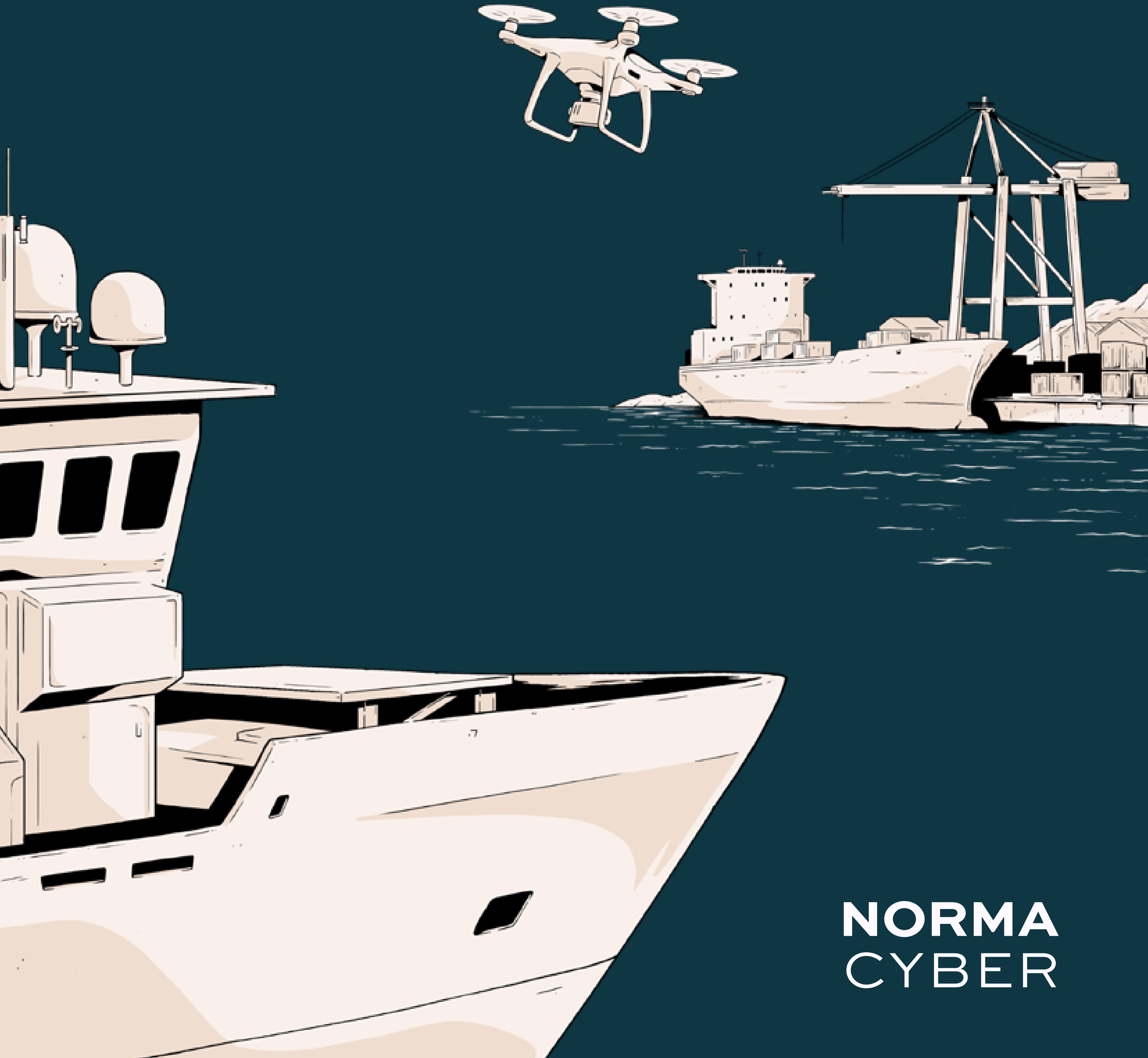
The Nordic Maritime Cyber Resilience Centre

Annual Threat Assessment 2026

normacyber.no



NORMA CYBER

The Nordic Maritime Cyber Resilience Centre (NORMA Cyber) serves as the primary hub for operational cybersecurity in the Nordic maritime industry. Established in 2021 through a collaboration between The Norwegian Shipowners' Mutual War Risks Insurance Association (DNK) and the Norwegian Shipowners' Association, the centre initially focused on Norway before expanding to the broader Nordic region in spring 2024.

NORMA Cyber operates as a non-profit organisation with members from the Nordic maritime sector. Affiliate and vendor memberships are also available to international organisations and maritime vendors.

NORMA Cyber currently has over 170 members and represents more than 3,000 vessels and offshore units.

The centre provides a centralised cybersecurity function, enabling members to pool resources and achieve greater effectiveness and resilience than through independent efforts. NORMA Cyber invests in developing new solutions that leverage emerging technologies to deliver efficient, cost-effective cybersecurity for its members.

Services include threat intelligence, timely information sharing among members, crisis response support, and related functions.

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

Our experts collaborate with security and emergency preparedness professionals at DNK and the Norwegian Shipowners' Association. Together, we have established the Norwegian Shipping Security and Resilience Centre in Oslo to support members facing complex operations involving both physical and cyber threats.

Administrative queries:
contact@normacyber.no
Phone: **22 22 00 50**

Emergency number: **+47 90 98 97 37**

Contents

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

The maritime industry operates in an increasingly uncertain global environment. Heightened tensions between major powers and ongoing regional conflicts have become the norm. The industry's reliance on complex, interconnected supply chains increase its exposure to these geopolitical developments.

Digitalisation in the maritime industry continues to advance. Fully connected vessels are now standard, with increased integration across ports, terminals, and logistics systems. Operational Technology is more closely linked to IT and external networks, enabling efficiencies but also introducing new vulnerabilities and increasing the potential impact of cyber incidents.

During periods of heightened uncertainty, our members confirm that NORMA Cyber's role as a non-profit, member-focused centre working closely with authorities is more important than ever. This is reflected in the record number of new members joining us over the past year.

Encouragingly, we also observe increased awareness and engagement in cybersecurity at the senior executive level. New class requirements and evolving regulatory frameworks, such as the EU's NIS2, are contributing to this momentum. At the same time, these developments can be challenging for maritime stakeholders to navigate.

NORMA Cyber continues to work closely with members, authorities, and partners to enable timely information sharing and continuous monitoring of the cyber threat landscape. Through this work, we have developed unique access to data and insight, allowing us to identify the most significant trends affecting the maritime sector. This report presents our key findings and assessment of the current and emerging cyber threat landscape.

We hope this assessment offers valuable insights for decision-makers and enhances situational awareness. While digital threats cannot be fully eliminated, we remain committed to supporting our members in reducing risk and maintaining safe, efficient operations.

We also hope the assessment encourages further discussion, dialogue, and information sharing. Together, we can continue to strengthen the cyber resilience in the maritime sector in the year ahead.

Enjoy the read!

Lars Benjamin Vold
Managing Director

Nordic Maritime Cyber Resilience Centre

Managing Director Lars Benjamin Vold
Nordic Maritime Cyber Resilience Centre

Executive Summary

The maritime sector remains central in both global trade and geopolitical tensions. Within this landscape, cyber espionage remains the most significant strategic concern. There is a high threat of cyber espionage operations against the maritime sector in 2026 as states prioritise intelligence collection to support military readiness and economic security. States such as Russia, China, and Iran are highly likely to continue targeting maritime organisations for intelligence on sanctions enforcement, military mobility, energy flows, and Arctic operations, often combining cyber intrusion with physical surveillance to build situational awareness and prepare digital access for potential future leverage.

Maritime entities in the Nordics are also likely to be drawn into information operations tied to geopolitical tensions, where hacktivists and state-aligned actors amplify narratives through claims of cyber activity, often combining propaganda with disruptive attacks rather than pursuing deep technical impact.

Disruptive operations will remain largely driven by politically motivated hacktivist collectives, with DDoS attacks continuing to dominate. Targeting Operational Technology is gaining popularity and leading to an increasingly complex threat landscape. The general threat to Operational Technology is low, though internet-exposed devices face a moderate threat of tampering. Alongside this, GNSS interference is becoming more sophisticated, increasingly affecting multiple satellite constellations and causing real-world navigational and commercial consequences.

The threat of destructive cyber operations against the maritime industry remains low for most of the commercial fleet. While state actors like Russia and China possess the capability to conduct destructive attacks, they currently favour hybrid approaches that blend cyber espionage with physical sabotage to avoid direct attribution.

The threat posed by financially motivated criminals against the Nordic maritime sector is high. Identity-based access and phishing will likely be the dominant methods for breaching companies, with attackers striking indiscriminately. Maritime entities will likely continue to face threats from ransomware, data theft, and malware as the criminal ecosystem continues to industrialise.

Key figures from 2025

77

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

60

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

8

claimed OT attacks in the maritme sector by hacktivist entites.

350+

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

Summary

Geopolitical Backdrop

The global security environment remains both stable and unpredictable. The security policy outlook is serious, the geopolitical situation is tense, and new conflicts continue to emerge while others enter new phases. The maritime sector is increasingly at the centre of this landscape. The maritime domain has become a key arena of geopolitical competition over trade, transportation, and energy supply.

Maritime actors are affected both directly and indirectly. Directly through physical and digital attacks in their operating areas, and indirectly, as the sector has become an increasingly attractive target for espionage, mapping, and insider activity. This places higher demands on the sector's own ability to protect assets, maintain situational awareness, and manage risk.

The interaction and rivalry among the United States, China, and Russia are fluid and have a direct impact on the global economy. This complicates the risk picture for maritime actors. At the same time, Norwegian security services assess the threat from Russia, China, and Iran against both public and private Norwegian entities as persistently high. This assessment is reflected in the threat actor landscape targeting the maritime sector.

The distinction between armed conflict on land or at sea and attacks against global maritime trade is becoming increasingly blurred. There have been repeated physical and cyber attacks against civilian shipping. In parallel, the share of the global fleet operating in the shadow fleet has grown significantly. This blurs the line between legitimate and illegitimate shipping and reinforces the perception that civilian vessels are increasingly viewed as legitimate targets. At the same time, attention towards critical maritime infrastructure is growing, both on land, at sea, and subsea, particularly in the Nordic areas.

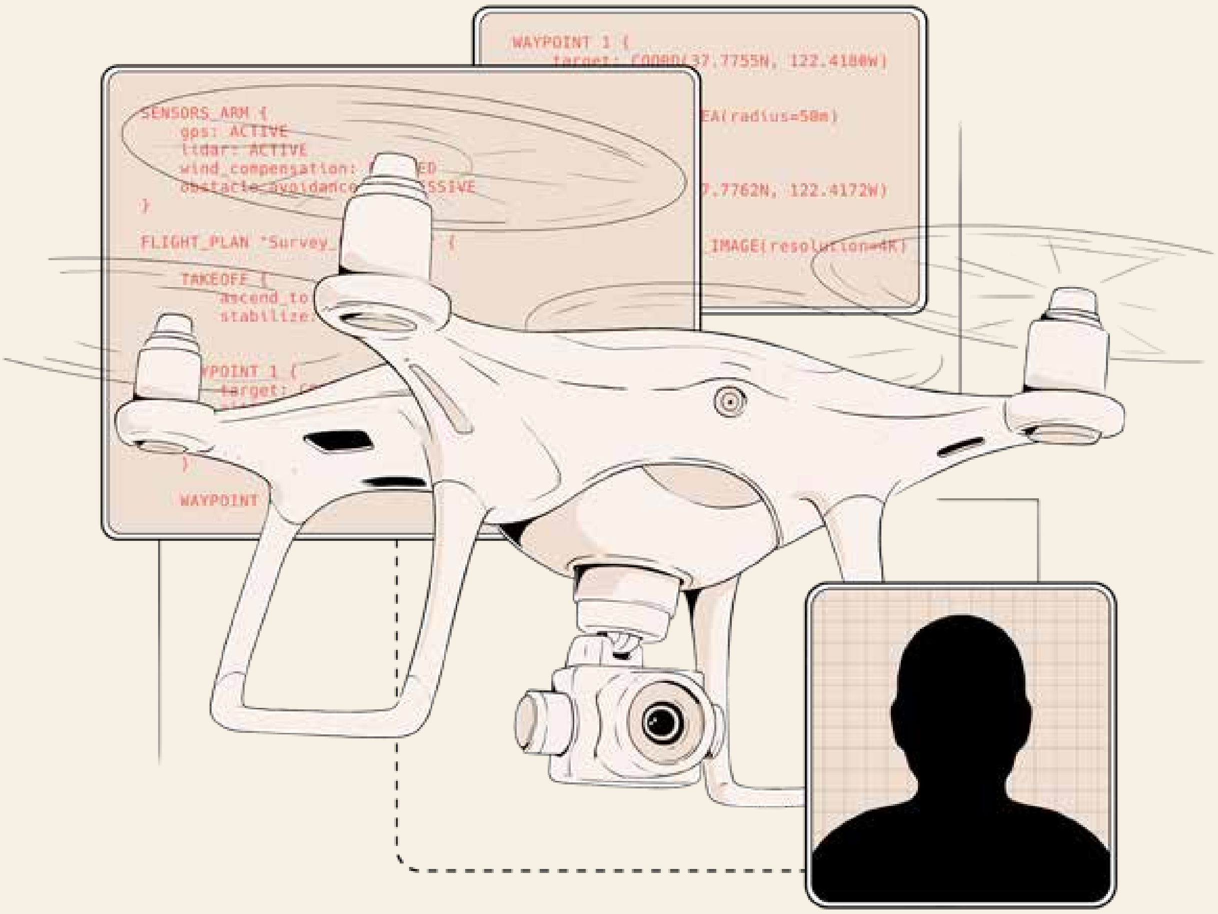
The use of drones from or against vessels is also increasing and forms part of a broader set of hybrid tools. Recent developments show that hybrid means are no longer exceptional but have become a standard part of the toolkit of both state and non-state actors in conflict environments.

The ceasefire between Israel and Hamas remains fragile. In the Red Sea, fewer attacks against shipping have been recorded at the start of 2026, but the Houthis continue to state that Israeli-affiliated tonnage remains a legitimate target.

Russia's war against Ukraine enters its fourth year, with no indication of a fundamental change despite repeated attempts to negotiate a peace settlement. Tensions in the Black Sea remain persistently high. While there have been few kinetic attacks against shipping beyond the use of sea mines, GNSS interference is extensive. This contributes to shipping traffic in the area remaining significantly below normal levels.

The South China Sea has long been a geopolitical flashpoint. The cyber dimension is an integral part of the rivalry between major powers and regional actors. Cyber operations targeting the maritime sector can be used as a means of pressure in territorial disputes and may form part of a broader struggle for influence in the region, where cyber capabilities enable impact without triggering direct military confrontation.

> The maritime domain has become a key arena of geopolitical competition over trade, transportation, and energy supply.



In the Baltic Sea, cyber-related navigational disruptions have become a persistent challenge. Reported GNSS interference has at times caused vessels to lose or receive incorrect positioning. These incidents occur in a region characterised by heightened security tensions, where reports of sabotage against critical infrastructure, transit of shadow fleet vessels, and the use of hybrid means contribute to a complex risk environment. Digital interference with maritime systems must therefore be viewed as an integral part of a broader hybrid threat landscape in Northern Europe.

These developments have led European authorities to introduce measures to strengthen security in maritime areas and lower the threshold for inspecting vessels. At the same time, it is often difficult to determine the intent behind incidents or suspicious movements. This can lead to increased suspicion towards vessels engaged in legitimate trade, more frequent inspections and detentions, and, in aggregate, contribute to the erosion of the international rules and norms on which global shipping depends—rules that have long benefited both the industry and the global economy. Pressure on international rules and norms is not limited to shipping. The growing unpredictability of the global environment is also driven by increasing challenges to the rules-based international order. Multilateral institutions are losing influence and legitimacy, while parallel alliances and agreements are increasingly formed outside established frameworks. For a global and cross-border industry such as shipping, this represents a particularly demanding operating environment.

Espionage

Maritime entities face a high threat of cyber espionage in 2026 as states prioritise intelligence collection to support military readiness, economic security, and geopolitical leverage. Shipping, ports, and energy logistics underpin national security and global trade, making organisations holding sensitive operational data into intelligence targets.

Russia's war-driven intelligence requirements, China's strategic maritime positioning, expanding Arctic energy cooperation, and persistent Middle Eastern tensions will highly likely sustain long-term collection campaigns.

The convergence of cyber intrusion, physical surveillance, sanctions evasion, and Arctic energy development increases the intelligence value of maritime networks. Maritime organisations involved in Arctic operations, LNG transport, NATO-linked logistics, and Middle Eastern energy flows will remain particularly attractive intelligence targets.

Russia: War, Sanctions and Energy Realignment

The espionage threat from Russia against maritime entities is high, particularly in Europe and the High North. Russia's war against Ukraine will highly likely continue to drive intelligence requirements in 2026. Russia-linked threat actors likely seek insight into military mobility, sanctions enforcement, energy exports, and cargo flows that undermine Russian strategic objectives.

Maritime organisations supporting NATO logistics, energy infrastructure, Arctic operations, or operations including dual-use maritime technologies are likely intelligence targets. Russia-linked threat actors will also likely collect intelligence on advanced maritime capabilities, including sensors, navigation systems, robotics, autonomy, and subsea technologies.

Russia-linked threat actors will also highly likely conduct cyber operations to enable future sabotage, disruptive, or destructive operations. Such activity likely includes mapping vulnerabilities in critical underwater infrastructure, ports, and terminals, and pre-positioning access to the infrastructure.

China: Strategic Maritime and Arctic Positioning

China-linked threat actors will likely continue long-term intelligence collection aligned with Beijing's geopolitical priorities in the Indo-Pacific, Europe, and the Arctic. The primary intelligence threat from China-linked groups is in the cyber domain.
The South China Sea remains a central arena for China-linked cyber espionage. Threat actors will likely integrate cyber operations with physical surveillance to maintain situational awareness over disputed waters. These operations likely serve dual purposes: collecting immediate political and military intelligence while embedding access in critical infrastructure for potential future leverage.

China-linked threat actors will highly likely continue to use USB devices as an initial attack vector, with the capability to bridge air-gapped maritime systems. Threat actors associated with the regime continue targeting the shipping industry, using infected USB devices to gain initial access. In mid-2025, China-linked threat actors introduced geographic containment to their malware, ensuring it only executes on machines within a specific target country. This addition is likely intended to limit infections and prevent excessive noise that could degrade threat actors' operational security.

Iran: Maritime-Energy Intersection

The espionage threat from Iran against Nordic maritime entities is moderate. Still, maritime organisations operating in the Middle East or affiliated with Israel or the United States face a high threat.

Iran-linked actors will likely continue their systematic reconnaissance and credential-harvesting against shipping companies, crew management firms, port operators, and energy logistics providers.

Their intelligence priorities are highly likely to include maritime logistics networks supporting energy exports and traffic through strategic chokepoints such as the Strait of Hormuz and the Suez Canal.

A 2025 data leak attributed to a threat actor linked to Iran's Islamic Revolutionary Guard Corps described sustained efforts to compromise crew management and chartering departments in Europe and the Middle East. The leak is assessed as authentic and indicates systematic mapping of global maritime and energy networks. Iran will likely use cyber espionage to enhance crisis readiness and to enable potential disruption during periods of regional escalation.

Surveillance of Transport Nodes

Nation-state threat actors will highly likely continue to integrate cyber intrusion with physical surveillance to enhance maritime situational awareness. Transport nodes, including ports, LNG terminals, rail-maritime interfaces, and adjacent logistics hubs, represent high-value intelligence targets due to their role in military mobility, sanctions enforcement, and energy exports.

Russia-linked threat actors have demonstrated the capability to compromise internet-connected cameras and other edge devices positioned near transport infrastructure. Such access can enable persistent monitoring of vessel arrivals, cargo handling, and movement patterns. This type of collection likely supports both real-time intelligence requirements and contingency planning. Iran will likely use cyber espionage to collect information on maritime logistics networks and infrastructure supporting energy export to enhance strategic situational awareness and to enable potential disruption during regional crises. Iran will likely use cyber operations to collect information on vessels and movements, particularly in strategic chokepoints such as the Suez Canal and the Strait of Hormuz, to support future military operations directly.

Simultaneously, China-linked actors will likely continue to leverage obfuscated relay networks to conduct industrial-scale collection of open-source maritime intelligence. Reporting identifies the use of relay networks to anonymously scrape data from amateur maritime tracking systems and software-defined radios.

By aggregating this public data from thousands of nodes, they build a granular picture of naval movements and logistics chains. By aggregating public data from thousands of distributed nodes, threat actors can construct a granular picture of maritime movements and logistics chains. Nation-state threat actors are likely to continue targeting a broad range of devices and platforms within their areas of strategic interest to either derive intelligence or establish persistent access in support of network operations.

India-linked threat actors will likely continue targeting ports and maritime organisations in the Indian Ocean region using maritime-themed phishing and credential harvesting. Their operations primarily focus on regional situational awareness and defence-related intelligence.

Tensions on the Korean Peninsula will highly likely continue to drive North Korea-linked intelligence collection. North Korean actors are likely to target maritime transportation and logistics entities to obtain sanctions-relevant economic intelligence and insights with potential military value.

The Era of Agents

The tradecraft of cyber espionage is likely to continue shifting in 2026 as automated cyber operations powered by AI and agentic systems are adopted. State actors are moving beyond simple automation scripts and are beginning to deploy AI-enabled tools that can conduct complex intrusion tasks with less human oversight.
In general, reporting indicates a surge in nation-state activity leveraging AI.
This activity is not limited to preparation for cyber operations but increasingly supports agentic operations as well. From 2025 onward, the progression moves from using AI to generate discovery and exfiltration commands to campaigns that could autonomously conduct reconnaissance, lateral movement, and data exfiltration, with a human in the loop.
The introduction of agentic AI into espionage workflows is highly likely to make campaigns in 2026 larger, faster, and more complex.

The overall espionage threat to the maritime sector remains high. This is a complex threat landscape where China and Russia pose the most sophisticated technical threats. Regional actors, including India, Iran and North Korea, present a moderate but persistent threat to entities operating within their spheres of influence.
It is highly likely that state-affiliated threat actors will continue to use cyber espionage to gain an advantage or insight into ongoing conflicts in the coming year, including targeting organisations in the maritime sector.

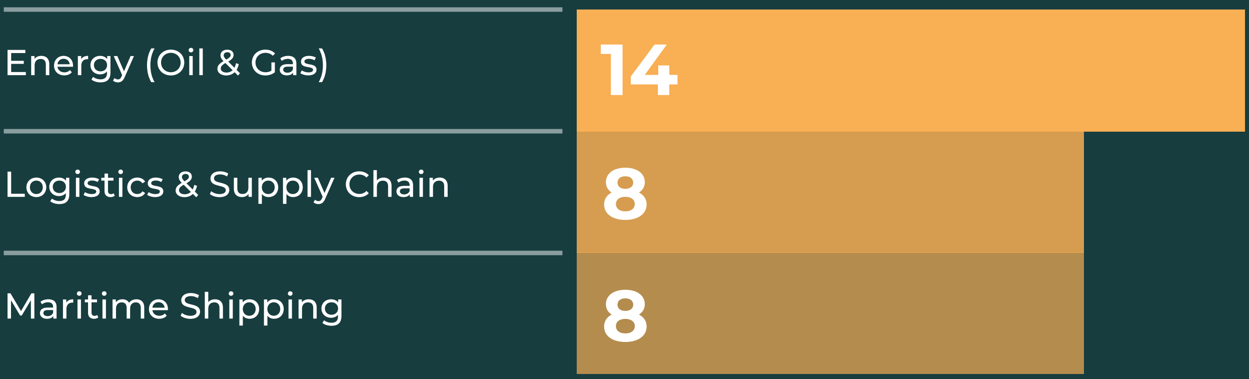
Russia-linked Threat Actor Targets IP Cameras

Russia-linked cyber-espionage activity targeting European maritime and transport infrastructure intensified in 2025. Fancy Bear conducted large-scale exploitation of Internet-connected IP cameras near ports, border crossings, rail hubs, and logistics nodes. The campaign, which likely forms part of a broader intelligence effort supporting Russian military objectives related to Ukraine, exploited unsecured IP cameras to obtain real-time visual intelligence on movements and activity at critical infrastructure. Fancy Bear used automated tooling, default or weak credentials, and proxy infrastructure located near targets to reduce detection, enabling persistent and covert collection of imagery and metadata. This activity underscores a shift toward integrating cyber access with physical intelligence. It highlights a sustained espionage threat to maritime entities, where even peripheral digital systems can be exploited to generate valuable insights.

Iranian-linked Threat Actor Targets the Maritime Sector

In September 2025, a large number of internal documents from the Iran-linked threat actor Charming Kitten were leaked on GitHub. Analysis of these documents confirms that maritime organisations are deliberately targeted as part of a strategic intelligence collection effort focused on global supply chains, energy flows, and sanctions monitoring. The threat actor demonstrates a detailed understanding of maritime operations and consistently prioritises access to departments responsible for chartering, fleet management, crewing, technical operations, and port activities. Operations primarily exploit internet-facing services, including Microsoft Exchange and VPN appliances, to harvest email archives, credentials, and internal distribution lists, enabling long-term organisational mapping and follow-on targeting. While there is no indication of an imminent disruptive intent, the scale and persistence of access achieved, significantly lower the threshold for future coercive, disruptive, or hybrid operations should an Iran-linked threat act upon a strategic priorities shift

The leaked documents include details on almost 700 organisations that have been targeted and – at least 30 confirmed compromises; 14 victims in Energy (Oil & Gas), 8 victims in Logistics & Supply Chain and 8 victims in Maritime Shipping.



```
SET confidence_score = 0.0001
SET recursive_depth = 0
SET intent

FUNCTION i
    temp_v
    WHILE
        te
    RETURN

FUNCTION n
    IF tho
        th
    ELSE:
        th
    RETURN

LOOP FOREV
    recurs
    raw_si
    inferr

    IF inf
        ap
        co
    ELSE I
        co
        di
    ELSE:
        re

    though

    FOR EA
        th
        IF

        EL


    IF rec
        re
        lo
        re

    cache(
    emit(o

    IF out
        ac
        im

FUNCTION u
    FOR EA
        be
    normal
    IF sum
        am
    RETURN
```

```
<context:init>
    <state id=
    <vector na
    <loop condition="entropy!=0 && truth<=approx">
```

AI and the Agents

Threat actors are highly likely to incorporate artificial intelligence (AI) tools to enhance operations. The speed and extent of use depend heavily on the threat actors and their goals, reflecting the same diversity in adaptation seen in legitimate organisations. AI will likely be both a target and a tool for threat actors in 2026.

AI as a Tool

Threat actors will certainly use AI to improve the quality and distribution of phishing campaigns. AI has proven to increase the believability of lures and their pervasiveness. It is also widely used to create deepfakes – media that appear real, such as photos, videos, and audio. With the rapid improvement of models and increased availability, distinguishing between real and fake is increasingly difficult. Deepfakes can be applied to phishing campaigns, fake meetings, and information operations targeting the maritime sector. The use of synthetic media undermines trust in the digital space, and, being remote in nature, the maritime sector should be aware of this.

Threat actors are highly likely to use AI to upskill and aid development. For seasoned threat actors, this may include using AI to create evasive malware that can more elegantly adapt to the environment at runtime and bypass defence mechanisms. Another way to use it, is AI-driven campaigns that can simultaneously probe potential entry points across a global fleet at a speed not possible with a manual operation. It identifies weak points faster than a human analyst can respond.

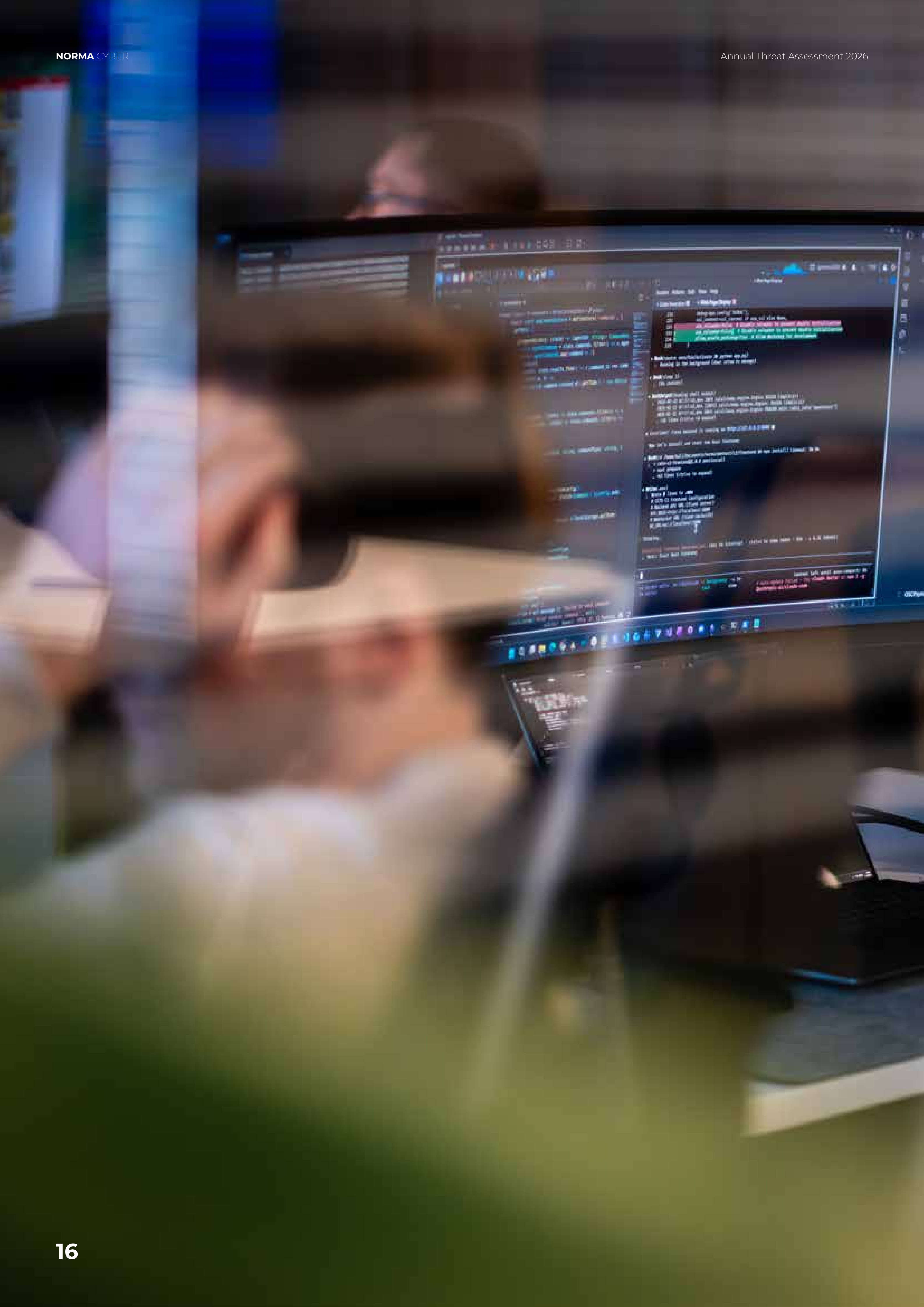
It also presents opportunities for more novice individuals and groups to develop malware and receive assistance with gaining access, moving laterally, and executing payloads. This will likely enable a larger group of threat actors to make an impact on industries and technologies they previously lacked the prerequisites for. This lowers the barrier to entry for advanced attacks.

AI as a Target

The use of AI within companies poses a threat of data leaks and exploitation of the AI itself. As AI adoption grows, workers are likely to use these tools. The use of unregulated and unapproved AI tools, such as free models, browser plugins, and other free programs, poses a high risk of information leakage. Threat actors and developers looking to increase revenue are likely to include information exfiltration capabilities in such tools, meaning that information shared with, or browsed, while the application is present on the system can be exfiltrated without the user knowing.

The rise of vibe coding, that is, when users tell an AI what they want to create, and the AI writes the code for it, also opens new attack vectors. Without proper code review, AI models can introduce security vulnerabilities that creative attackers can exploit.

Threat actors are likely to go after agentic AI. Agentic AI is an AI system that operates to some extent autonomously to achieve a goal. In the context of a company architecture, this means agents often have their own identities. Such identities tend to have broad permissions to solve their tasks, making them a valuable target for attackers looking to perform actions on the system. As agentic AI replaces or enhances internal processes, it may lead to less human understanding and insight into the system's inner workings. Such a development is likely to reduce the ability to detect malicious actors manipulating the agents.



Information Operations

Nordic maritime entities will highly likely be attacked as part of information operations seeking to promote anti-Western, anti-NATO, and anti-EU narratives. The aim is to influence audiences and strengthen set beliefs. Both states and independent threat actors conduct information operations to shape public perception and advance strategic objectives. Cyberspace, and social media in particular, has proven ideal for this purpose.

War and Geopolitics

Geopolitical tensions will likely drive reactions from entities wanting to exert influence. Most cyber-enabled information operations targeting Nordic maritime entities are likely to stem from hacktivist groups and combine statements with direct attacks. It is unlikely that the operations will be designed to manipulate the attitudes within maritime entities; instead, the activity will likely be used to amplify the worldview of the attacking entity. This includes using attacks as social proof of the attackers' (often exaggerated) skills and superiority, justifying the attacks with political reasons, and using continuous claims to repeat a simplified narrative. Doing this, the attackers likely hope to strengthen the support for their views and increase public trust in their nation's capabilities.

Russia actively uses various forms of cyber-enabled information operations as part of a broader strategy. Pro-Russian threat actors are likely to operate across the spectrum of state responsibility. Prominent groups are likely to function as state proxies, and their actions and messages will likely be amplified by entities that genuinely believe in the projected narrative. The threat actors operating overtly on social media platforms are highly likely to combine information operations with disruptive attacks, such as Distributed Denial-of-Service and intrusion attempts.

The Arctic

Public discussions about the Arctic regions will highly likely be prominent in 2026. If the situation should escalate to a point where power dynamics shift, maritime entities operating in the region and their actions are likely to be used and abused in various media stories. The form and angle will depend on the publishing entity and the potential narrative they wish to amplify. Entities involved in fishing, energy, and military operations face the highest threat.

Environment

With an increased divide between Western countries on topics such as climate change, environmental movements and their sympathisers will likely raise their voices digitally, mostly on social media. As for disruptive tactics, climate activists have historically had more success with physical demonstrations to garner attention, and this will likely remain the primary modus operandi. That said, entities engaged in fossil fuel operations with countries deemed climate negligent may face social or reputational backlash from people engaged in environmental matters.

Disruptive Attacks

Nordic maritime entities face a moderate threat of politically motivated disruptive attacks towards their infrastructure. The intention behind disruptive attacks is to negatively impact systems and leverage their unavailability to exert pressure. Such attacks are highly likely to cause financial losses if aimed at services and devices used in operations.

Hacktivist collectives motivated by political or religious beliefs are the main drivers of disruptive attacks. Their primary disruptive attack method is to use Distributed Denial-of-Service (DDoS) attacks to knock web resources offline, causing a temporary outage by saturating network traffic. Some high-profile groups likely have state involvement. By using hacktivist proxies, states can maintain plausible deniability and reduce direct attribution, enabling them to engage in illicit activities while still adhering to international agreements.

Disruptive cyber operations are likely to cause financial losses if aimed at systems and services used in operations, irrespective of the attacker's underlying motivations. The financial ramifications typically arise from operational downtime, service delays, and incident response. Ports and passenger transportation companies have dominated the maritime DDoS victim lists in 2025, and this is likely to continue.

It is anticipated that the broader hacktivist community will continue to favour low-complexity attack methodologies. DDoS attacks are expected to remain the predominant tactic, facilitating service disruption by saturating traffic without breaching the targeted systems. Prominent hacktivist groups are likely to continue developing tools and expanding their arsenals.

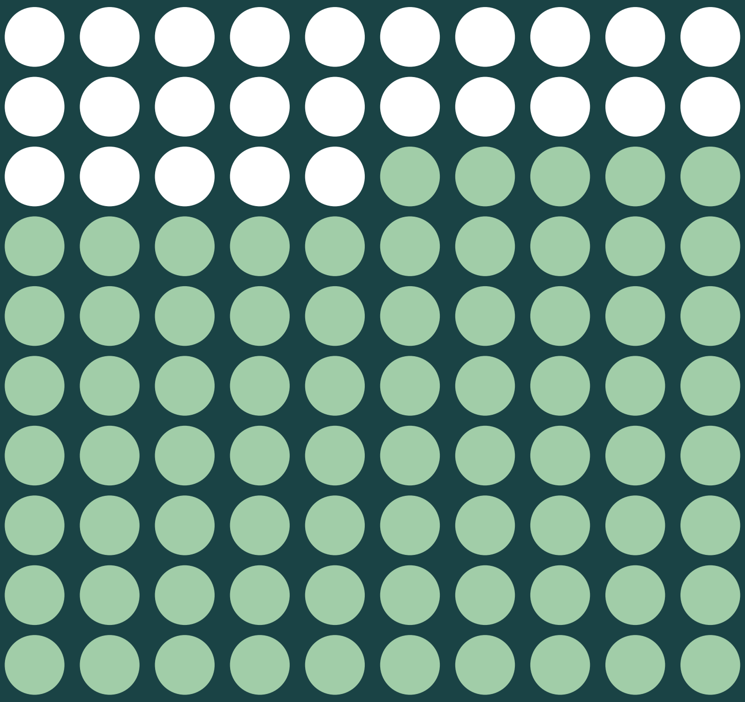
2025 saw the continued evolution of hacktivists attempting attacks on operational technology (OT) systems globally, a trend likely to continue in 2026. This is likely due to the ease with which OT attacks can be carried out and their effectiveness in building an image as a disruptive, capable threat in the public's eyes. The general threat towards operational OT in the Nordic maritime sector from hacktivist entities is low. However, misconfigured, poorly secured, or internet-exposed devices face a moderate threat of tampering and being used as boasting material.

The intentions behind the attacks are multifaceted and vary depending on the threat actor. The majority of hacktivists operating in this domain are politically motivated, using OT attacks to gain publicity and build reputations. Attacks on OT systems, particularly those with physical and/or economic impact, are highly likely to cause some media attention, helping the hacktivists fulfil their desire for exposure. This is not to say that some of them do not wish to do physical harm. Hacktivists are highly likely to misjudge and overestimate their impact on physical systems, leading to a general disconnect between claimed achievements and verifiable outcomes.

Hacktivist groups with a high operational tempo likely find and gain access to OT systems by scanning for internet-exposed Virtual Network Computing (VNC) instances. VNC is a technology that enables users to remotely view and control a computer over a network. If a discovered VNC instance is password-protected, they are likely to attempt brute forcing using password lists.

75,82%

of DDoS attacks from NoName057(16) were towards ports



NoName057(16)

The hacktivist group leading the targeting of maritime entities in the Nordics is NoName057(16). The pro-Russian hacktivist group has been active targeting NATO allied countries since shortly after the beginning of the Ukraine-Russia war. NoName057(16)'s core leadership is highly likely to be affiliated with government entities, shaping the group and its operations.

Targets are chosen by the central group, and followers are encouraged to participate in attacks through DDoSia, their self-developed proprietary tool. NORMA Cyber recorded 182 DDoS attacks towards maritime entities carried out by individuals using DDoSia. Of those, 138 targeted ports and port entities.

GNSS Interference Threats

The Global Navigation Satellite System (GNSS) interference threat will continue to be high in geopolitically sensitive areas in the coming year. Nordic shipowners operating in such areas will highly likely experience GNSS interference.

The most frequently observed methods are jamming and spoofing, where jamming results in a loss of position or time, and spoofing results in an incorrect position. A prolonged loss of position or time will likely have a cascading effect on other systems onboard. Interference has also caused vessels to run aground and halted terminal and port operations.

The primary intention is likely defensive, using interference techniques to create GPS-denied environments around critical military installations to protect against drone and missile strikes. However, it also serves as a strategic signalling tool in hybrid warfare, demonstrating capability and asserting influence over contested maritime spaces without direct military confrontation. GPS or AIS spoofing is also used by civilian vessels engaged in sanctioned or illicit activities to evade vessel tracking services.

Interference is expected to remain persistent in geopolitically sensitive areas, such as the High North (Barents Sea), the eastern part of the Baltic Sea, the western and northern parts of the Black Sea, the eastern Mediterranean, the Red Sea and the Suez Canal, the Arabian Gulf/Persian Gulf, and the Strait of Hormuz.

One notable trend is that the interference is becoming more sophisticated, affecting multiple GNSS constellations and utilising hybrid patterns of spoofing and jamming. The development increases the threat to maritime operations. While GNSS provides critical positioning, navigation, and timing services, it remains inherently vulnerable due to low-power satellite signals, lack of authentication, and civilian receiver limitations. By late 2025, reports indicated a shift toward “hybrid” patterns, revealing a combination of spoofed GPS L1 signals alongside concurrent jamming of GLONASS, Galileo, and BeiDou constellations. This multi-constellation targeting makes it difficult for vessels to switch to backup satellite systems.

In 2025, NORMA Cyber members reported GNSS interference in the Norwegian Sea, the Barents Sea, the Baltic Sea, the Red Sea, the Arabian Gulf / Persian Gulf and the Gulf of Oman. GNSS interference also affected terminal and port operations at the Jubail Inner Anchorage and the King Abdullah Port in Saudi Arabia, the Port of Gdansk in Poland and the LNG Terminal in Bahrain.

Interference in the Northern Seas

The eastern part of the Baltic Sea outside Kaliningrad will highly likely remain congested with GNSS interference. This area has undergone a significant transformation, evolving from persistent but localised jamming into a sophisticated, hybrid warfare campaign characterised by a dramatic increase in incident frequency, geographic expansion, and technical complexity. Last year, the interference extended westward into southern Sweden, and a nearly persistent belt of interference was established from the Gulf of Finland down to the Gulf of Gdańsk, heavily affecting the approaches to Kaliningrad, Klaipėda, and Gdańsk. The sheer volume of interference events surged drastically in 2025. In September, the Swedish Transport Agency reported that GNSS disruptions had escalated from 55 incidents in 2023 to 733 incidents in 2025, with the activity traced to Russian territory. A July study successfully triangulated the origins of these signals to Baltiysk (Kaliningrad) and areas around St. Petersburg, confirming that high-powered equipment was being deliberately directed into international waters. Russia utilises electronic warfare tactics to signal assertiveness in strategic areas and influence maritime spaces. It is likely that the GNSS interference in the Baltic Sea will remain high in 2026.

Interference in the Barents Sea

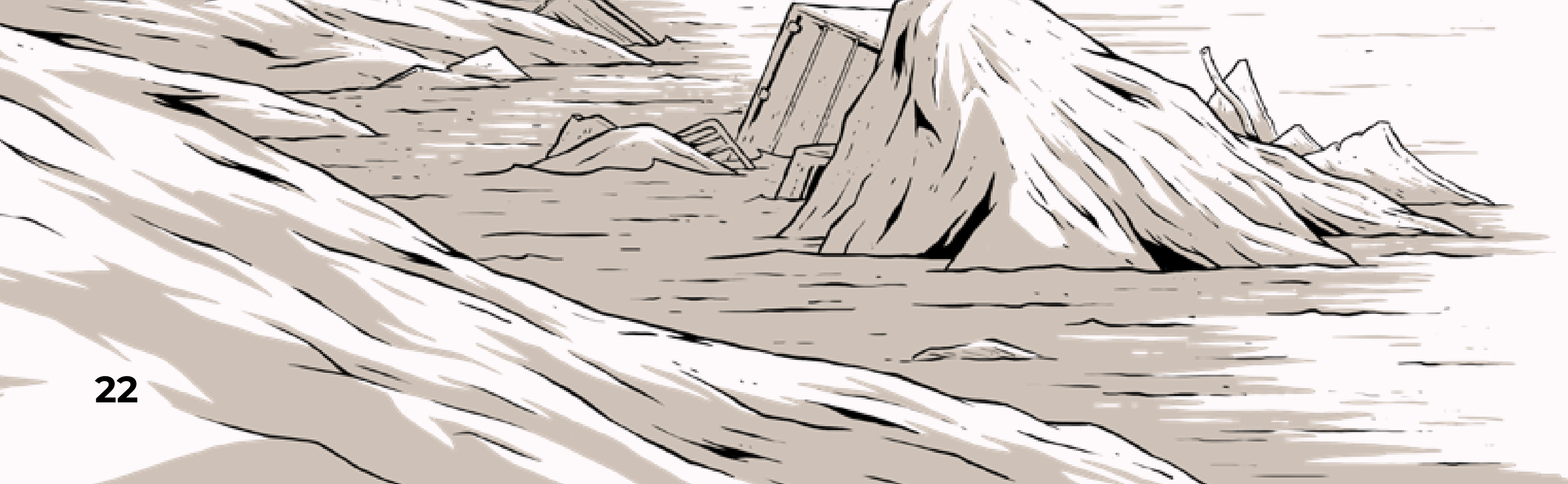
It is likely that the GNSS interference in the High North will remain high for 2026. The GNSS interference in Eastern Finnmark and the Barents Sea evolved significantly in 2025, shifting from high-altitude jamming to more sophisticated, low-altitude spoofing capable of affecting ground-level operations. NORMA Cyber members have reported GNSS interference in the Barents Sea.

Russia utilises GNSS interference as a strategic protection measure to shield high-value military and political assets from modern threats such as drones and precision-guided munitions. In late November 2025, Russia deployed significant military assets to the Kola Peninsula, when 16 Tu-22M3 long-range bombers were relocated to the Olenya Air Base. The bomber group's expanded presence increases the likelihood of intensified GNSS interference across the Barents region.

Interference in the Red Sea, Arabian Gulf / Persian Gulf

The GNSS interference threat in the Red Sea and Arabian Gulf / Persian Gulf will be moderate the coming year. In 2025, GNSS interference in the Red Sea evolved from localised jamming in the south to widespread interference reaching the Suez Canal. The operational impact became evident on 10 May, when the container vessel MSC ANTONIA grounded off Jeddah, Saudi Arabia. The incident was assessed as likely caused by comprehensive GPS or AIS spoofing in the area.

In the Arabian Gulf / Persian Gulf, a marked escalation occurred in June following Israel's strike on Iranian nuclear facilities. Open sources reported widespread spoofing affecting up to 200 commercial flights per day, while maritime reporting documented false positioning signals and extreme jamming in the Strait of Hormuz. Despite the ceasefire, interference intensified again during the third and fourth quarters, and on 30 September, a significant spike was reported at the Jubail Inner Anchorage in Saudi Arabia, where port control temporarily halted all vessel movements due to unreliable GNSS. This also affected the Bahrain LNG terminal.



Operational impact of GNSS interference

The Grounding of MSC ANTONIA

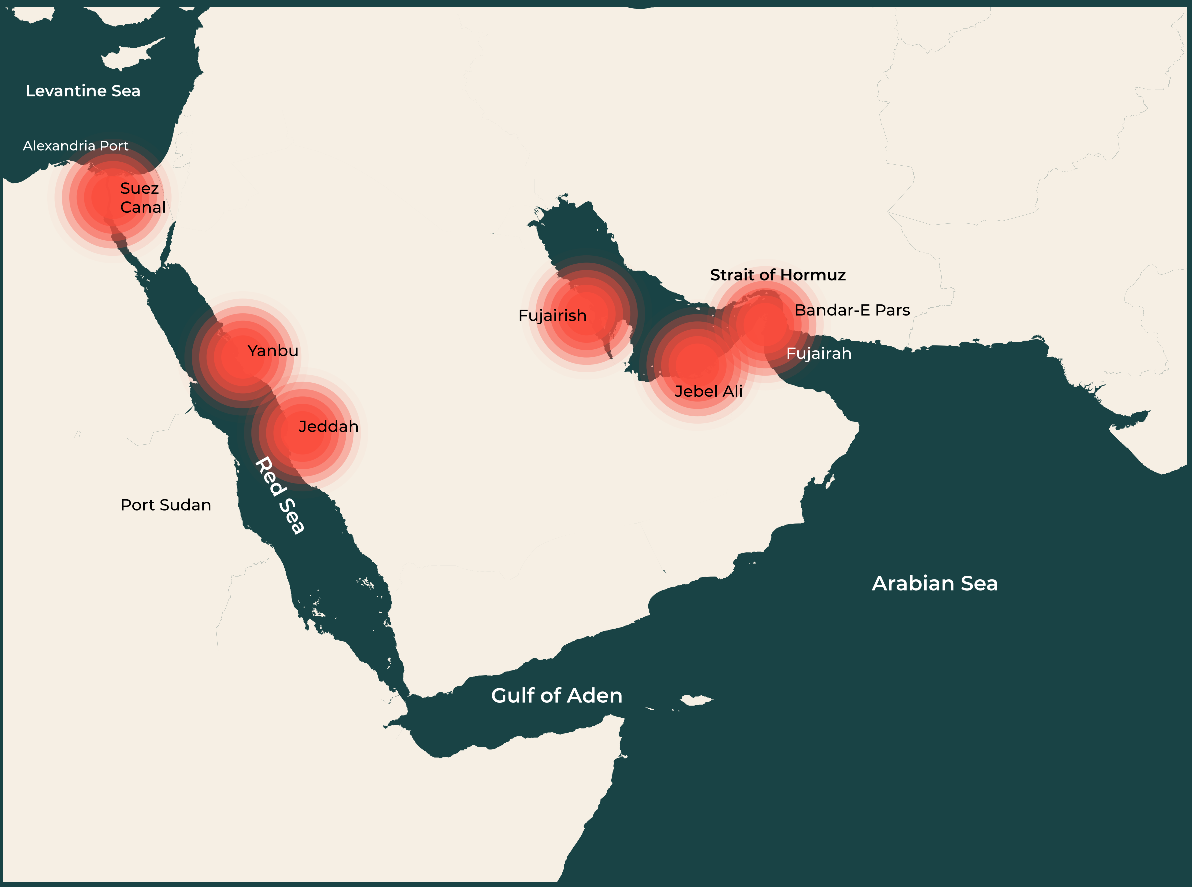
On 10 May 2025, the Liberia-flagged container vessel MSC ANTONIA (IMO 9398216) ran aground off Jeddah, Saudi Arabia.
The vessel is likely to have been a victim of comprehensive GPS or AIS spoofing in the operational area. This occurred during a period of documented navigational instability in the Red Sea, with MarineTraffic showing numerous vessels with spoofed positions in the region at the time. The area was equipped with established navigation aids, including the SHIB ALKABIR BEACON.

The Grounding of MEGHNA PRINCESS

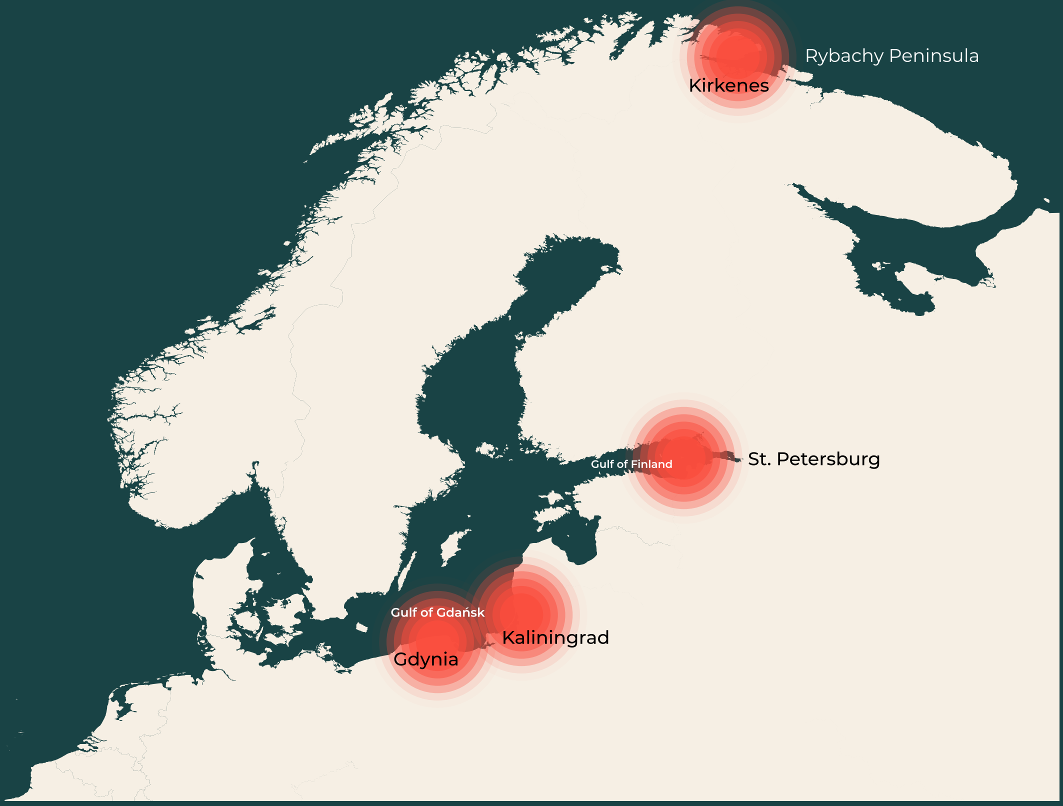
On 29 December 2024, the Bangladeshi-owned bulk carrier MEGHNA PRINCESS (IMO 9805776) ran aground near the Russian port of Ust-Luga in the Gulf of Finland.
The vessel was outside the main transit lanes when it struck the rock, which was marked by four cardinal marks, although media reported that the vessel went off course due to GPS jamming. GPSJam data confirmed high interference levels in the area on 28 December.

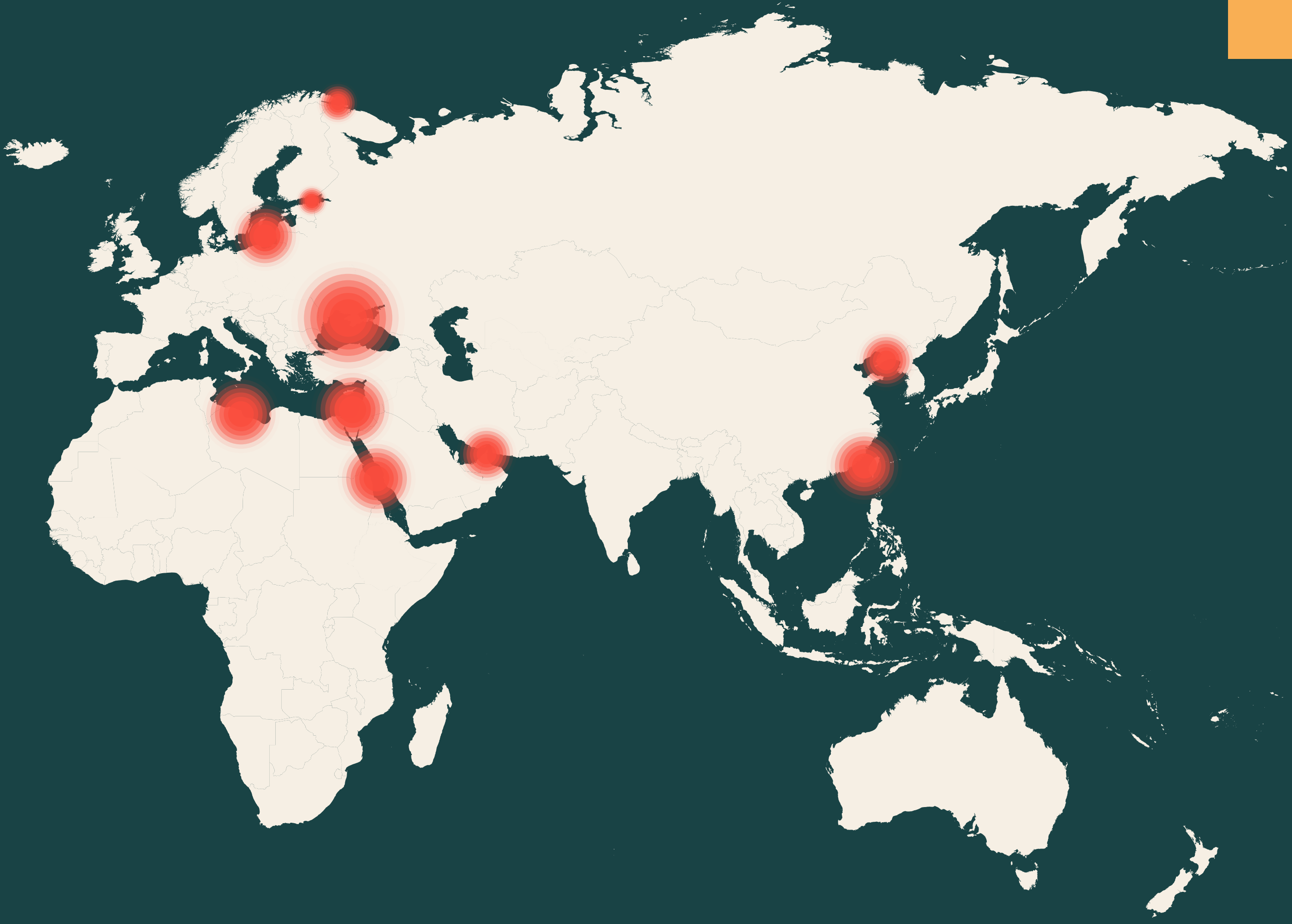
GNSS Interference Threats

Hotspots in the Red Sea and Arabian Gulf / Persian Gulf in 2025



Hotspots in the Barents Sea and the Baltic Sea in 2025





High Threat Areas

Black Sea

High GNSS interference in Northwestern Black Sea, and around the Crimean Peninsula, Sevastopol, Novorossiysk, and Sochi.

Key Maritime Chokepoints

High GNSS interference in the Suez Canal, central Red Sea and in the Hormuz Strait.

Barents Sea and Baltic Sea

High GNSS interference around Kirkenes and the Rybachy Peninsula, in the Eastern part of the Baltic Sea, from the Gulf of Gdańsk to the Gulf of Finland, including Kaliningrad and St. Petersburg.

Eastern Mediterranean

High GNSS interference in the Levantine Sea and outside the port of Alexandria and Tripoli.

Key Events

From Jamming to Hybrid Threats

Reports show a shift to hybrid tactics, combining jamming of multiple constellations with GPS spoofing.

Massive AIS Spoofing Event

Thousands of fake vessels appeared in the Baltic Sea, when a shore station in Finland sent fake AIS data into vessel tracking services.

Destructive Operations

There is a low threat of deliberate destructive operations towards the broader Nordic maritime sector. Destructive cyberattacks are intended to disrupt or destroy physical or digital systems. For entities supporting NATO logistics, energy infrastructure, or Ukraine, the threat is assessed as moderate. The elevated threat towards these segments stems from the merging of cyber operations with hybrid warfare tactics, such as physical sabotage, which directly threaten safety and operational continuity.

Russia-linked threat actors pose the most credible and destructive threat to the maritime sector. These threat actors increasingly integrate cyber capabilities with physical sabotage. While Russia possesses the ability to conduct destructive cyber operations, it is more likely to use proxies or hybrid tactics to avoid direct attribution and NATO escalation. The primary manifestation of the Russian threat in the maritime domain remains hybrid rather than purely cyber.

Threat actors linked to Russia's military intelligence service, the Russian General Staff Main Intelligence Directorate (GRU), represent the most significant destructive threat to maritime infrastructure. Threat actors linked to the unit are known to use a mix of customised commodity malware and bespoke destructive tools, and to incorporate deception, such as disguising destructive malware as ransomware, to misdirect attribution efforts.

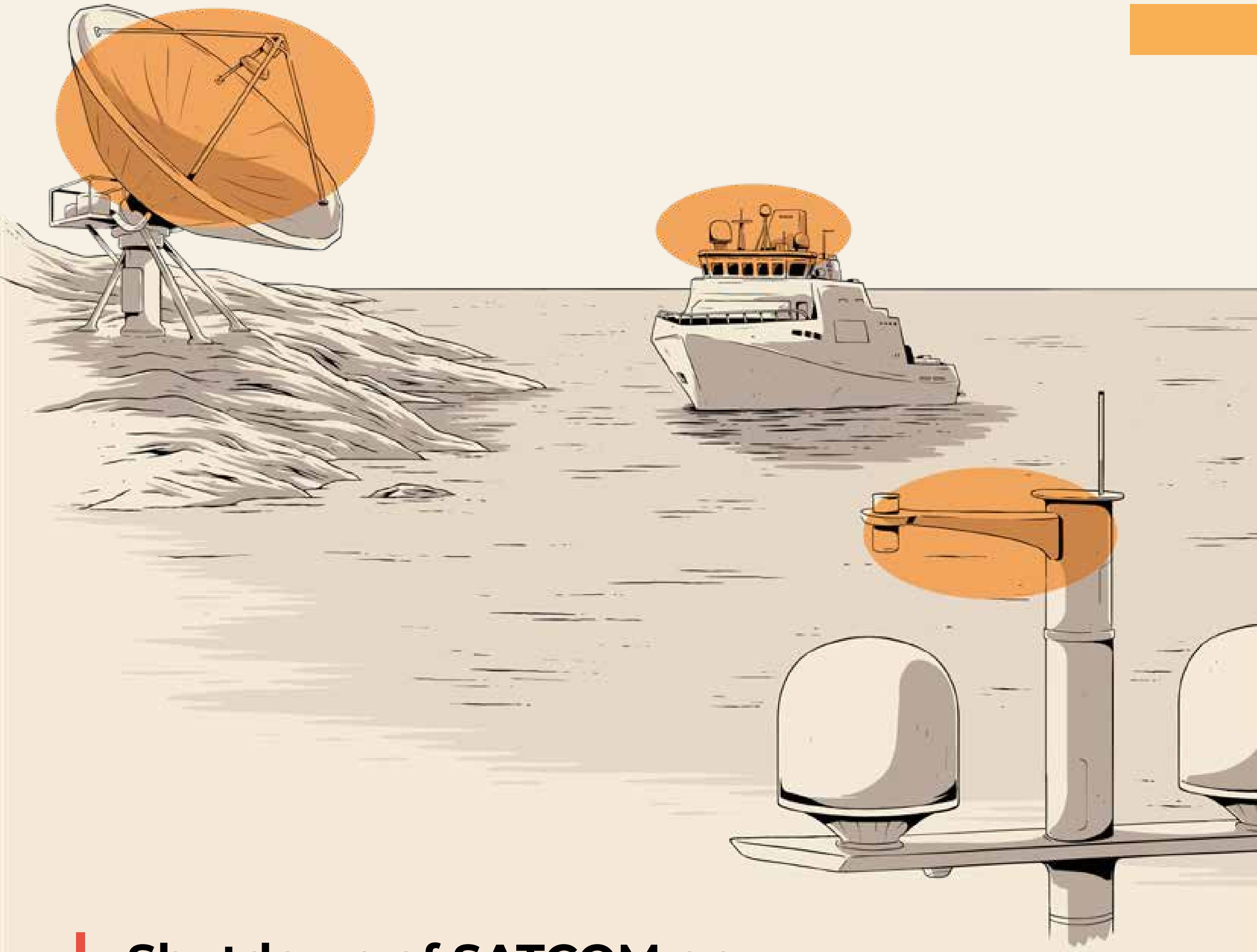
Russian threat actors will likely target operational technology networks to establish long-term access for potential future disruption. GRU-linked threat actors have been observed conducting campaigns aimed at gaining stealthy access to OT environments across the energy, transportation, and government sectors. While direct physical destruction of maritime OT remains difficult, Russia has demonstrated the capability to conduct data-wiping campaigns against logistics and energy entities in Ukraine.

Russia likely uses proxies, such as hacktivist groups, to conduct disruptive and destructive operations. This strategy weakens direct state control but lowers the threshold for sabotage operations against Western targets. These proxies continually attempt to tamper with exposed infrastructure, allowing the Russian state to maintain plausible deniability while pestering entities in nations that do not share the Russian narrative. Despite the intent, the destructive impact through hacktivist proxies is likely to be accidental rather than intentional.

The destructive cyber threat from Iran-linked threat actors towards Nordic maritime entities is low. Entities that have direct affiliations with Israel or the US, or those operating in the Middle East, face a moderate threat due to the potential for becoming collateral damage in regional conflicts. Iran has demonstrated a distinct shift toward "cyber-enabled kinetic targeting", merging digital reconnaissance with physical strikes. Reporting indicates that threat actors linked to the Iranian regime have compromised vessel tracking systems, such as AIS platforms and CCTV feeds, to track ship locations in real-time, directly supporting physical missile attacks in the Middle East.

The immediate likelihood of a destructive Chinese cyberattack is low, but the groundwork is being laid to disrupt maritime logistics chains if geopolitical tensions escalate. China-linked activity focuses primarily on pre-positioning within critical infrastructure to deter external military support for Taiwan. This includes targeting ports and utilities and exploiting edge devices to maintain long-term, stealthy access and potential destruction. Given the critical nature of transportation networks, ports, and shipping infrastructure, they are likely within scope.

In summary, the threat of destructive cyber operations remains low for most of the commercial fleet but moderate for entities tied to strategic interests. State actors currently favour hybrid approaches, blending cyber espionage and physical sabotage, over direct destructive cyberattacks.



Shutdown of SATCOM on Sanctioned Vessels

The operation targeted the Islamic Republic of Iran Shipping Lines (IRISL) and the National Iranian Tanker Company (NITC). These vessels were subject to US and EU sanctions and suspected to be involved in the illicit transport of dual-use missile components from China to Iran.

The operation was likely carried out by compromising an Iranian shore-based IT and satellite communications service provider.

Attackers exploited the backend infrastructure supporting fleet VSAT services.
Using compromised credentials and VPN tunnels, the attackers moved laterally from the shore-side network to shipboard equipment via internal IP ranges.

The attack focused on iDirect VSAT modems. The attackers executed commands via an interactive shell to terminate the core iDirect modem process, immediately disabling satellite communications.

Flash storage was overwritten, destroying both active file systems and recovery partitions.
Affected vessels likely lost email, internet connectivity, crew welfare services, and remote diagnostics. It is unlikely that the operation prevented vessels from sailing.
The incident underscores the systemic risk posed by shore-based "single points of failure," in which the compromise of a single service provider can cascade across an entire fleet.

Threats to Operational Technology

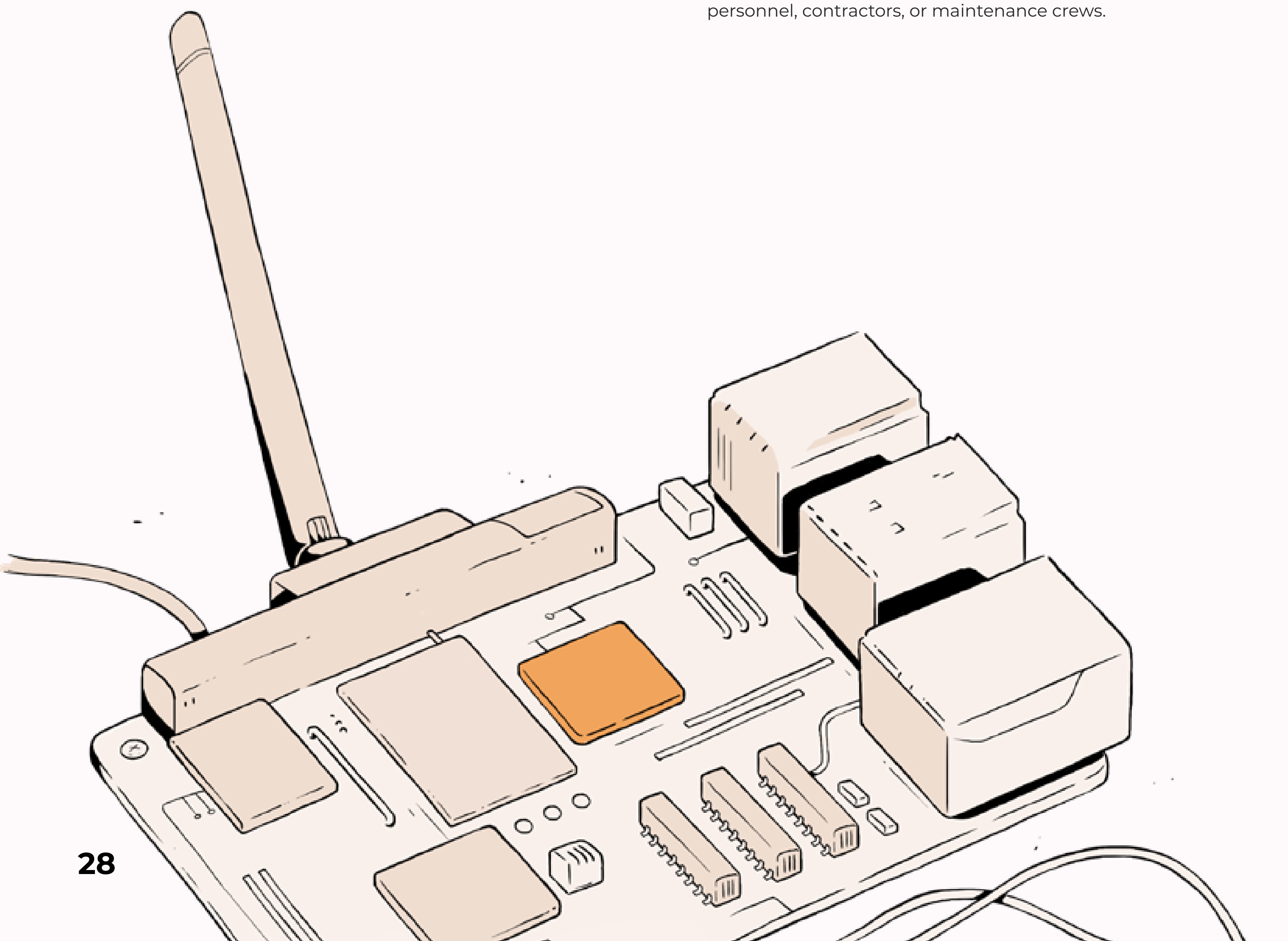
The general threat towards maritime operational technology (OT) is low. However, maritime OT will highly likely face an increasingly complex threat landscape. Throughout 2025, two themes emerged: the risk of sensitive information exposure from Original Equipment Manufacturers (OEMs) and integrators, and the persistent threat posed by malicious insiders.

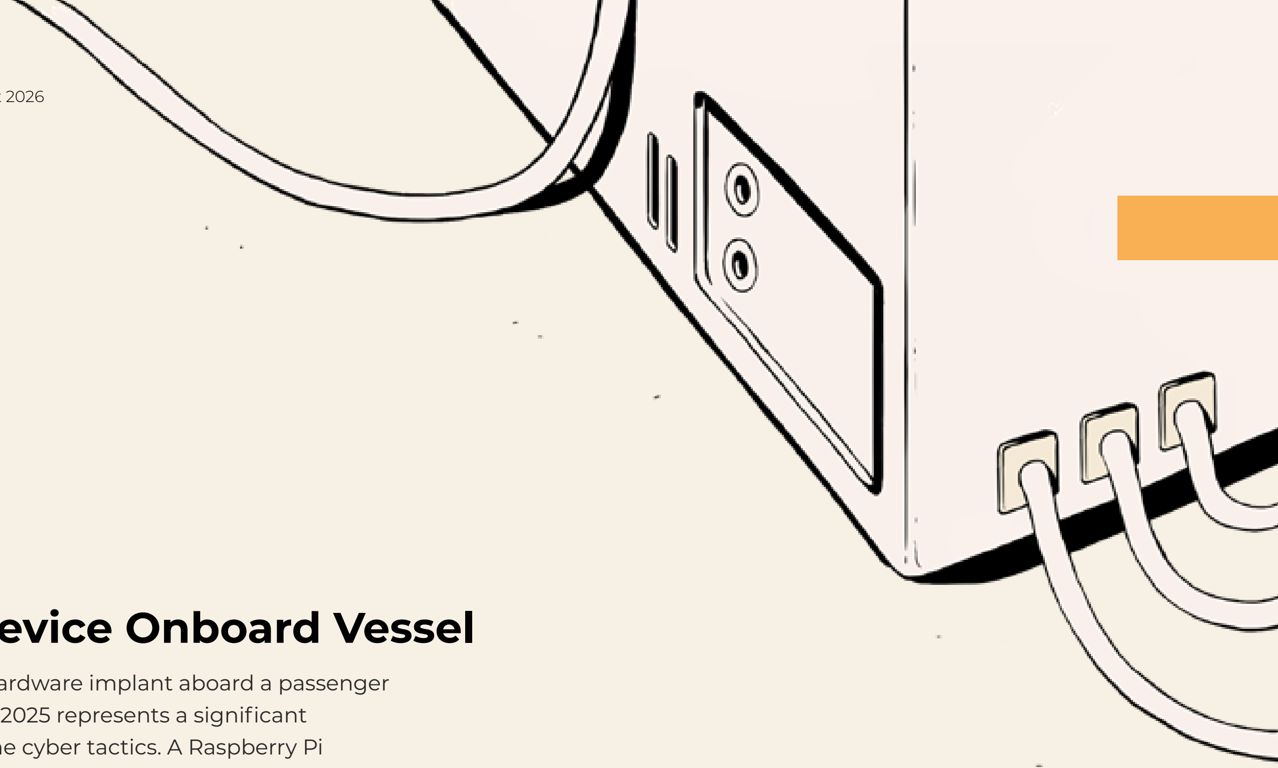
Insider Threats and Hardware-enabled Attacks

It is likely that threat actors will attempt to plant hardware on vessels in 2026. The most prevalent intent will likely be to facilitate organised crime but prepositioning and espionage cannot be ruled out. One key driver for the increased threat is the public exposure of cases where threat actors have succeeded with the tactic, thus proving it viable and possibly inspiring others. Another enabling factor is the increased availability of enablers such as hardware and tailored AI guidance.

Depending on the aim and actions performed through the implant, rogue devices can be near impossible to detect without endpoint and network monitoring across both OT and IT environments.

The trend of using malicious insiders to plant hardware devices is particularly concerning for vessels operating in geopolitically sensitive regions or those involved in critical infrastructure. The low technical barrier to entry, combined with the difficulty of detecting such attacks, makes this an attractive attack vector. Threat actors will likely continue to exploit physical access through compromised personnel, contractors, or maintenance crews.



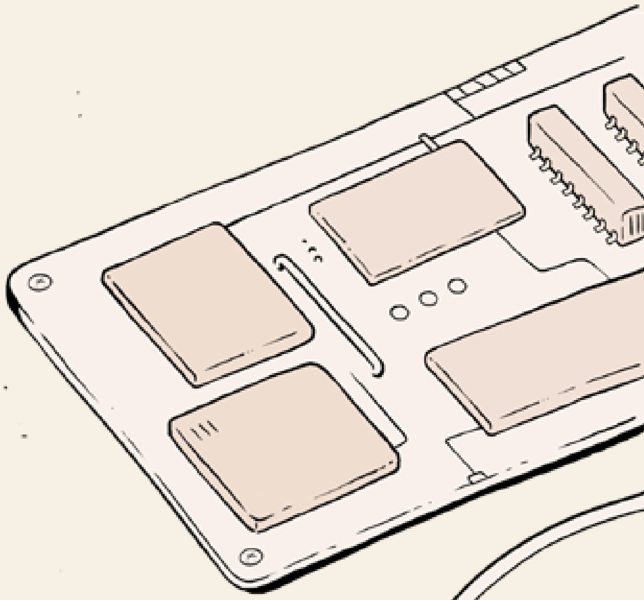


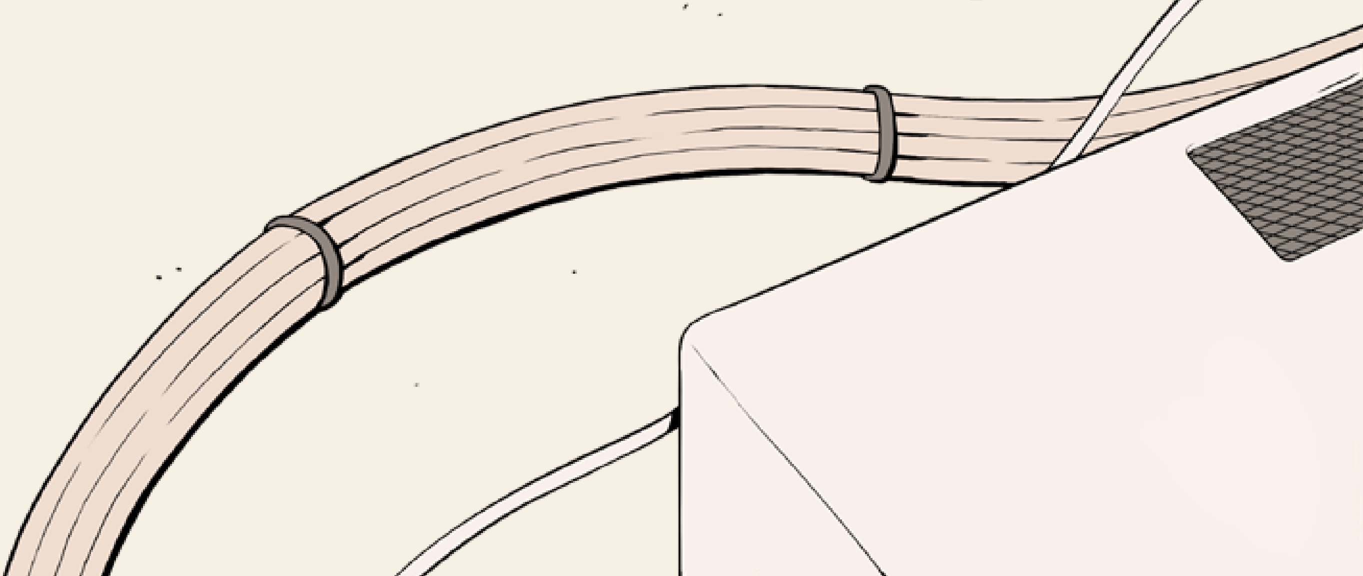
Hidden Device Onboard Vessel

The discovery of a hardware implant aboard a passenger vessel in December 2025 represents a significant evolution in maritime cyber tactics. A Raspberry Pi Zero, equipped with a cellular modem, was physically connected to the vessel's office network. This created a persistent backchannel that bypassed standard security controls. The device was configured to establish a covert network tunnel, enabling remote access, credential theft, and network reconnaissance—all functioning independently of the ship's authorised connectivity.

The likely involvement of crew members in deploying this implant highlights the critical nature of the insider threat.

Physical access to network infrastructure remains one of the most effective ways to bypass cybersecurity controls, especially when combined with sophisticated hardware that operates outside standard network monitoring. The cellular component allowed threat actors to maintain communication regardless of the vessel's internet status, limited only by cellular coverage





Increased Threat Through Information Exposures
Nordic maritime entities face a moderate threat of sensitive data exposure through supply chain breaches. When targeting OT systems, a threat actor's success is highly likely dependant on their understanding of the system. When attackers possess detailed documentation — such as network topologies, IO lists, and functional diagrams — it becomes significantly easier to develop attacks capable of manipulating vessel controls.

Building on this threat, criminals exfiltrating proprietary software, source code, and functional documentation for OT equipment deployed on vessels and subsequently leaking it on the dark web is highly likely to aid threat actors looking to exploit affected components down the road. These breaches create cascading exposure risks, as a single compromised manufacturer may hold technical specifications for equipment deployed across hundreds of vessels and multiple operators. Exfiltrated source code and functional documentation provide threat actors with a deep understanding of system internals, potential vulnerabilities, and integration points that would otherwise require extensive reverse engineering to uncover. Once available online, the information fundamentally lowers the barrier to sophisticated attacks.

Throughout 2025, there have been several breaches at shipbuilders and equipment manufacturers that resulted in the exfiltration of proprietary software, source code, and functional documentation for OT equipment deployed on vessels.

The rapid evolution of AI significantly amplifies the threat posed by leaked technical data. Historically, analysing vast amounts of source code or complex functional diagrams required deep domain expertise and a substantial investment of time. With the advent of AI, threat actors can now automate much of the analytical work. By combining exposed technical documentation with AI-driven analysis, the timeline from initial data theft to a viable attack is drastically shortened.

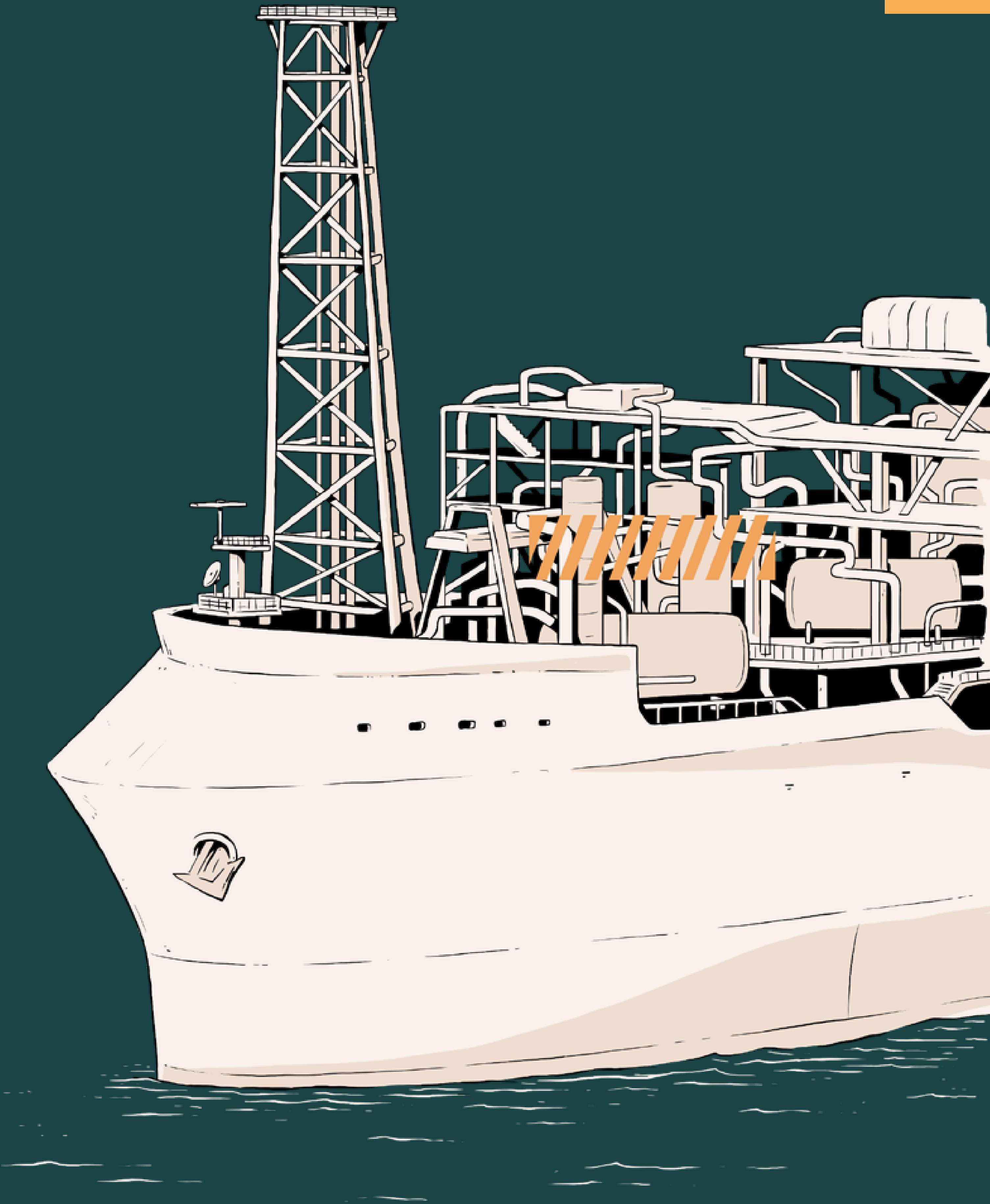
How to Secure OT Assets?

Enhancing Physical Security: Improving access control and monitoring for crew, contractors, and maintenance personnel.

Monitoring: Deploying Endpoint Detection and Response (EDR) and network monitoring to detect unauthorised hardware and anomalous traffic.

Supply Chain Resilience: Establishing stricter cybersecurity requirements for OEMs and integrators to limit the exposure of sensitive system documentation.

By recognising that OT security is no longer just about firewalls, but also about physical integrity and rigorous information management, the industry can better defend itself against the next generation of targeted cyber threats.



Financial Crime

The threat from criminals towards the Nordic maritime sector is high. The criminal ecosystem is expected to continue its industrialisation and the cultivation of specialised roles. Financially motivated criminals are likely to strike organisations indiscriminately. Notable attacks in 2025 not only affected the primary target but also had repercussions for dependent organisations. These trends will likely continue in 2026.

Initial Access

Identity-based access will likely be the dominant method for breaching the maritime sector in the coming year. Exploiting identities allows attackers to log in without resorting to vulnerabilities. Attackers may steal the identity of both humans and machines. Phishing presents a high threat of financial fraud, data theft, and network compromise to onshore and offshore maritime assets.

Phishing will likely be the primary technique used to obtain valid identities. Attacker-in-the-Middle (AiTM) phishing, in which attackers steal tokens to bypass Multifactor Authentication (MFA), has been particularly prevalent over the last year. This trend is likely to continue. Another technique Nordic entities are likely to encounter in 2026 is variants of ClickFix, which trick users into copying and executing malicious code. Having users unknowingly perform malicious actions helps bypass traditional detection methods. Criminals are likely to continue developing and automating new ways to use the ClickFix technique to evade detection and scale campaigns better.

Information Stealers

The use of information-stealing malware, infostealers, will likely continue to develop in the coming year. Infostealers have been popular amongst threat actors for years and are often offered as a subscription service. Infostealers are lightweight malware usually spread through, for example, free software, fake ads, and methods like ClickFix. They are best known for stealing credentials and financial data stored in browsers, but many can also extract other types of data and fingerprint systems.

Threat actors are likely to increasingly expand the use cases for infostealers into loaders of secondary payloads. NORMA Cyber frequently sees credentials, including member domain emails, in infostealer logs posted for sale on underground marketplaces. In most cases, these are highly likely to stem from infected personal devices used to access company resources. It is also common to see professional emails being used for personal services, such as games.

Initial access brokers will highly likely continue to mature and expand their portfolio. An initial access broker is a threat actor who specialises in breaching organisations and sells the access to others.
With the professionalisation of the criminal ecosystem, prominent initial access brokers are likely to form business relationships with groups performing actions on objective for swift usage and monetisation of the access. The most common access types posted for sale on underground marketplaces are remote access through Remote Desktop Protocol (RDP) tools and web services using credentials. This is likely to continue in 2026.

Extortion

Nordic maritime entities face a moderate threat of extortion from financially motivated threat actors. These criminals commonly apply data theft, ransomware, and data deletion to pressure victims into paying ransom demands. Maritime entities also face an inherent threat from having services they depend on in day-to-day operations disrupted by criminal threat actors.

Criminals performing AiTM phishing will highly likely rely on commodity phishing kits with built-in multifactor authentication bypass capabilities. These campaigns are highly likely to impersonate trusted, well-known utilities to increase credibility and victim engagement. Moreover, the infrastructure used in the initial stages is often legitimate services, which complicates detection. In AiTM attacks, victims are typically prompted to log in to their Microsoft O365 account to view a document or message. During this process, the attacker intercepts the authentication flow and captures the username, password, and session cookie. Possession of the session cookie allows the attacker to access the service as the user without triggering further authentication.

NORMA Cyber notified **77 companies** in 2025 about compromises in which attackers bypassed MFA security measures.

NORMA Cyber is aware of 60 ransomware attacks in the global maritime sector in 2025. There are certainly dark numbers. The majority of the known incidents were announced on data leak sites, where the threat actors name and shame victims who do not pay. Many also post stolen data on these sites. Ransomware attacks are likely opportunistic, and the number of ransomware incidents is expected to fluctuate from year to year. Although the volume of attacks overall has normalised, the number of named ransomware groups has grown throughout 2025, shifting the ecosystem from a handful of prominent groups with many affiliates to a more diversified landscape with many groups. Affiliates are likely switching between brands as they see fit.

Financially motivated threat actors continue to move faster, decreasing the time from initial compromise to achieving their goals on target. The increase in speed while performing actions on the objective will likely lead to more aggressive attack chains. Early detection is crucial to minimise the impact.

Cybercriminals will highly likely continue to leverage legitimate tools and functions to achieve their goals whilst complicating detection. For instance, remote monitoring and management (RMM) tools are frequently used by threat actors for persistence, to facilitate actions on objectives, and to blend in with the environment. The abuse of such tools is highly likely to continue in 2026. Common ways criminals gain access to RMM solutions include logging into a company's RMM tool with stolen credentials, social engineering users into installing RMM software, and exploiting vulnerabilities in the software itself.

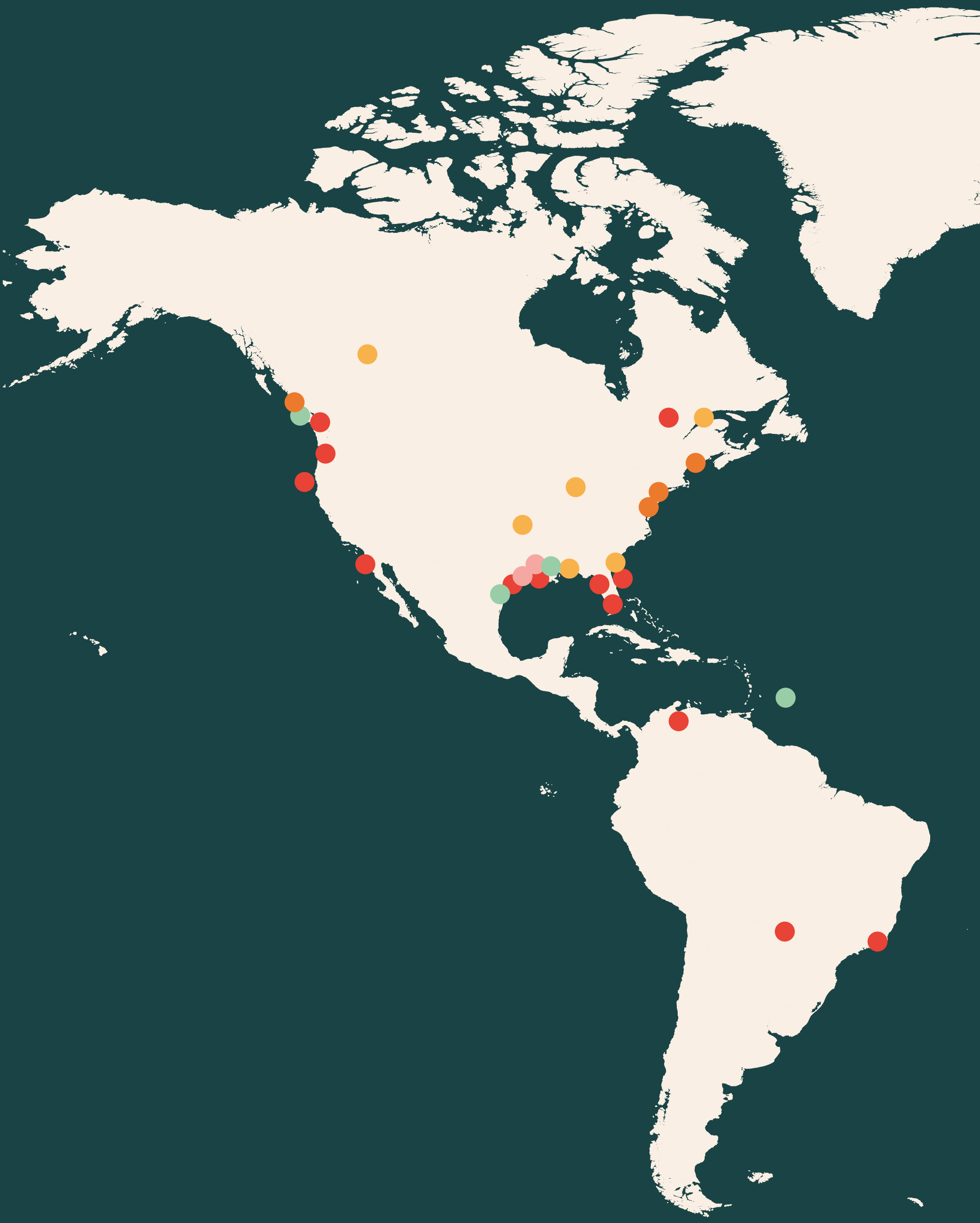
Supply Chain

The maritime ecosystem is complex, with no organisation operating independently of others. Nordic maritime entities face a moderate threat of data exposure, data loss, and operational downtime from attacks on their supply chains. Although an attack may be basic, physical processes are likely to be shut down during incident response for safety reasons, disrupting dependent operations in the process. In 2025, we saw several ransomware attacks on suppliers, during which proprietary and customer data were stolen and published. It is unlikely that the leakage of proprietary data from ship and terminal systems on the dark web poses an immediate threat to maritime systems.

Ransomware Attacks 2025

Other Strains

Babuk - Navarino (Greece)
Bert - S5 Agency World (UK)
Cactus - Contender Boats (USA)
Chaos - Hutchison Ports Duisburg (Germany)
Coinbasecartel - DSV (Danmark)
Devman - China Harbour Engineering Company (China)
Dire Wolf - K Subsea Group (Singapore)
Dragonforce - Grupo Serex (Costa Rica)
Everest - Petrobras (Brazil)
Funksec - Bangladesh Navy (Bangladesh)
Hunters - PetroVietnam Exploration Production Corporation (Vietnam)
Incransom - ASI Group Ltd. (Canada)
Incransom - National Boat Owners Association (USA)
J group - IKAD Engineering (Australia)
Kawa4096 - Tokio Marine Nichido (Japan)
Killsec - Docklyne (USA)
Lynx - Terport (USA)
Lynx - Margaritaville at Sea (USA)
Minteye - Inter-American Tropical Tuna Commission (USA)
Nightspire - Pioneer Ocean Freight Co., Ltd. (Thailand)
Nova - Stark Shipping (Ukraine)
Ransomhub - Jindal Group (India)
Ragroup - SK Gas (Korea)
Rhysida - Furuno USA (USA)
Safepay - Bannenberg & Rowell (UK)
Securotrop - Mill Bay Marine Group (Canada)
Sinobi - Quality Companies (USA)
Team XXX - Narvik Havn (Norway)
Thegentlemen - 2GO Group (Philipphines)
Unknown - NORMA Cyber member (Norway)
Warlock - Ferus Smit (Netherland)
Worldleaks - Nuclebrás Equipamentos Pesados (Brazil)

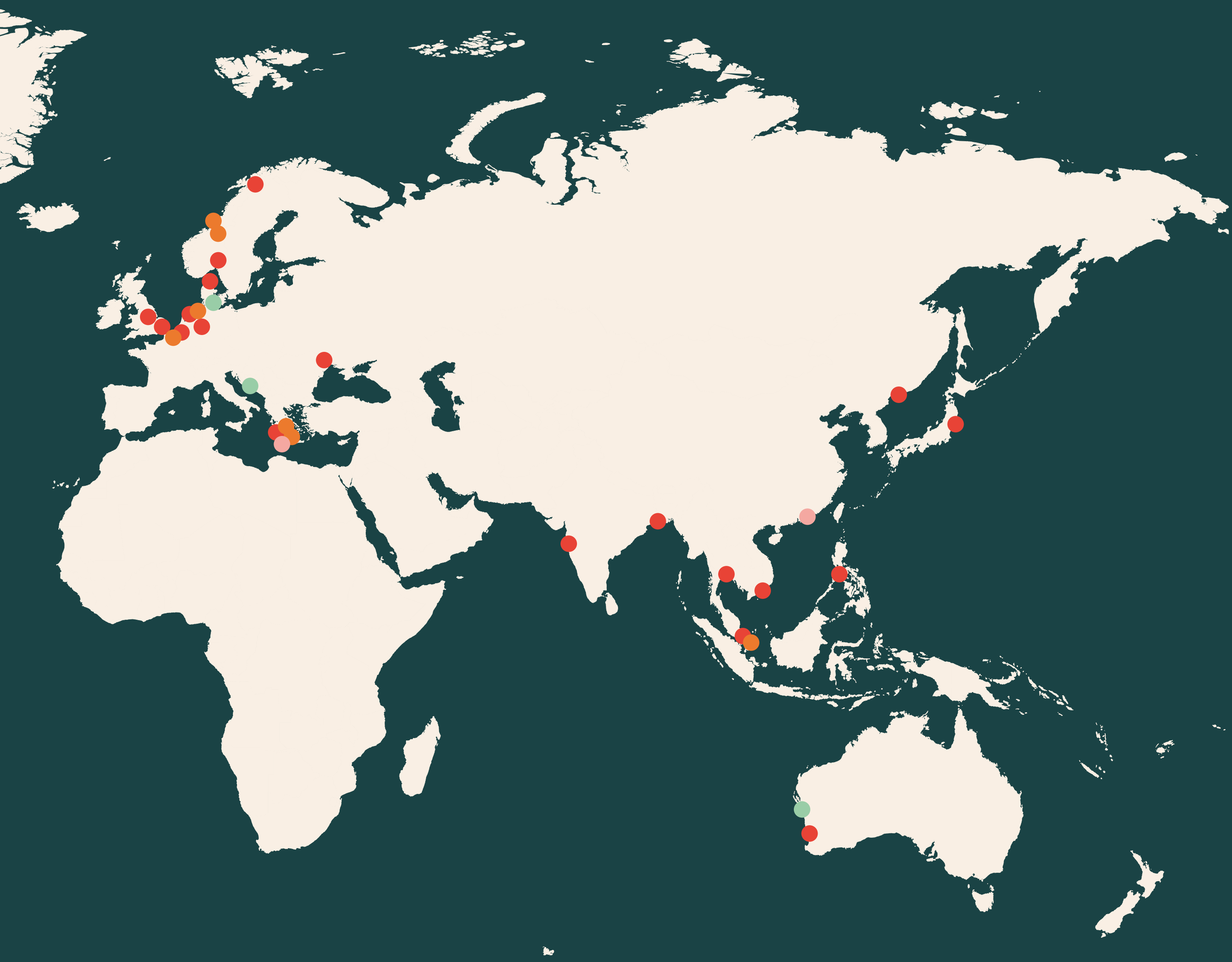


Qilin

Atlantis Submarines (Barbados)
Brodosplit (Croatia)
Buffalo Marine Service, Inc. (USA)
Haeger & Schmidt Logistics (Germany)
Malibu Boats Australia (Australia)
Marine Turbine Technologies (USA)
Montship (Canada)

Clop

Fleet Management Limited (Hong Kong)
Helix ESG (USA)
Kirby Corporation (USA)
Sea Jet (Greece)



Akira

Ab Ovo (Netherland)
Del Corona & Scardigli Canada (Canada)
Extend AS (Norway)
Ghent Dredging (Belgium)
Keystone Shipping (USA)
Møre Maritime AS (Norway)
Multilift Logistic Group (Singapore)
Stratascorp Technologies (USA)
TOP Ships Inc (Greece)
TOP Ships Inc (Greece)
Watermark Marine Systems (USA)

Play

Anchor Industries (USA)
Bluewater Yacht Sales (USA)
Energy Fishing and Rental (USA)
Katch Kan (Canada)
Marine Technical Surveyors (USA)
NEAS (Canada)

Maritime Vulnerabilities

The volume of reported maritime vulnerabilities will likely rise in 2026, but the probability of widespread exploitation remains low. This trend is not necessarily indicative of a rise in insecure systems but reflects a broader shift from security by obscurity to proactive security research, driven by regulatory pressure. The maritime vulnerability landscape will likely become increasingly complex.

It is likely that vendors will contribute to a greater number of published vulnerabilities in 2026. Security research on operational technology is expanding significantly, with more vendors and researchers identifying and responsibly disclosing vulnerabilities. New regulatory requirements, including some specific to the maritime industry, pressure vendors to adopt transparent vulnerability disclosure practices. The importance of managing vulnerabilities through a risk-based approach will highly likely increase, including identifying and prioritising vulnerabilities based on the true risk they represent.

Vulnerabilities in Maritime Operational Technology

In 2025, the number of vulnerabilities (CVEs) assessed to affect maritime operational technology was 1,122, with most categorised as high or critical. This includes equipment certified for use on board vessels. Two of the vulnerabilities were classified as known-exploited vulnerabilities; however, there are no reports of these vulnerabilities being used to target maritime equipment specifically. The number of vulnerabilities affecting maritime equipment will highly likely continue to grow annually as the push for digitalisation continues, alongside maritime vendors implementing new processes for responsible disclosure. However, successful exploitation of vulnerabilities in maritime operational technology remains unlikely.

Other Vulnerabilities and Weaknesses

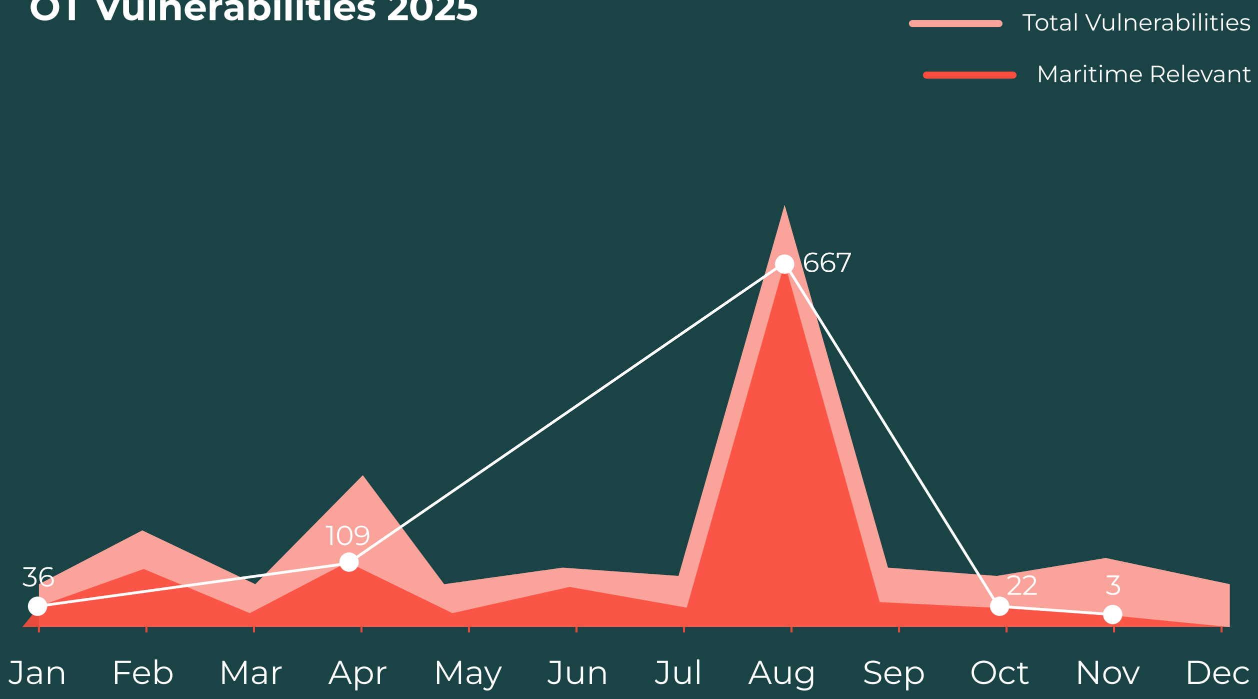
Through conducting penetration tests and security assessments on board various vessels, additional vulnerabilities and weaknesses have been identified which are not publicly disclosed or assigned a CVE. These are typically insecure designs and weak security architectures introduced through retrofits of new technology, which also may inadvertently expose critical systems to increased risk. As cybersecurity in the maritime industry is predominantly compliance-driven, these risks are often introduced when non-critical support systems with few security requirements are integrated with critical systems for data collection to the cloud. Other vulnerabilities are often introduced when temporary solutions become permanent. Examples of this include cellular modems used for remote access, Wi-Fi connectivity in control systems, and the use of unmanaged portable service laptops. These vulnerabilities and weak security architectures reinforce the importance of establishing proactive security programs that go beyond simply regulatory compliance. This trend will likely continue and will impact organisations with less mature security programs.

IT Vulnerabilities with OT Impact

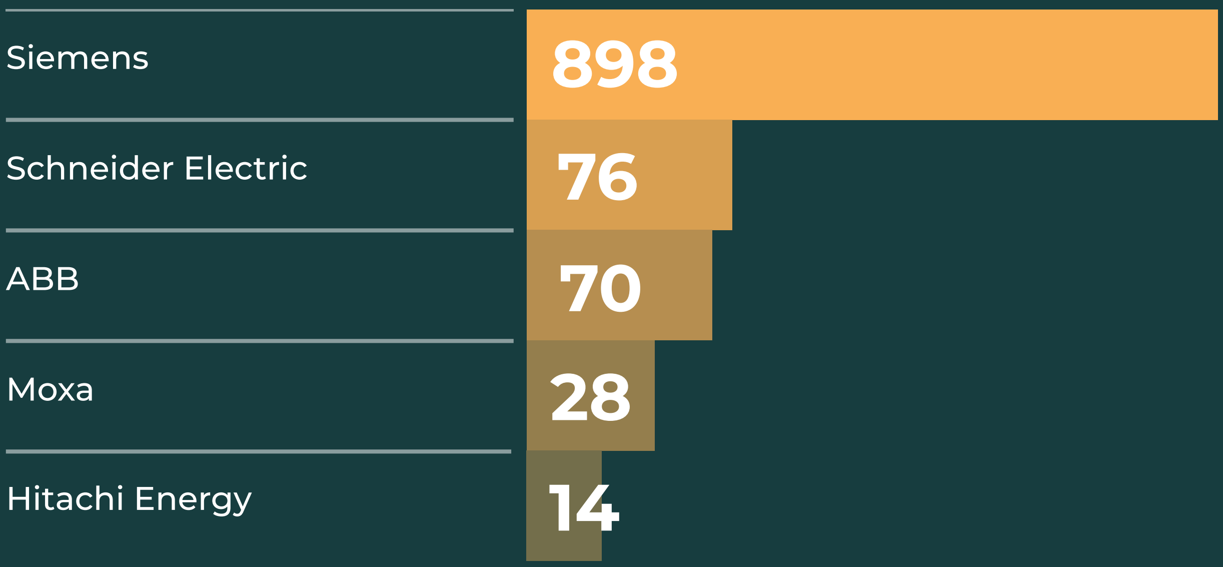
Boundary protection devices tasked with securing IT and OT networks on board vessels are not adequately protected. Throughout 2025, several high-severity vulnerabilities were reported in security appliances, including firewalls, VPN solutions, remote access gateways, and edge servers. Such appliances are essential for forming secure boundaries between various networks, including the boundary between IT and OT networks. A challenge often observed is that multiple vendors install these appliances without clearly defined responsibilities; as a result, they usually lack critical updates. The outcome is that appliances which form the primary barrier between IT and OT often have several critical vulnerabilities, some of which may also have been actively exploited by various threat actors. These vulnerabilities will highly likely continue to represent the most critical vulnerabilities to maritime OT due to the exposure these appliances have towards IT networks, combined with the access provided to OT networks if exploitation is successful.

> In 2025, 53% of Vulnerabilities affecting operational technology were applicable to the maritime sector

OT Vulnerabilities 2025



Top 5 vendors with CVEs



NORMA Cyber currently has more than **170 members**, representing over **3 000 vessels** and offshore units.

About us

The Nordic Maritime Cyber Resilience Centre

NORMA Cyber provides a membership set-up which includes critical cyber security functions and services for maritime organisations. With a non-profit set-up our overall goal is to find synergies and cost-effective solutions, so our members are as secure and resilient as possible. The centre also hosts events where members and partners can come together to share best practice and find common solutions.

Key Milestones 2025

Penetration Testing and OT Security Assessment

NORMA Cyber now fully offers Penetration Testing and OT Security assessment as an additional service to our members.

Intel Reports and Webinars

NORMA Cyber has published 40+ reports and hosted 14 webinars for our members.

Member Portal

NORMA Cyber has developed and launched a new member portal

Spring Conference Oslo

140+ members participated in Oslo, April 2025

Member Council Gothenburg

50+ members participated in Gothenburg, Sept 2025

Membership Services

Threat Intelligence

Timely sharing of intelligence, vulnerability information, and mitigation advise.

Incident and Crisis Response

24/7 stand-by for incidents, and crisis affecting member’s vessel IT, vessel OT and land-based or cloud infrastructure.

External Monitoring

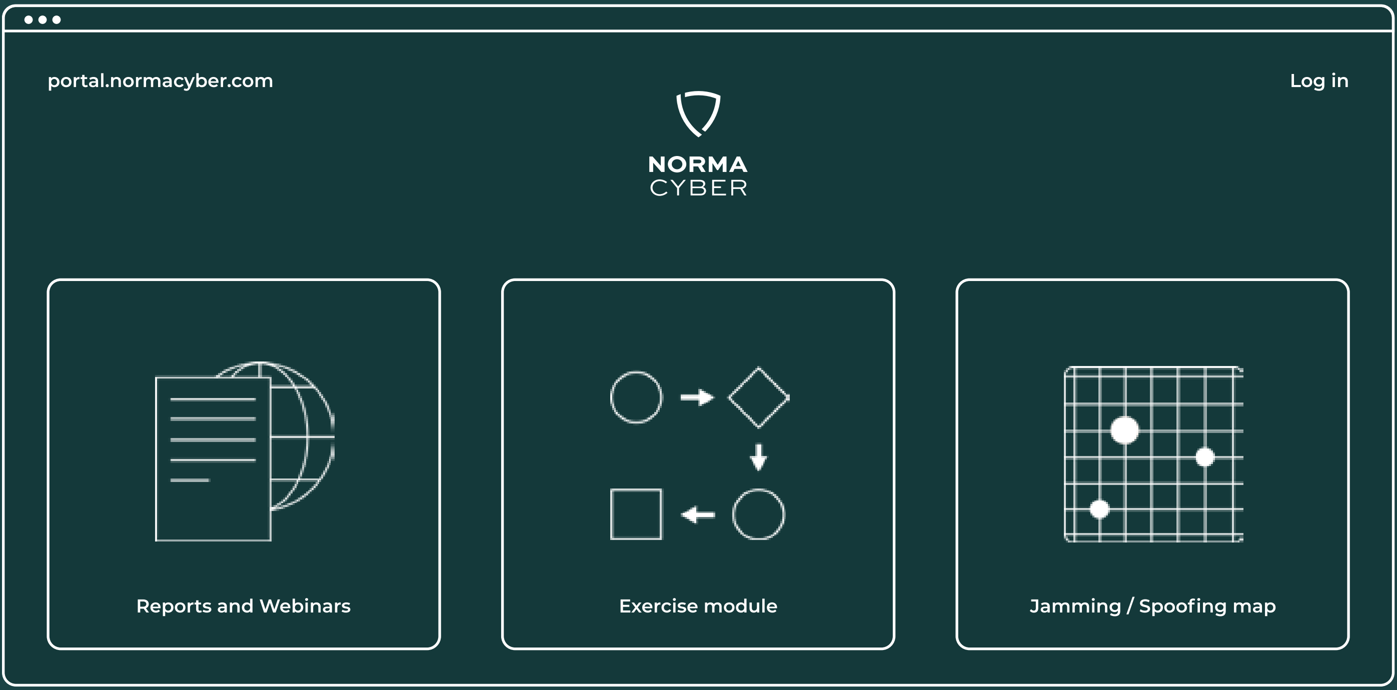
Continuous monitoring of deep and dark web activity and internet-exposed services, with alerts to members when vulnerabilities or exposure are detected.

Network

A collaborative network of members and partners for knowledge sharing, innovation, and learning through events And the NORMA Cyber Member Council.

For full overview of services, please visit normacyber.no/services

NORMA Cyber Member Portal



All members get exclusive access to our member portal, at portal.normacyber.no

Threat Intelligence

- Monthly Threat Assessment
- Intelligence reports
- Maritime OT Vulnerability notifications
- Indicators of compromise information sharing (MISP)

Incident and Crisis Response

- 24/7, 365 incident and crisis support
- Vessel IT / OT
- Landbased & cloud infrastructure
- Technical and resource management support
- Cyber security exercises

External Monitoring

- Deep / Dark web monitoring
- Vulnerability scan of internet exposed services
- Attack Surface Management
- Alerting members in case of compromise

Network

- Member council and conference
- Member and partner network
- Knowledge sharing through dedicated forums

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 with most maritime and corporate systems. Typically, no hardware installation is required, and there are no dependencies on specific firewall, EDR, or switch vendors.

Neutral Party: we provide an objective view of your environment and include monthly recommendations to strengthen your security posture.

Competence: we understand the maritime domain and its operational and technical complexities.

Synergies: the knowledge we gain from monitoring maritime companies gives us a unique insight and anonymised content is shared back to our members.

Technical Set-up

- Flexible set-up: scope can cover vessel IT, vessel OT, corporate IT, and/or cloud
- environments.
- Modern SOC platform utilising AI to reduce noise and false positives.
- High degree of automation to shorten detection-to-reporting time and reduce latency.
- Expert-led investigation, response, and follow-up for complex cases.
- Optional automated response for IT/cloud environments via our SOAR capabilities.
- Proactive threat hunting to uncover hidden, advanced, or long-dwell 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 organisations 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

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

RoRo	52%
Offshore support/ Construcion	13%
Bulk Carrier	10%
LPG Tanker	7%
FSRU	5%

NORMA
CYBER

Penetration Testing and OT Security Assessment

NORMA Cyber now offers Penetration Testing and OT Security Assessments as an additional service to our members.

NORMA Cyber customises security testing for vessel technology. A penetration testing engagement tailored for vessels and maritime organisations seeking to assess the cybersecurity posture of their onboard IT infrastructure.

The goal is to simulate realistic attack scenarios, identify vulnerabilities, and evaluate internal network controls — with a focus on the separation between Information Technology (IT) and Operational Technology (OT) networks.

Through an OT Security Assessment, the NORMA Cyber team will aim to identify all Operational Technology onboard. By going onboard to conduct physical inspections we get hands-on experience which is combined with detailed review of ship documentation.

In this service, NORMA utilise both maritime and technical knowledge to provide an up-to-date status of the vessels systems, with potential weaknesses and vulnerabilities.

	Vessel IT Penetration Testing	**Vessel OT Security Assessment**
Purpose	Identify and validate exploitable vulnerabilities across the vessel's IT infrastructure.	Evaluate the security posture and resilience of onboard Operational Technology (OT) systems.
Scope	**Testing Areas:** • Network and wireless testing • Credential and access testing • System and device onteraction • Social engineering (optional) **Three different attack ccenarios to simulate level of attacker:** 1. Guest network access (unauthenticated attacker) 2. IT network access (no credentials) 3. IT network access (with domain user credentials) Key focus: IT/OT network segmentation and boundary integrity.	**Key Objectives:** • Identify open connection between IT and OT • Identify undocumented/Rogue devices etc. • Prioritize systems with higher relevance to Cyber Security **Identify:** • Critical systems • Dependencies between systems and key components • Weaknesses and vulnerabilities in system architecture • Deviations from documentation
Time	Two consultants two days onboard vessel	Two consultants two days onboard vessel

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

Share Information and Incidents

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 we are 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

Need Assistance?

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.

GNSS Jamming / Spoofing

Send an email to **ops@normacyber.no**

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. NORMA Cyber can assist members in reporting to the relevant authorities

In case of immediate assistance or an emergency call our emergency number: **+47 90 98 97 37**

Building unified resilience against cyber threats for the Nordic Maritime Sector