.

At NORMA Cyber we work closely with members, national and international stakeholders to achieve timely information sharing and monitoring of the threat landscape. We have unique access to data through this work and we do our best to maintain the competence to interpret the findings in an objective and methodical way.

This report aims to present the most important findings and trends in the maritime cyber threat landscape together with our predictions for the coming year. We hope this insight can assist decision makers on many levels with their situational awareness in a changing and fast paced world. Digital threats are difficult to mitigate fully, but we work on a day-to-day basis to support members so they can operate effectively and with as little risk as possible.

We hope the assessment inspires further discussions, dialogue, and sharing within member organisations and between stakeholders. We at NORMA Cyber look forward to another year of meaningful interactions to continue building resilience in the maritime sector.

Enjoy the read!

Lars Benjamin Vold
Managing Director

Nordic Maritime Cyber Resilience Centre

Annual Threat Assessment 2025
NORMA Cyber

Managing Director Lars Benjamin Vold
Nordic Maritime Cyber Resilience Centre

Geopolitical Backdrop

As 2025 enters the second quarter the world sees several significant changes. The world order as we know it is challenged, bringing historical political alliances and international structures into question. These changes, as well as geopolitical conflicts, influence the world economy and free trade, and challenges the security of not only states but all other private organisations operating globally.

Geopolitical tensions will highly likely be drivers for cyber operations targeting maritime entities in 2025. President Trump's upheaval of the international political and economic order, the fragile cease fire between Hamas and Israel, and Russia's continued occupation and warfare in Ukraine, will continue to influence security dynamics. So will China's continued posturing on the global scene, and regionally in the South China Sea, whilst they struggle with a declining economy.

All these factors influence cyber security and the threats of espionage, disruption, destruction, and information operations against the maritime sector. Cyber tactics can be used as a means of influence or as a part of hybrid operations. These are operations that use one or several means to apply pressure against its target, while remaining below the threshold of war, and maintaining plausible cover of deniability.

A blurring of the threat landscape causes challenges for organisations when assessing the threat against their operations globally. In most instances, economic loss and reputational damage caused by financially motivated threat actors are most visible. However, in a fast paced and unpredictable geopolitical environment, sudden changes in the threat landscape become more likely. Therefore, it is likely that also the maritime sector can expect changes in frequency, types of organisations that are targeted, as well as more severe consequences.

The maritime sector is influenced by geopolitical tensions through a wide range of factors. Companies are targeted based on traits such as country of origin and location, type of operations, and segment they operate in. Cyber operations could hit all aspects of company operations, making maritime entities vulnerable to supply chain attacks as well as targeting of port and terminal infrastructure.

State-sponsored threat actors have been observed cooperating in the physical domain. In 2024 Russia alone was suspected of carrying out more than 40 sabotage operations in Europe, including both cyber and physical initiatives.

In 2025, it is crucial to maintain a vigilant focus on changes in the geopolitical landscape to prepare for and minimise the consequences of potential future cyberattacks.

Executive Summary

Despite the rapid changes in the geopolitical environment and advancements in technology, the threats cyber operations pose to the maritime industry remain consistent. That said, the capability to increase the attacks against the maritime sector including vessels, ports, and terminals is likely present among various threat actors, particularly state actors like Russia and China. Nevertheless, the intent to increase operations to disrupt and cause significant damage remains low, except for hacktivists, who will likely continue to launch Distributed Denial of Service (DDoS) attacks and pose a moderate threat. The threat of attacks on Operational Technology (OT) is low due to the absence of internet-facing components in many of these targets.

There is a high threat of cyber espionage operations against the maritime sector due to its role in national security and the global economy. States are expected to continue to use cyber espionage to gain advantages or insights into ongoing conflicts in the coming year, affecting organisations within the maritime sector.

While the threat of a directed campaign is low, maritime entities in the Nordics are highly likely to be leveraged as examples in information operations related to geopolitical tensions in 2025. Both state and independent threat actors engage in information operations to shape public perception and further their strategic objectives. Regardless of their actual capabilities, these actors may use claims of cyber-attacks as a tactic to amplify their narratives and impact. Entities operating in, or connected to, regions with geopolitical tensions are especially exposed.

The threat posed by financially motivated actors against the maritime sector is high. However, the impact may vary from compromised user accounts to million-dollar losses. Maritime entities will highly likely continue to be indiscriminately targeted by financially motivated threat actors.

Key figures from 2024

72
confirmed compromised accounts and devices have been reported by NORMA Cyber to maritime organisations.

45
instances of ransomware groups naming maritime entities were recorded by NORMA Cyber.

237
published DDoS attacks were registered by NORMA Cyber in 2024, of which 153 were linked to NoName057.

301
incidents were handled by NORMA Cyber Security Operations Centre (SOC) on behalf of SOC members.

Summary

Financial Crime

The threat from criminal campaigns affecting entities in the Nordics, either directly or indirectly, is high. Financially motivated threat actors will likely remain opportunistic in their targeting. In terms of business impact, ransomware attacks pose the most significant threat, although a successful fraud scheme may be equally expensive. Instead of deploying malware for initial access and actions on the objective, criminals are increasingly likely to use deception and legitimate tooling.

Initial Access
There is a high threat of phishing campaigns towards the maritime sector. Criminals will highly likely apply a human-centric tradecraft, such as phishing, to gain valid credentials and to obtain access to resources. Exploiting vulnerabilities and other methods are also prevalent, although it is reserved for the more technically apt threat actors and not as widespread in sheer volume. Most cybercriminals attempting to gain access through vulnerabilities will likely exploit unpatched historical vulnerabilities, especially those with readily available Proof of Concept guides on the internet.

To gain initial access through phishing, criminals will highly likely use commodity phishing kits with multifactor authentication bypass capabilities to compromise user accounts. These phishes will highly likely emulate services and names the criminals assume people are familiar with and trust, increasing the chance of a successful attack. Dubbed Attacker-in-the-Middle (AiTM) attacks, the phishes often require the victim to log into their O365 to view something sent to them. The attacker will spy on the authentication process and steal the username, password, and the session cookie. The session cookie allows the attacker to log into the resource as the user, without being prompted for authentication. During Q3 and Q4 2024, NORMA Cyber alerted on over 80 user accounts that had been successfully compromised in a AiTM phishing attack. This type of phishing presents a high threat of financial fraud, data theft, and network compromise to onshore and offshore maritime assets.

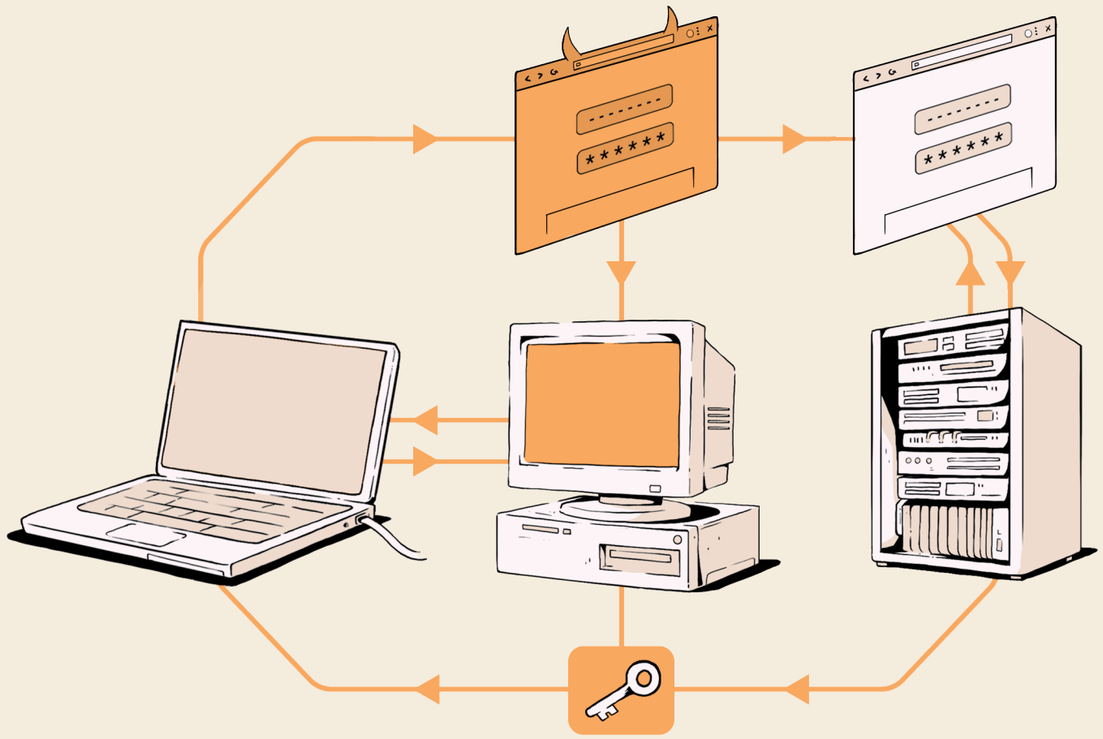
Extortion
Ransomware and data theft is highly likely considered both profitable and thrilling by threat actors, and it is unlikely that the volume of attacks will decrease in 2025. NORMA Cyber recorded 45 instances of threat actors openly claiming maritime victims in 2024. There are likely dark numbers, as not all threat actors use the name-and-shame tactic and victims who pay the ransom demand tend not to be listed.

Although 45 maritime victims are less than the 72 reported in 2023, the opportunistic nature of cybercrime makes it likely that the numbers will fluctuate in between years. Moreover, one did not see mass exploitation of zero-day vulnerabilities at scale in 2024.

International law enforcement made several strikes at the ransomware ecosystem in 2024, and although a handful of the most prolific actors suffered blows to their operations, the criminal ecosystem remains resilient. In the wake of the actions towards LockBit and Alphv, threat actors have either joined other groups or created their own. 2025 started with a diverse ransomware landscape, with numerous medium-sized groups consistently conducting operations. However, Ransomhub in particular is attracting affiliates and will likely be the most prolific ransomware group in 2025 unless disrupted. However, due to the influx of newly created groups, the ransomware threat landscape will likely remain varied in the coming year.

Maritime entities face a significant threat of becoming collateral damage in ransomware attacks striking their supply chains—both physically and digitally. This is especially true if a port or terminal facility suffers a ransomware incident at a scale that leads to closures and the disruption of dependent operations. Beyond operational shutdowns, attacks on suppliers also pose a high threat of sensitive data leaks and the unavailability of critical digital tools.

Bespoke Maritime Campaigns
Fraud campaigns tailored to the maritime sector will likely occur at a low but steady rate in 2025. These campaigns use industry-specific terminology and topics. Criminals familiar with the sector likely perceive it as lucrative. Maritime-themed phishing emails observed by NORMA Cyber in 2024 were centred around vessel and cargo information and port operations, a theme that is likely to continue in 2025. Email will highly likely persist as the favoured delivery method, although threat actors such as Braz Conus may occasionally approach vessels by sending phishing emails over Inmarsat C.

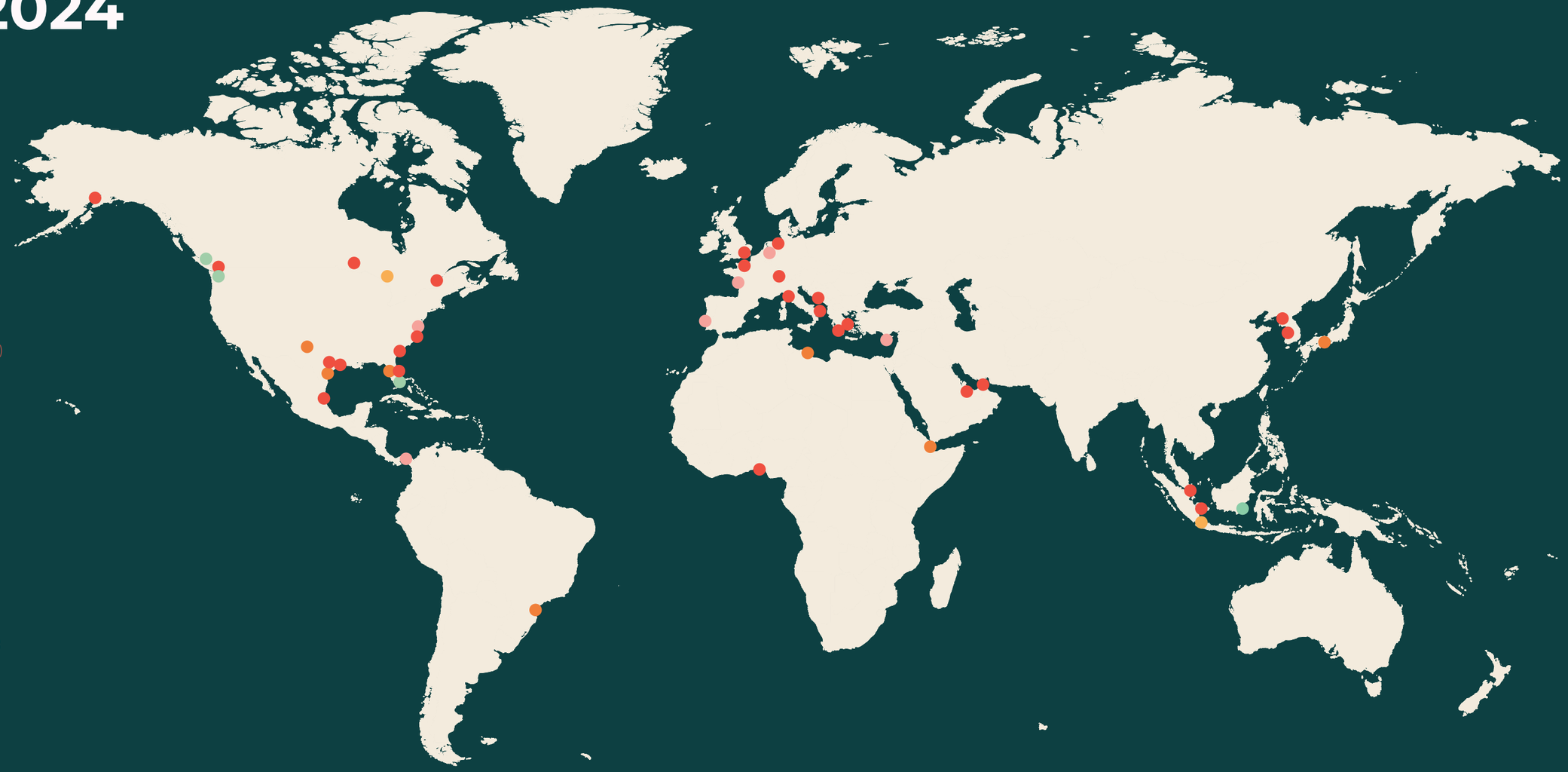


Financially motivated threat actors are highly likely to increasingly adopt generative artificial intelligence (GenAI) for operational enhancements, mirroring the rest of society. Threat actors are highly likely to use GenAI models to become more efficient, as well as to develop code and social engineering materials. The emergence of capable and cheaper models will likely continue to inspire threat actors to create their own specialised versions. These versions will not have the same ethics restrictions as commercial GenAI services. Moreover, GenAI lowers the barriers of entry, likely making e.g. ransomware operations more lucrative for threat actors looking for quick financial gain. Predicting the extent to which these technologies might aid in the development and execution of cyberattacks is challenging, as the usage can be difficult to confirm.

During 2024, threat actors progressively used GenAI to support their efforts. Within social engineering, one notable usage was voice manipulation, where threat actors used AI to replicate voices the victim knows. Threat actors are likely to increasingly incorporate voice phishing (vishing) into their attacks in 2025. Entities with offices in English-speaking countries are particularly exposed to this, due to English being a global language and easier for attackers to emulate in a trustworthy manner. As for using GenAI to enhance operations and create scripts and code, there are several examples of threat actors being aided by GenAI models. This is expressly apparent in code and malware samples that include extensive code comments with good English, which are derivative from the normal mannerisms of threat actors.

Annual Threat Assessment 2025
NORMA Cyber

Ransomware Attacks 2024



Other Strains

8base - Atlantic States Marine Fisheries Commission (USA)
Akira - Heidmar (Greece)
Akira - ShoreMaster (USA)
Alphalocker - Geodis (France)
Alphv - Infraestructura Portuaria Mexicana S.A. (Mexico)
Blackbasta - Cavotec (Switzerland)
Blackbasta - Hanwha (South Korea)
Blackout - Neda Maritime Agency (Greece)
Blacksuit - nestoilgroup.com (Nigeria)
Cactus - Coastal Cargo Group (USA)
Cactus - Rio Marine (USA)
Darkvault - Nejoum Aljazeera (UAE)
Eldorado - Tankerska plovidba (Croatia)
Helldown - Albatros S.r.l. (Italy)
Incransom - Graypen Ltd (UK)
Killsecurity - PT Pertamina (Indonesia)
Lynxblog - Cruz Marine (USA)
Lynxblog - Tricon Energy (USA)
Medusa - Autorità di Sistema Portuale del Mar Tirreno Settentrionale It (Italy)
Play - Livingston International (USA)
Play - Maldives Ports Limited (Canada)
Ragroup - Reederei Jüngerhans (Germany)
Ragroup - SK Gas (Korea)
ransomhouse - Berge Bulk (Singapore)
Snatch - Seven Seas Group (UAE)
Spacebears - Keystone Engineering (USA)

Ransomhub

Djibouti Ports and Free Zones Authority (Djibouti)
Halliburton (USA)
Mellitah Oil & Gas / Enigas Ly (Libya)
Naniwa Pump Mfg. Co., Ltd. (Japan)
Overseas Shipholding Group (USA)
port administration for São Francisco do Sul (Brasil)
West Gulf Maritime Association (USA)

LockBit 3.0

Eastern Shipbuilding Group Inc. (Panama)
Groupo Idea (France)
Lyon Shipyard (USA)
Northsea Yacht Support (Netherland)
Portline (Portugal)
Semesco (Cyprus)

Hunters

Carigali Hess Operating Company (Malaysia)
Indika Energy (Indonesia)
SeaLandAire Technologies (USA)

Rhysida

Delmar International (Canada)
MarineMax (USA)
Port of Seattle (USA)

Espionage

The maritime sector is subject to a high threat of cyber espionage operations because of its central role in both national security and the global economy. Shipping lanes, seaports, and energy supply chains are the arteries of international trade and logistics. Cyber espionage is used to access crucial information that helps improve military readiness, secure advanced technologies with dual-use, and strengthen economic or political insight. Espionage is traditionally applied by states. Russia and China are the most prominent actors in the maritime sector.

Threat actors will likely use a broad spectrum of operations to infiltrate maritime systems, ranging from physical access to conducting digital attacks. These operations blend traditional espionage with advanced cyber operations, empowering threat actors to access and exfiltrate sensitive information from maritime organisations.

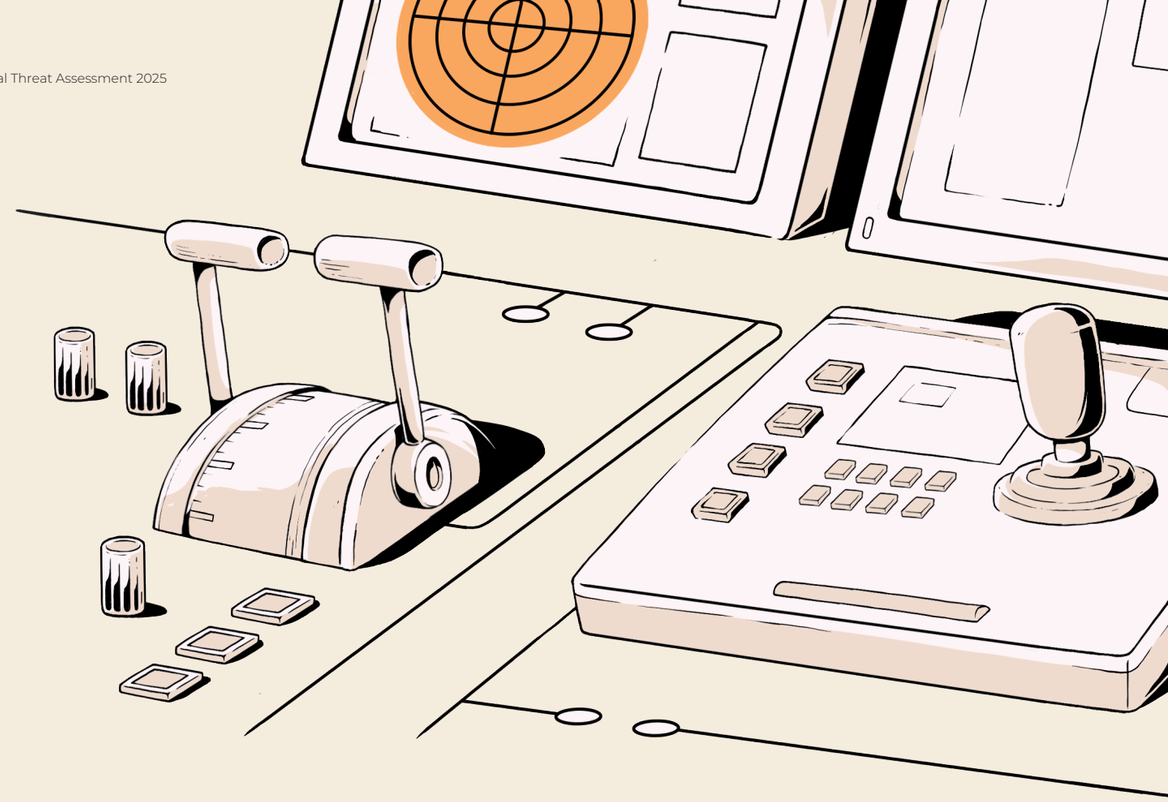
Russia relies on civilian vessels, such as commercial fishing boats, research ships, and cargo carriers, as covers for intelligence collection. Operating in strategic maritime regions like the Baltic Sea, North Atlantic, and Arctic waters, these vessels can discreetly monitor naval movements, undersea infrastructure, and military logistics.

In parallel with these hybrid methods, threat actors rely on technical cyber espionage techniques that exploit everyday vulnerabilities. External devices, such as USB devices, have been observed used as initial attack vector when targeting maritime organisations. Originally used for data storage and transfer, these devices have been weaponised to deliver hidden malware payloads. Multiple incidents linked to a threat actor named Mustang Panda have demonstrated that weaponised USB devices can effectively infiltrate maritime systems by tricking users into executing malicious code.

To further enhance the stealth and persistence of their operations, threat actors use Operational Relay Box (ORB) networks. These networks consist of a mesh of compromised devices, often routers and IoT systems. The devices relay traffic and obscures the command-and-control channels. By exploiting vulnerabilities in these systems, threat actors create covert communication pathways that blend with legitimate network traffic. This strategy not only evades detection but also complicates attribution, as the diversity of intermediary nodes masks the true origin of the attack. The decentralised design of ORB networks also ensures operational resilience, allowing continued access even when nodes are identified and remediated.

Another threat actor known for espionage, the Russia-linked Fancy Bear, has employed a wide range of tactics to infiltrate and persist within targeted networks, leveraging password spraying, phishing emails, and exploitation of internet-facing edge devices and servers.

The combination of covert physical intelligence gathering via civilian vessels and cyber espionage operations underscores the high espionage threat for the maritime sector, a persistent threat expected to consist in the following year. By integrating hybrid approaches with cyber operations, adversaries can bypass conventional defences and maintain prolonged access to critical maritime information.

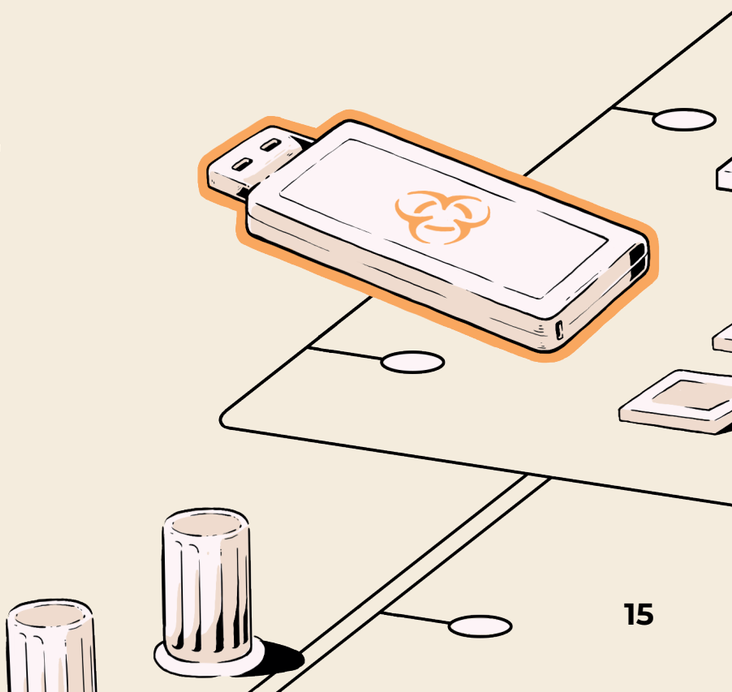


Pursuit of Advanced Maritime Technology

Threat actors continue to leverage cyber espionage to secure advanced maritime technology and dual-use systems that enhance both military and economic power. China-linked threat actors have persistently targeted maritime engineering, open-source platforms, and proprietary research related to undersea technology and autonomous underwater vehicles. Their goal is likely to bolster global influence and strengthen strategic capabilities in areas crucial for undersea exploration, navigation, and communication. Over recent years, incidents have demonstrated the use of sophisticated techniques, to gain long-term access to this valuable information, or likely prepare for sabotage operation.

At the same time, Russia has shown a strong interest in acquiring dual-use technologies that can enhance its military capabilities. Restricted by Western sanctions and export limitations on advanced weaponry, Russian efforts via cyber espionage have focused on maritime communication systems, navigation technology, robotics, and maritime autonomy. By targeting these systems, Russian actors aim to circumvent conventional supply channels and secure technology that serves both civilian and defence needs.

Organisations involved in the development of advanced maritime technology face a high threat of cyber espionage from state actors. By acquiring advanced maritime technologies with dual-use capabilities, these state-linked entities aim to influence the balance of maritime power, compromise the confidentiality of strategic research, and affect regional stability.



Threat Actors

Selection of threat actors attributed by trusted intelligence sources.

Fancy Bear

Fancy Bear is a Russia-linked threat actor, with activity observed as recently as January 2025. The group conducts intelligence collection and information operations to support Russian geopolitical objectives. Fancy Bear employs techniques, such as spear-phishing with malicious documents, exploitation of public-facing applications and devices, and brute-force attacks and password spraying. Fancy Bear uses multi-stage delivery chains and exploits zero-day and known vulnerabilities to gain and maintain access while evading detection. Its primary targets are high-value entities, including government, military, and strategic organisations, primarily across Europe, but also extending beyond to other regions, aligning with Russia's broader geopolitical and strategic interests.

Mustang Panda

Mustang Panda is a China-linked threat actor with operations dating back to 2012. The group focuses on espionage and intelligence gathering to support China's political, economic, and military objectives. Mustang Panda uses spear-phishing campaigns, USB-based infection vectors, and exploits internet facing devices for initial access. It often uses DLL sideloading techniques to install malware and persist within networks. The group has targeted a wide range of entities, including maritime organisations, energy infrastructures, and political think tanks. Mustang Panda's operations are focused on regions vital to China's strategic interests, especially those related to its economic and military power.

Razor Tiger

Razor Tiger is an India-linked threat actor. The group conducts targeted intrusion operations to support Indian intelligence priorities, focusing mainly on government and military sectors. It demonstrates advanced operational security, employing techniques like geofencing and infrastructure obfuscation to evade detection and restrict malware execution. Razor Tiger uses custom remote access capabilities, like its multi-stage installation chain to improve persistence and bypass defences. The group targets sectors such as government, military, maritime, and defence, traditionally focusing on countries near abroad, but recently expanding to the Middle East and Southeast Asia.

Strategic Value of Maritime Intelligence
Information from maritime organisations has emerged as a target in today's geopolitical landscape. Sea ports play a role in military logistics, energy security, and commercial trade. As these assets are vital in the event of a crisis or war, they draw attention from nation-state actors who not only target them physically but also seek to extract critical information through cyber operations.

Since Sweden and Finland joined NATO, Russia has increased its strategic focus toward the Baltic Sea and Nordic regions. Sea ports in these areas are far more than just hubs of commerce. They serve as essential gateways for NATO reinforcements, enabling rapid military deployments to the Baltic and Arctic theatres. Moreover, these ports underpin European energy security, supporting the Nordics gas exports and LNG terminals, making them indispensable for fuelling the continent's energy demands. With such significance, these maritime hubs, along with the numerous Vessels that call at these ports, have become attractive targets for intelligence Gathering. Russian efforts in this arena are designed to exploit these strategic chokepoints. Cyber operations are tailored to underpin these goals and makes maritime entities operating in the energy sector vulnerable.

Nation-state threat actors, particularly those linked to Russia, China and India, are using cyber espionage to gain strategic insights into maritime operations.

These cyber operations aim to penetrate systems that manage or monitor maritime infrastructure, thereby providing intelligence on key elements such as logistics, defence strategies, and energy supply chains.

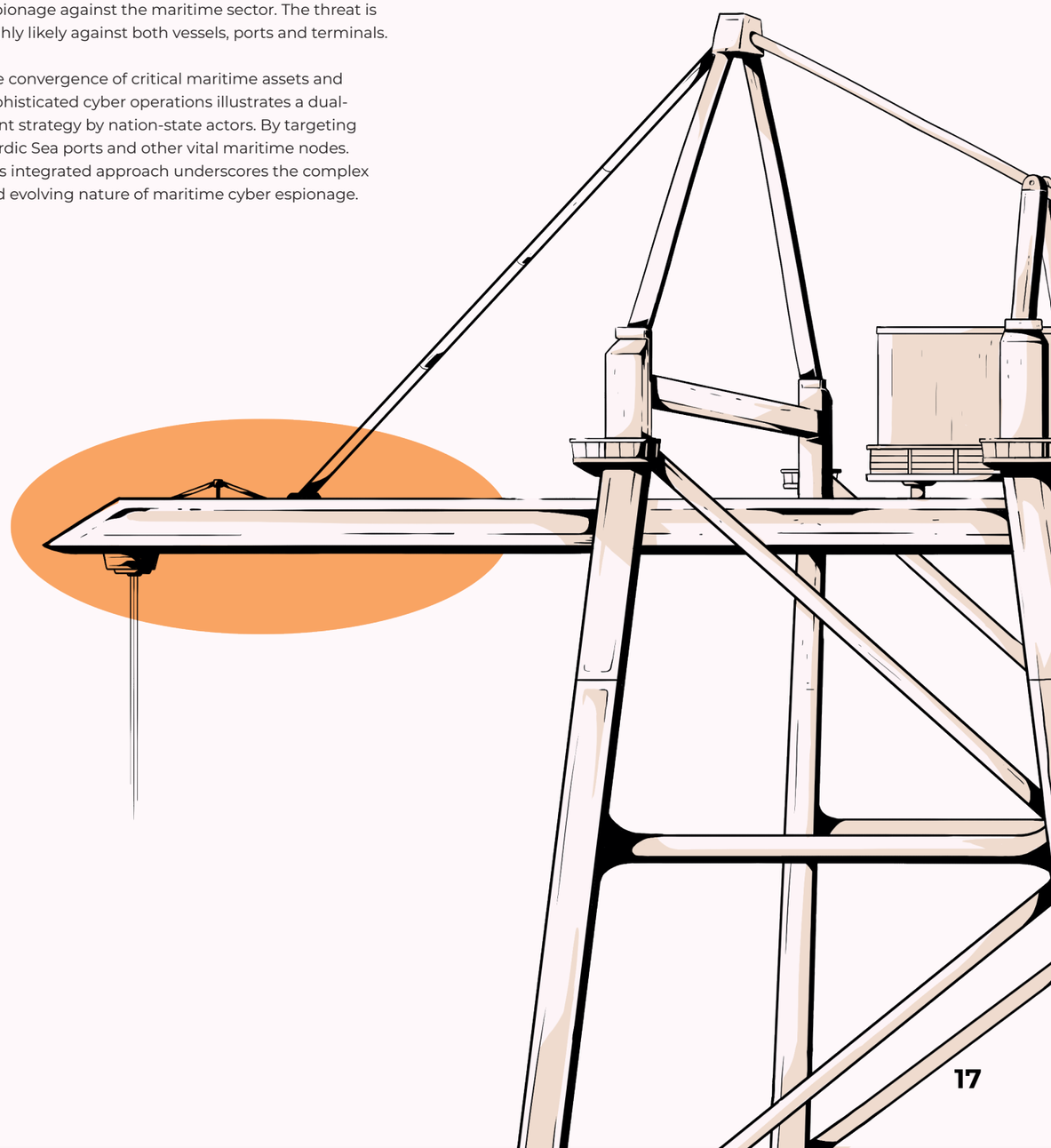
The Russia-linked threat actor Fancy Bear has increased its targeting of the transportation sector last year, focusing on civilian aviation, rail, and maritime logistics. The group has targeted air traffic control systems, logistics providers, and maritime organisations in at least 11 countries, aiming to monitor humanitarian and military logistics flows to Ukraine. These efforts will likely continue as part of a broader strategy to gather intelligence on NATO-aligned transportation networks and pre-position access for potential future cyber operations in case of escalation between Russia and NATO.

China-linked groups have employed maritime-themed phishing campaigns with malware to infiltrate networks involved in disputes in the South China Sea. They also target countries near abroad like Taiwan. They focus on government bodies, defence technology firms, and telecom companies that manage submarine cables, likely to gather both commercial and military intelligence. Similarly, India-linked threat actors have used spear-phishing to compromise systems at port facilities and defence networks in regions where their geopolitical interests are at stake, such as the Mediterranean Sea and the Indian Ocean.

These cyber operations provide threat actors with valuable intelligence on how different stakeholders respond to regional security challenges. By compromising sensitive data related to infrastructure, logistics, and defence strategies, these campaigns offer a comprehensive view of maritime operations, which can be leveraged to influence broader strategic and economic outcomes. It is likely that state actors use supply chain as an attack vector to access information and conduct espionage against the maritime sector. The threat is highly likely against both vessels, ports and terminals.

The convergence of critical maritime assets and sophisticated cyber operations illustrates a dual-front strategy by nation-state actors. By targeting Nordic Sea ports and other vital maritime nodes. This integrated approach underscores the complex and evolving nature of maritime cyber espionage.

The maritime sector is subject to a high threat of cyber espionage operations because of its central role in national security and the global economy. It is highly likely that nation-state threat actor will continue to use cyber espionage as a method to gain an advantage or insight into ongoing conflicts in the coming year, which includes organisations in the maritime sector.



Information Operations

The threat from influence operations directly targeting the Nordic maritime sector is low. However, maritime entities in the Nordics will highly likely be used as pawns in information operations as part of geopolitical tensions in 2025. Both states and independent threat actors conduct information operations to shape public perception and advance strategic objectives. Regardless of actual capabilities, threat actors likely use claims of attacks as a tactic to amplify their narrative and impact. Entities that operate in, or have ties to, states or areas with geopolitical tensions face the highest threat.

Hacktivist groups will likely produce the most overt campaigns, where messaging and political statements will be used to advertise their activity and influence audiences. The threat actors who target maritime organisations will likely combine influence operations with disruptive tactics such as Distributed Denial-of-Service attacks.

States seeking to influence will likely operate across the spectrum from using direct political statements to media outlets, social media, fake personas, and groups. In addition to this, entities who sincerely believe in a set narrative will highly likely function as significant amplifiers.

Maritime entities are more likely to encounter threat actors operating as state proxies and true believers seeking to rebel against opposing views. Regional conflicts will likely be the primary drivers for their actions. These threat actors are likely to combine influence attempts with disruptive attacks. The threat from influence operations directly targeting the Nordic maritime sector is low.

The Spectrum of State Responsibility*

State-aligned

Third parties control and conduct the attack, but the national government encourages them as a matter of policy

State-executed

The national government conducts the attack using cyber forces under their direct control

State-integrated

The national government attacks using integrated third-party proxies and government cyber forces

*The Spectrum of State Responsibility is borrowed from the Atlantic Council

Disruptive Cyber Attacks

Maritime organisations operating in, or with ties to, states or regions affected by geopolitical tensions face a moderate threat from threat actors exerting pressure through cyber disruption. Disruptive attacks are a strategic tool to achieve various objectives, including political, economic, and operational gains. Regional conflicts will likely prompt reactions from threat actors who conduct disruptive attacks as part of their operations. Distributed Denial-of-Service attacks are most frequent but tampering with control systems and deploying ransomware are also common.

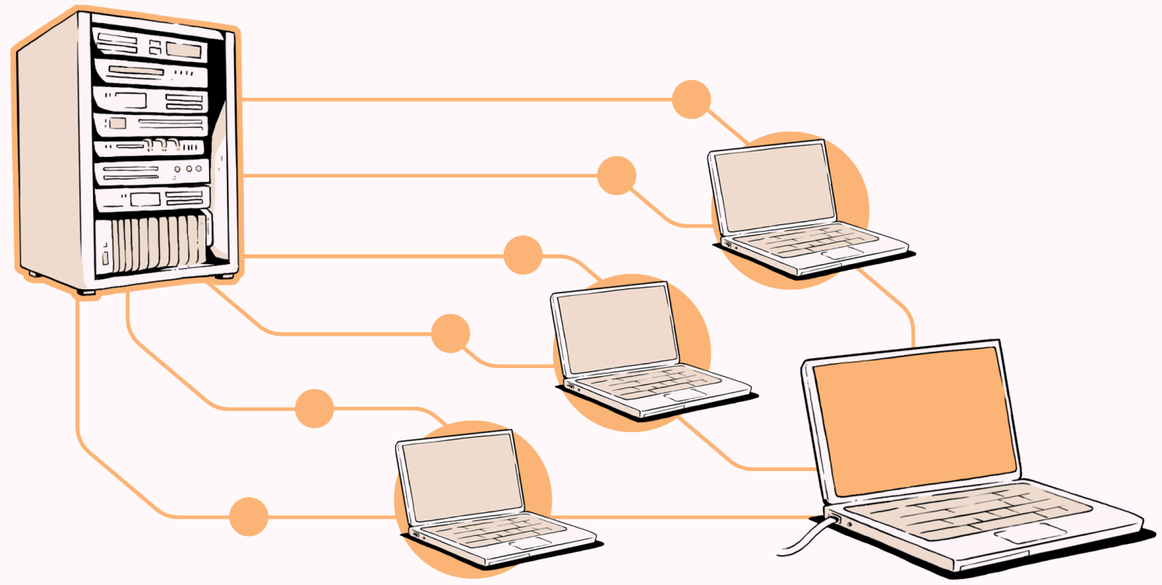
Disruptive attacks will highly likely cause economic loss if aimed at services and devices used in operations. This is true regardless of the motivation of the attacker. The financial impact is due to operational downtime, delays, and incident response. As an example, a prolonged Distributed Denial-of-Service (DDoS) attack towards booking systems likely leads to the loss of customers while also requiring extra staffing during and following the attack.

While most hacktivist collectives are likely composed of individuals motivated by political or religious causes, evidence points to the involvement of state actors in some prominent groups. By leveraging hacktivist proxies, states gain plausible deniability and avoid direct accountability, allowing them to act covertly while maintaining adherence to international agreements. This strategy enables states to exploit hacktivists as tools for advancing their objectives without violating diplomatic norms.

Iran will highly likely support threat actors conducting operations that align with their interests, in addition to using directly tasked fake online personas and front companies to mask their direct involvement in cyber operations. Iran-linked threat actors are likely to use disruptive attacks to spread distrust in their target's systems, components, and processes. The targeting will likely focus on Israeli entities and those with an affiliation to Israel.

Notably, in January 2024, Iran-linked cyber operations were actively coordinated with kinetic military activity for the first time. A hacktivist persona likely operated by an Iranian military contractor claimed responsibility for a DDoS attack against tankertrackers.com, an oil tanker tracking website. This attack was reportedly timed to coincide with Houthi missile strikes on a US-owned tanker in the Red Sea. This incident highlighted Iran's willingness to integrate cyber operations with proxy military engagements. It demonstrated a capability to coordinate operations, not only within its own cyber and military assets but also in close collaboration with aligned groups in the region.

Russia is likely using disruptive attacks as a force multiplier alongside kinetic attacks. However, the frequency and extent of these attacks have decreased since the first year of the Russia-Ukraine war. Limited insight into the full scale of Russian state-ordered attacks complicates assessing the effectiveness of their campaigns. The number of Russian state-ordered disruptive cyber-attacks towards maritime entities and infrastructure will likely remain low unless there is a significant geopolitical trigger. However, pro-Russian hacktivists will highly likely continue to target European maritime entities in 2025. Entities involved in port operations and passenger transportation face the highest threat. This assessment is based on observed targeting patterns and that the hacktivists likely favour entities many rely on.

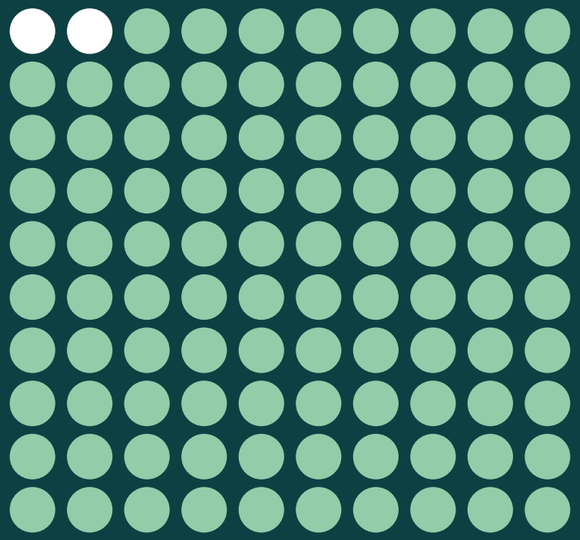


Hacktivist groups will likely target maritime entities with connections to states embroiled in geopolitical tensions and NATO member countries that provide military support to Ukraine. The intention is likely to retaliate against opposing political views and influence public morale. DDoS attacks will likely continue to be the most prominent attack method, but some smaller groups will likely attempt attacks on internet-exposed OT components.

Hacktivists are likely to employ basic attack methods requiring minimal technical expertise. DDoS attacks dominate their techniques, overwhelming services with excessive traffic and creating operational disruptions without breaching victim systems. However, as groups evolve and mature, a few will likely try incorporating techniques associated with criminal threat actors for operational efficiency and financial gain

NORMA Cyber is familiar with 239 publicised disruptive attacks against the maritime sector in 2024. All but two were DDoS attacks towards internet-facing services carried out by hacktivist groups. The two remaining attacks were website defacements, where the threat actors exploit weak and misconfigured websites to show a message or design of their choosing. The pro-Russian group NoName057(16) was behind 153 of the recorded attacks, but the true number of attacks is highly likely significantly higher.

95.95%
DDos



247 total reported attacks

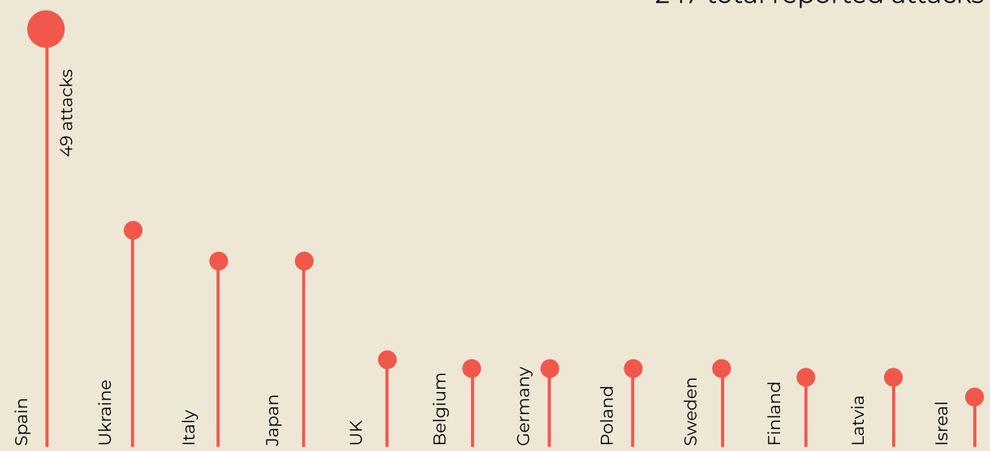
2024 also saw the emergence of more hacktivists focusing on OT being amplified by the larger hacktivist channels and forming alliances. This trend will likely continue in 2025. Hacktivists claiming OT breaches are not a novelty, and particularly groups active in the Middle East region have consistently turned to claims of such breaches in retaliation to conflict developments. However, as the hacktivist space matures, the allure of attempting more flashy hacks likely grow. Tampering with OT is likely to yield some peer recognition within the hacktivist community. Hacktivists will highly likely focus on improperly secured internet-facing devices, as these are likely the only OT assets they are capable of exploiting.

Hacktivists will highly likely use GenAI tools extensively to enhance their capabilities in 2025. This is especially true for hacktivists seeking to shift to the crime segment, as criminal endeavours require the threat actors to be more technically apt to have success. Typical use cases are likely to be the development of malware and guidance on how to perform operations to increase their success rate.

However, these groups' general lack of technical expertise will likely prevent them from accessing victim environments and deploying malware effectively.

The general threat of DDoS attacks against the Nordic maritime sector in 2025 is moderate. Entities involved in port operations and passenger transportation face the highest threat, as hacktivists historically aim at striking services that they perceive many uses. Disruptive OT attacks are unlikely, as they would typically require a component to be openly exposed on the internet before an attacker could attempt to tamper with it.

The 12 most attacked countries out of 247 total reported attacks



Destructive Cyber Operations

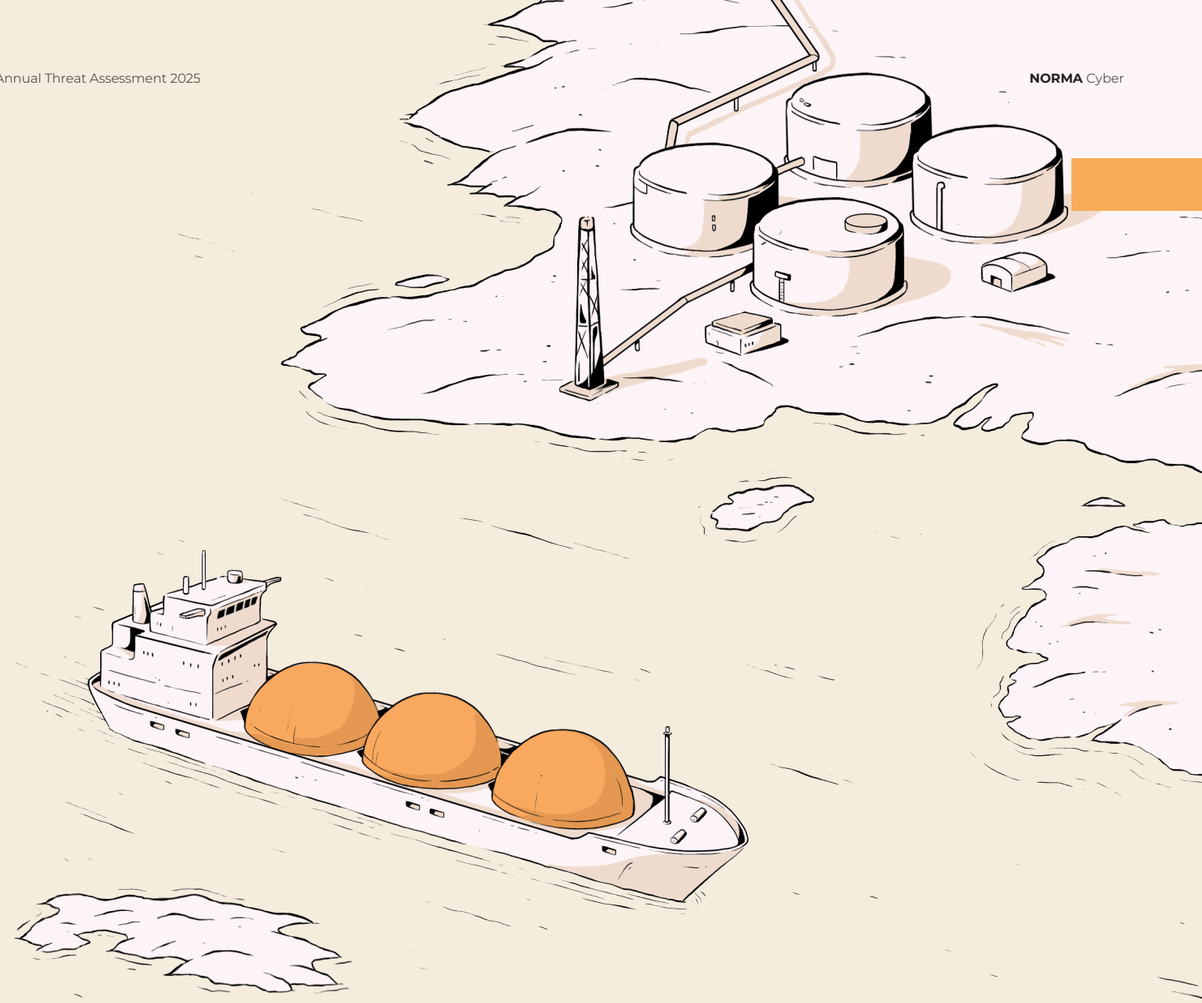
The threat against maritime entities from destructive cyber operations is low. That is, deliberate cyberattacks intended to destroy digital or physical systems. The motivation behind such attacks is often multifaceted. While any system can be targeted, destructive attacks on OT are likely to have the most significant impact on maritime entities. Key actors in potential cyberattacks on maritime systems are anticipated to be Russia, Iran, and various hacktivist groups.

Over the past year, attacks on OT components have risen across critical infrastructure sectors, suggesting that threat actors have the capability to launch similar attacks within the maritime industry. However, the opportunity for conducting destructive cyberattacks on maritime equipment is likely limited, as most attacks require the equipment to be accessible via the Internet.

Russia likely has various intentions when conducting sabotage. Motivations include undermining the Western support for Ukraine, exerting pressure on the West, weakening opposing nations, and demonstrating a willingness to use riskier tactics. All destructive activities are aimed at achieving Russia's broader geopolitical goals, while avoiding a direct military confrontation with NATO.

Moreover, Russia appears to be increasingly utilising proxy actors to carry out acts of sabotage. These proxies are often recruited through social media channels, making it difficult to trace their activities back to the Russian state. The observed methods of sabotage include both physical acts, like arson and vandalism, as well as cyber-attacks targeting critical systems and networks, although such incidents have yet to be reported against maritime targets. In the past 15 months, more than eleven incidents of damage to undersea cables have been recorded, raising concerns about potential deliberate sabotage. While some incidents have been attributed to accidents—such as ships dragging anchors—the frequency and timing of these events have led to suspicions of coordinated sabotage. Investigations into these incidents are ongoing.

While the current threat of destructive cyber operations against the maritime sector from Russia is low, the threat levels could change rapidly if the Russian regime feels threatened or seeks leverage against European nations. In such a scenario, cyber operations are likely to be launched as part of a hybrid attack, with entities affiliated with energy infrastructure, undersea infrastructure, and critical digital infrastructure likely being the preferred targets.



Voodoo Bear

Voodoo Bear is a Russia-linked threat actor attributed, by many researchers, to the GRU. The group conducts targeted intrusions aiming to undermine public trust in state institutions and critical industries in key target regions.

Voodoo Bear employs a blend of customised commodity malware and bespoke destructive tools, known for multi-stage payload delivery and innovative initial infection techniques that often incorporate deceptive indicators, such as disguising malware as ransomware, to misdirect attribution efforts.

Their operations include destructive campaigns, such as data wiping using tools that mimic legitimate utilities, and credential-collection activities targeting military, defence, and strategic sectors.

The group focuses on a broad range of high-value sectors, including military, utilities, financial services, aerospace, energy, transportation, government, media, and telecommunications. Voodoo Bear highly likely have the capability to conduct destructive campaigns targeting maritime entities if needed.

Given the extensive deployment of cameras in global ports, shipping yards, and offshore platforms, the exploitation of these weaknesses pose a high threat to maritime entities.

Threats to Operational Technology

Operational technology is key to maritime operations, both onboard vessels and at ports and terminals. The threat against these systems is multifaceted, but the common denominator is that systems exploited by threat actors are usually internet-facing. Threat actors will likely attempt to take advantage of vulnerabilities and target internet-exposed OT systems. While this may lead to the destruction of the isolated systems and financial damage for the companies, it remains highly unlikely that maritime OT systems will be targeted in a way that will lead to significant physical damage.

It is unlikely that the threat actors dabbling with OT attacks are capable of conducting efficient and large-scale cyber-attacks against maritime entities. Most threat actors openly proclaiming an intent to target OT and similar systems fall within the hacktivist category. These individuals, although some state proxies, likely have limited technical skills. In cases where they have had success, they have exploited poorly secured internet-exposed devices and still have had limited impact on physical processes.

They often present themselves as hacktivists, claiming political or religious motives for their attacks. Notable examples include the 2024 Unitronics Vision attack and the attack on water and wastewater treatment facilities in the United States. Both incidents are strongly believed to have been carried out by a group known as CyberAv3ngers, which is likely linked to the Islamic Revolutionary Guard Corps (IRGC). The targets of these attacks, Israel and US-affiliated entities, highlight their connection to geopolitical tensions. The attackers' intention seems to be to damage the reputation and critical infrastructure of their adversaries. Although these attacks had minimal consequences, they generated some fuzz in the OT security environment. They illustrate the potential impact of cyber operations in OT if technically skilled threat actors were to execute them.

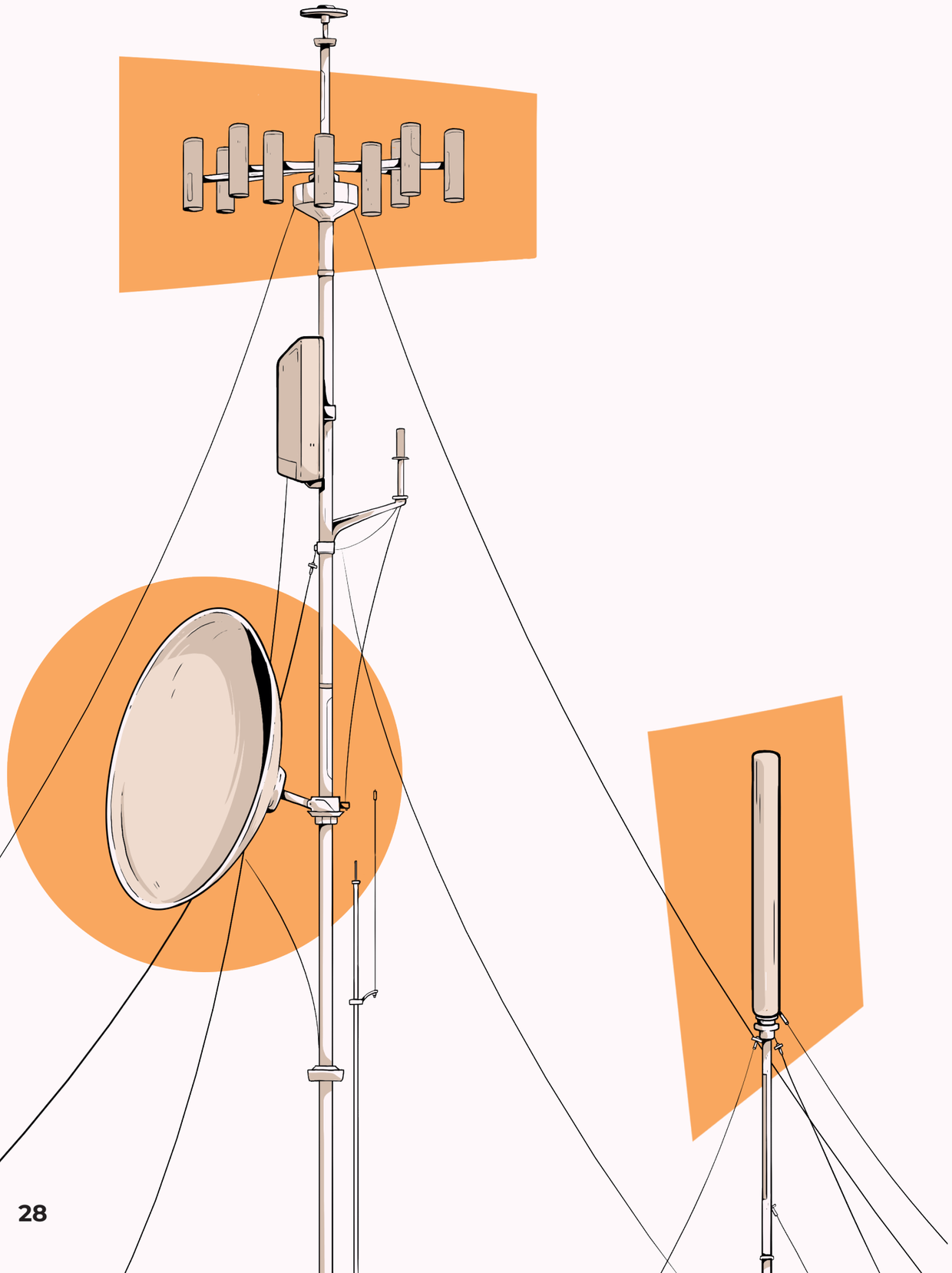
However, among the currently active hacktivists, it seems unlikely that any possess the technical capabilities necessary to successfully destruct OT systems.

Another example is the attacks against Hikvision CCTV. The attack shows how to take advantage of vulnerabilities in the systems to conduct espionage, but also as an attack vector to access more critical systems and infrastructure.

Operations against maritime entities in all examples seen thus far have relied on access through an internet-facing system.

Another area of concern is that vessels become increasingly digitalised, and the potential attack surface increases. NORMA Cyber has over the last year identified vulnerabilities specific to the maritime sector. Vessels are equipped with technology solutions from various vendors that lack a strong security architecture. Examples of such systems include load and stability calculators, systems for emission reporting, and generic systems for data transfer to the cloud. Weak security architectures in these systems expose shipowners to unnecessary vulnerabilities, primarily from an operations and compliance perspective, but may also in some cases create a potential attack vector to essential OT systems.

The threat level of destructive operations against OT in maritime entities is low. Attacks targeting remote access solutions, vulnerable firewalls and weak architectures are likely. In some cases, this may provide attackers with access to OT networks, however, it is unlikely that attackers have the technical expertise nor the intent to use this access efficiently. Due to the complexity of performing destructive attacks, we consider an attack targeting maritime operational technology with physical consequences highly unlikely.



GNSS Interference

Global Navigation Satellite System (GNSS) interference has emerged as a growing security concern for maritime operations. State-sponsored actors are increasingly leveraging jamming and spoofing techniques to disrupt navigation and logistics. In 2025 the threat will be high in strategic regions such as the Baltic Sea, the Black Sea, and the High North and in the Middle East. Russia remains the primary state actor responsible for GNSS interference, utilising this capability to disrupt military operations, civilian shipping, and energy infrastructure.

Russia has deployed GPS jamming extensively as a defensive measure to protect critical installations, including military bases, air defence systems, and strategic infrastructure. Russian military units have likely used electronic warfare (EW) capabilities to create GPS-denied environments around key operational bases, particularly near Kaliningrad, the Kola Peninsula, and Crimea.

GPS jamming serves multiple functions: it prevents precision-guided munitions from reaching high-value targets, disrupts adversary reconnaissance efforts, and complicates the navigation of enemy aircraft and drones.

Such jamming will also unintentionally affect civilian aviation, but also maritime navigation. As long as the Ukraine – Russia war continues, it is likely that GPS jamming will represent a threat to maritime navigation, particularly in areas in the High North, the Baltic Sea, and the Black Sea.

Russia has used GPS jamming not only as a defensive measure but also as a strategic signalling tool in geopolitical conflicts. By selectively disrupting satellite navigation systems in contested regions, Russia can demonstrate electronic warfare capabilities, deter adversaries, and exert influence without direct military confrontation.

Instances of GPS jamming coinciding with NATO military exercises in the Baltic and Arctic regions highlight how these operations are often intended to send a message to Western allies.

Multiple cases of AIS spoofing have been reported in 2024; in the Red Sea, in the Arabian Gulf / Persian Gulf, the Black Sea and the eastern Mediterranean. In most of these cases the spoofing has been done by military units, but GPS or AIS spoofing capabilities has also been adopted by civilian vessel engaged in sanctioned or illicit activities, often linked to the Russian shadow fleet or Iranian oil smuggling operations. By manipulating AIS data, these vessels can obscure their true locations and evade vessel tracking services.

GNSS interference will likely continue to be a major threat to maritime operations in 2025. Russia remains the dominant actor, but also Iran and China have electronic warfare capabilities that can deliberately or unintentionally affect maritime navigation.

The threat from GNSS interference will likely remain high in the High North, the eastern part of the Baltic Sea (particularly outside Kaliningrad and in the Gulf of Finland), eastern part of the Black Sea (particularly outside Crimea and Sótsji), eastern part of the Mediterranean, the Red Sea and the Arabian Gulf / Persian Gulf.

Annual Threat Assessment 2025
NORMA Cyber

GNSS interference 2025

Areas with a moderate and high threat of GNSS interference in 2025. Most of the reported incidents in 2024 occurred in the same areas.

Annual Threat Assessment 2025
NORMA Cyber

About us

Together Stronger

The Nordic Maritime Cyber Resilience Centre (NORMA Cyber) delivers a centralised cyber security function for its members to pool together resources and be more effective and resilient than if the companies were to establish similar resources independently.

Our overall goal is to find synergies and cost-effective solutions, so our members are as secure and resilient as possible.

Membership Services

Members get access to centralised functions and services such as timely information sharing, threat intelligence reporting, incident and crisis response and external monitoring.

The center also hosts events where members and partners can come together to share best practices and find common solutions.

Threat Intelligence

- Monthly Threat Assessment and other Intelligence reports
- Maritime OT - Vulnerability notifications
- Indicators of compromise information sharing (through MISP)
- Mitigation advice
- Member log-in portal for easy access

Incident and Crisis Response

- 24/7, 365 stand-by for incidents and crisis affecting member's vessel IT, vessel OT and land-based or cloud infrastructure
- Technical support and mitigation advice
- Resource management
- Coordination between members, authorities and other relevant stakeholders
- Participation in cyber response exercises (and exercise scenarios available in member portal)

Network

- Be part of our network of members and partners.
- Competence and knowledge sharing through conferences, webinars and workshops.
- Access to the NORMA Cyber member council, an arena to share knowledge and information, as well as innovation and lessons learned. The member council is part of the organisations governance structures.

External Monitoring

- Deep/Dark web monitoring
- Vulnerability scan of internet exposed services
- Alerting to individual members where exposure is detected

Managed Security Operations Center

Flexible and cost-effective solutions for monitoring of Vessel IT, Vessel OT, land-based infrastructure, or cloud infrastructure. Automated response can be provided.

Additional service

OT Security Assessments & Penetration Testing

Security assessments are conducted through documentation reviews, physical inspections, and packet capture analyses of OT systems. This process provides a thorough understanding of vessel asset inventory and topology, vulnerabilities, and weaknesses. The findings are then evaluated from a consequence perspective, concluding with recommendations for mitigative actions.

Penetration testing may also be performed by simulating cyberattacks on IT and OT systems. This approach helps identify vulnerabilities and assess the effectiveness of existing security measures

Additional service

Security Operations Centre

What we do

NORMA Cyber provides a managed Security Operations Centre (SOC) as an additional service for our members. The SOC can monitor member systems on a 24/7 basis and conduct analysis, respond to, and notify members when cybersecurity related incidents are detected.

Our SOC philosophy

Technology and vendor agnostic: we can integrate towards most maritime or corporate systems. There is normally no hardware installation needed or particular type of firewall, EDR or switches.

Neutral party: we have a neutral view on the infrastructure and the SOC team also provides monthly advice on how to increase security posture.

Competence: we understand the maritime domain with all its complexities.

Synergies: the knowledge we get from monitoring several maritime companies gives us an unique insight and anonymized content is shared back to our members.

Technical set-up

- Flexible set-up and the scope vary between IT on vessels to OT on vessels, to corporate IT or Cloud systems.
- Leveraging the most modern SOC systems utilising AI to minimise false positives.
- Automation of as much as possible reducing latency in reporting.
- Manual response and follow up of the complex cases.
- Automated response for IT/cloud systems through our SOAR systems can be provided.
- Threat hunting conducted to detect hidden and advanced threats.

Key Features Across All SOC Services:

- ✓ 24/7 Monitoring & Alerting
- ✓ Incident Response
- ✓ Threat Hunting
- ✓ Monthly Reports with Mitigation Advice
- ✓ Automated Response (SOAR) for IT-related services

NORMA Cyber Managed SOC Services

Enterprise SOC Services (IT & Cloud)

Designed for organisation with larger fleets or those requiring a unified security view across land-based and vessel IT infrastructure.

Feature	Details
Scope	Vessel IT, land-based IT, Cloud services
Prerequisites	None, parsers available for multiple log types
Remote Implementation	Yes
Detection Capabilities	Rule-based, MISP integration, AI-driven baselining & detection

Vessel SOC Services

Tailored for maritime environments with limited/variable bandwidth and specific security needs.

Vessel Tier 1: Strictly Firewall Logs

Feature	Details
Scope	Vessel IT (Firewall logs)
Prerequisites	None, all firewall vendors supported (requires FW to export syslog)
Remote Implementation	Yes
Detection Capabilities	Rule-based, MISP integration

Vessel Tier 2: Multiple Log Types

Feature	Details
Scope	Firewall logs, EDR logs, O365, email, and other log types
Prerequisites	None, all firewall and EDR vendors supported (EDR vendor must export data)
Remote Implementation	Yes
Detection Capabilities	Rule-based, MISP integration, AI-driven baselining & detection

Annual Threat Assessment 2025

SOC Services for vessel OT

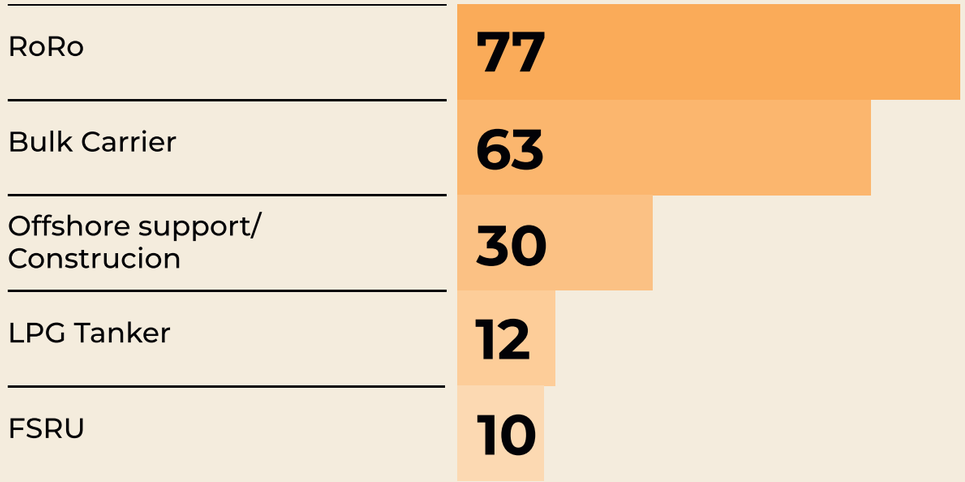
Our SOC team now monitors several vessels' OT networks.
Through solutions we are able to identify assets and create detailed assets lists and identify vulnerabilities and continually evaluate risks. The services include detection of anomalies and threats and will also act on alerts and perform forensic analysis of events.

Vessel Tier 3: OT-Network Monitoring

Feature	Details
Scope	Vessel OT
Prerequisites	None, can work independently or with Tier 1/2
Remote Implementation	Yes
Detection Capabilities	AI-driven baselining & detection, rule-based monitoring
Additional Benefits	Asset inventory of OT network, vulnerability management

SOC members distributed by vessel type

The five most common types out of 239 total



Public-Private collaboration on Cybersecurity in Norway

Sectorial Response function for Norwegian Maritime Sector
In 2023 the Ministry of Trade, Industry and Fisheries assigned the Norwegian Coastal Administration (NCA) the task of establishing a sectorial response function for the Norwegian maritime sector. The NCA cooperates with the Norwegian Maritime Authority on this assignment.

In January 2024 an agreement was established between NCA and NORMA Cyber, where the latter is to assist with technical expertise and other resources to operationalise and support NCA in their sectorial response function.

NORMA Cyber will share relevant and time sensitive vulnerability warnings to the maritime sector and contribute to transparency and information sharing of relevant information from cyber security incidents. Furthermore, NORMA Cyber will act as an advisory body during crisis- and incident management, as well as contribute to warnings and reports.

About the sectorial response set-up in Norway
Norway has a sectorial focused set-up for contingency preparedness for digital crisis. This means that each sector is responsible to establish and maintain the necessary information sharing and response functions. This function is responsible for coordination between stakeholders in the sector and towards Norwegian National Security Authority's (NSM) National Cyber Security Centre (NCSC). Details about how this system works and who does what is defined in the document "Framework for handling of ICT-security incidents" by NSM.

Examples of how the sectorial response function is set up for other sectors in Norway, that has been models for the set up in the maritime industry:

- **For the finance sector** the Norwegian Finance Authority is overall responsible, and the operational aspects are managed by the Nordic Finance CERT (NF-CERT).
- **For the Energy sector** the Norwegian Water Resources and Energy Directorate (NVE) and The Norwegian Ocean Industry Authority (Havtil) are overall responsible, and the operational aspects are managed by KraftCERT/InfraCERT.

Sjøfartsdirektoratet
Norwegian Maritime Authority

KYSTVERKET

NORMA CYBER

Sharing cyber event information with NORMA Cyber

Sharing cyber security information is essential to the collective defence and strengthening of the cyber security within the maritime sector. NORMA Cyber encourage our members to voluntarily share information about cyber related events that could help mitigate current or emerging cyber security threats. This includes events related to SATCOM, AIS and GNSS interference. Together stronger!

When cyber incidents are reported quickly, NORMA Cyber can use the information to render assistance and provide warnings to prevent other members or entities from falling victim to similar attacks. Access to information is critical to identify trends that can help us reduce the threat to our members, reduce potential consequences and be preventive for the maritime sector in general.

Types of activities you should share:

- Unauthorised access to your system
- Denial of Service (DOS) attacks that last more than 12 hours
- Malicious code on your systems, including variants if known
- Targeted and repeated scans against services on your systems
- Repeated attempts to gain unauthorised access to your system
- Email, mobile, or SATCOM messages associated with phishing
- Any type of interference, GNSS, AIS, SATCOM as well as spoofing or jamming

How should you share?
We encourage you to send an email to **ops@normacyber.no** and be as detailed as possible. Please include contact information for us to take timely and appropriate action.

Key elements to share:
Incident data and time, incident location, type of activity and a detailed narrative of the incident and how to reach you e.g. email and phone number.

Emergency number: +47 90 98 97 37

Reporting to Authorities:
Sharing of information with NORMA Cyber does not replace legally obligated reporting to the rightful authority such as Flag State, Coast State, or National Police. We always encourage our members to file a complaint to the police after being victim to cybercrime or fraud.

Building unified resilience
against cyber threats for the
Nordic Maritime Sector