NORMA CYBER

The Nordic Maritime Cyber Resilience Centre

Annual Threat **Assessment**

2024

The Nordic Maritime Cyber Resilience Centre - NORMA Cyber – is the leading hub for operational cyber security efforts within the Nordic maritime sector. From 2024 NORMA Cyber has changed its name to reflect the expansion of the center's member base. The centre has been operating since 2021 and is a joint effort between The Norwegian Shipowners' Mutual War Risks Insurance Association (DNK) and the Norwegian Shipowners' Association.

NORMA Cyber operates as a non-profit, and the members are organisations within the maritime sector. From April 2024 NORMA Cyber has expanded to the Nordic countries and will also offer affiliate and vendor membership to international organisations.

NORMA Cyber currently has 115 members and represents more than 2 500 vessels and offshore units.

The centre delivers a centralised cyber security function for its members, including intelligence, security operations and crisis response.

From 2024 NORMA Cyber was chosen to support the Norwegian Coastal Administration in their mission to establish a sectorial response function for cyber security within the Norwegian maritime sector.

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 mutual members within complex operations where 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 the third edition of the NORMA Cyber Annual Threat Assessment.

Cybersecurity continues to rise in importance and relevance among our stakeholders. The technological development within the maritime industry is moving fast. The supply chains grow in complexity and there is an increased demand for live data from critical system. Along with these developments comes an increased attack surface and the threat actors are adapting. It is therefore critical for success to approach cyber security through timely information and structured analysis.

NORMA Cyber concentrates on building competence and developing solutions paired with a diligent focus on information sharing and intelligence. We continue to develop our member services and partnerships, including government agencies. A new development from 2024 is that the Norwegian Coastal Administration has chosen NORMA Cyber as their partner in the sectorial response to cyber security within the maritime sector.

This threat assessment is based on data from multiple sources, including NORMA Cyber members, to give you a reliable forecast for maritime cyber threats in the coming year.

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

Lars Benjamin Vold
Managing Director

Norwegian Maritime Cyber Resilience Centre

Managing Director Lars Benjamin Vold
Norwegian Maritime Cyber Resilience Centre

Summary

01 State Actors

Nation state linked threat actors remain a persistent and evolving threat to the maritime sector, with Russia and China-linked actors as the most prominent threats. With extensive resources at their disposal, their operations encompass espionage, theft of intellectual property, and disruption of infrastructure to meet national strategic goals. In 2024, maritime entities, especially those involved in energy, critical subsea infrastructure projects, logistics and transportation, will be likely targets of Russia-linked cyber espionage operations. China-linked threat actors are likely to target maritime entities in naval engineering, subsea technology, and those tied to critical infrastructure projects or government collaborations in geopolitically sensitive areas.

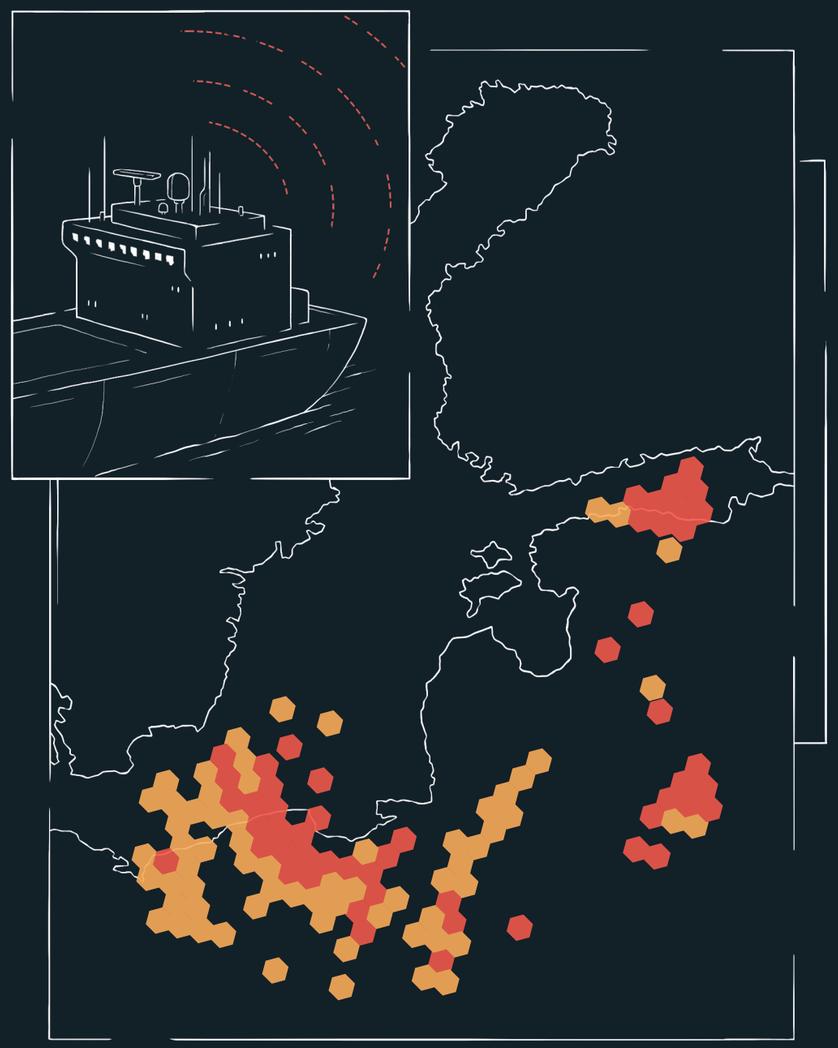
02 Cybercrime

The risk of digital theft, fraud, and ransomware campaigns targeting the maritime sector remains high and is expected to continue through 2024. Maritime organisations will persistently face threats from economically motivated actors, with the threat actors' approach likely remaining opportunistic. The malicious use of AI will threaten maritime organisations due to its ability to create persuasive fake communications, facilitating fraud attempts. Moreover, ransomware threat actors are likely to increasingly target edge devices.

03 Hacktivism

Hacktivist groups will highly likely target maritime organisations who operate in, or have ties to, states or areas with geopolitical tensions in 2024. Conflict developments will likely drive reactions from hacktivist groups of various skills, focusing on disruptive attacks and information operations. Hacktivists will likely continue to favour basic attack methods that do not require the attacker to be particularly technically apt. Hacktivist initiated Distributed Denial-of-Service attacks will likely have an economic impact on maritime organisations due to operational downtime of services in 2024.

01 State Actors



GNSS interference in Baltic Sea on January 13th.

GNSS interference

GNSS interference, including jamming and spoofing of AIS or GPS signals continue to pose challenges to maritime safety, security, and the enforcement of laws at sea during regional conflicts. In 2023 such activity was reported to occur in the Black Sea, the eastern Mediterranean, the Red Sea, the Arabian Gulf / Persian Gulf and in the South China Sea. These are areas with ongoing conflicts or geopolitical tension. It is highly likely that this activity will continue in 2024.

Spoofing and jamming
Automatic Identification System (AIS) is a safety system used by vessels and vessel traffic services (VTS). AIS spoofing refers to manipulation of AIS data, such as vessel's identity, type, position, course, speed, navigational status, and other safety-related information. AIS spoofing can be used to conceal illicit activity, creating ghost ships and to evade detection. In 2023 AIS spoofing was reported in the Mediterranean and in the Arabian Gulf / Persian Gulf. It is likely that this activity will continue in 2024. AIS spoofing poses significant challenges to maritime safety, security, and the enforcement of laws at sea. It undermines the reliability of AIS data, which is crucial for collision avoidance, traffic management, and security monitoring. GPS spoofing refers to the generation of false signals to deceive GPS receivers, making the receivers provide inaccurate location information.

Baltic Sea
After Sweden and Finland joined NATO there has been an increase in GNSS interference in the Baltic Sea region. GPS jamming has been reported in the Gulf of Finland, likely from the Russian island Gogland / Hogland (Suursaari in Finish).

The Russian Baltic Fleet operating out of Kaliningrad have conducted large Electronic Warfare (EW) exercises which have resulted in GNSS interference in southern part of the Baltic Sea and Sweden. It is likely that this activity will continue in 2024 and that the GNSS interference inadvertently may impact merchant vessels. Russia has previously conducted GPS jamming close to NATO exercises. In 2024 the exercise Steadfast Defender will be NATO's largest exercise in decades. This exercise takes place from February to May in central and northern Europe. Norway will host exercise Nordic Response 2024, which is an expansion of the Cold Response exercise taking place every second year in Northern Norway. Following the expansion of NATO with Finland and Sweden, Cold Response has been expanded to a Nordic Response, and will take place in March 2024. Russia has used GPS jamming as "signalling" towards military units; however, this activity can inadvertently impact merchant vessels. It is likely that GNSS interference will be experienced in conjunction with these exercises which will take place in the Norwegian Sea, the North Sea and the Baltic Sea.

GNSS interference 2023

Areas with an increased threat of GNSS interference in 2024. Most of the reported incidents in 2023 occurred in the same areas

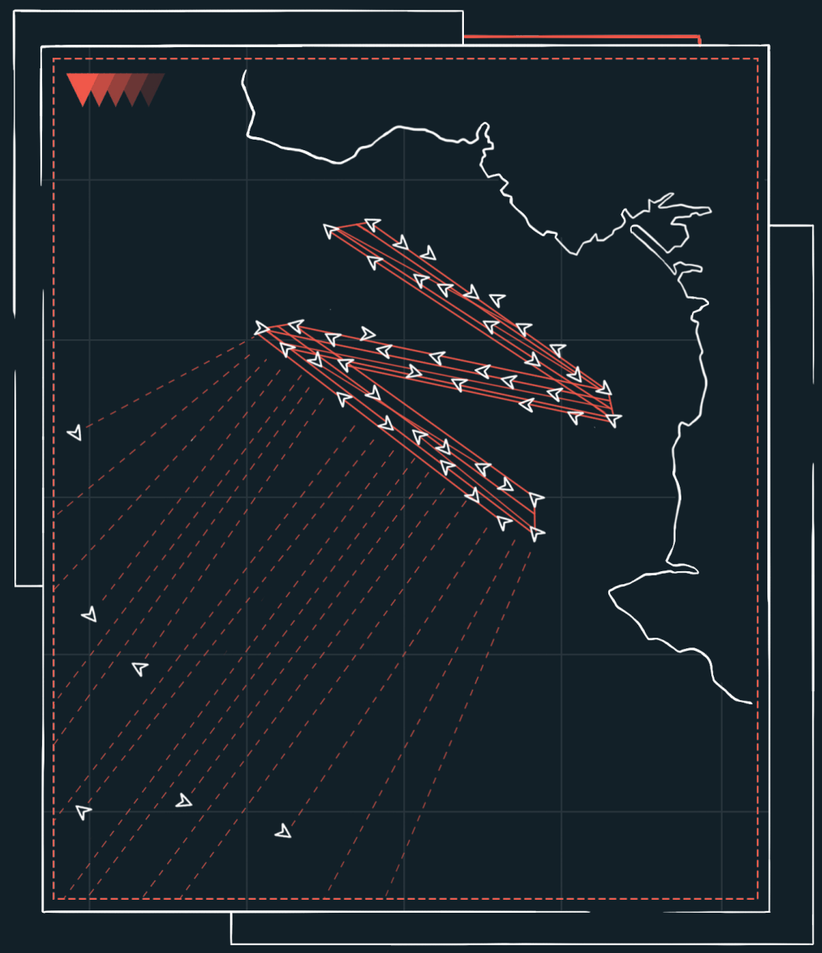
NORMA Cyber | Annual Threat Assessment 2024

Black Sea
In May 2023 media reported that the AIS positions from several commercial vessels at the Constanta anchorage outside Romania in the Black Sea were spoofed to project the impression of a 65 km long Russian pro-war “Z” symbol outside Crimea. The AIS spoofing was likely conducted by Pro-Russian actors as an information operation, potentially to bolster Russian morale ahead of an anticipated Ukrainian counter offensive.

The main base for the Russian Black Sea fleet in located in Sevastopol and is supported by major Electronic Warfare capabilities. Russia will likely use GPS jamming to protect the naval base from Ukrainian drone attacks. This jamming will likely inadvertently impact merchant vessels in the north-western part of the Black Sea as long as the war between Russia and Ukraine continues.

Red Sea and Arabian Gulf / Persian Gulf
After the terror attack by Hamas against Israel 7 October 2023, the ongoing armed conflict between Israel and Palestinian led militant groups, has also resulted in GNSS interference in the eastern Mediterranean, in the northern part of the Red Sea and in the Bab al-Mandab Strait.
As part of the ongoing conflict in the Middle East, where the Houthis have conducted kinetic attacks against merchant vessels in the Strait of Bab al-Mandab, there has been reports of GPS spoofing in the same area. The signal has likely originated from a location on the border between Saudi Arabia and Yemen. This indicates that the Houthis have attacked merchant vessels in the Strait of Bab al-Mandab with missiles and drones in support of Hamas. There has been reports of GPS spoofing in the Bab al-Mandab Strait where the signal has likely been originated from a location on the border between Saudi Arabia and Yemen, indicating that the Houthis likely have Electronic Warfare capabilities. It is likely that merchant vessels sailing through the Bab al-Mandab strait in 2024 will experience GPS spoofing or jamming.

GNSS interference, including jamming and spoofing of AIS or GPS signals continue to pose (significant) challenges to maritime safety, security, and the enforcement of laws at sea during regional conflicts. Last year such activity was reported in the Black Sea, eastern Mediterranean, Red Sea, Arabian Gulf / Persian Gulf and in the South China Sea. It is likely that this activity will continue in 2024.



Spoofed AIS data projecting the Russian pro-war “Z” symbol outside Crimea in the Black Sea.

The intelligence threat from Russia to maritime organisations in the Nordics

The Nordic countries are facing a more serious threat environment now than they have in decades. With Sweden and Finland as new NATO members the geopolitical situation in the region has changed. Russian intelligence services will seek information about politics, energy, the High North, the Baltic Sea, allied activities, and defence. Maritime entities involved in energy, critical subsea infrastructure projects, logistics and transportation, will be likely targets of Russia-linked cyber espionage operations.

Military positioning in High North and the Baltic Sea

Following the attack on Ukraine, the Northern and Baltic Fleets have become more important to demonstrate Russia's naval power in the north, as well as in the Atlantic and the Baltic Sea region. Russia's display of forces during the naval exercise Ocean Shield, which took place in the autumn of 2023 in the Barents Sea, the North Sea, and the Baltic Sea, confirms that Russia views the High North and the Baltic Sea region as one continuous area.

Maritime entities will play a key role in allied reinforcement and re-supply, with chemical and product tankers capable of transporting fuel, as well as Roll-on Roll-off (RoRo) vessels capable of transporting vehicles, supplies, and personnel.

The logistics and transportation sectors also remain a critical component in delivering foreign military aid to Ukraine, which Moscow strongly opposes and views as a key hinderance to its military objectives in the region. Poland has experienced disruptive cyber-attacks on the country's railway network and Polish government have reported that Russian Intelligence Services have paid individuals in Poland to hide tracking devices in military cargo, place cameras along railways, and identify Polish seaports.

It is likely that Russia-linked threat actors will conduct cyber operations as a means to collect intelligence on maritime entities. Especially entities involved in logistics and transportation of humanitarian or military equipment to Ukraine will be vulnerable for at least the duration of the war.

Vulnerable petroleum and Internet infrastructure
Norway is a key supplier of gas to Europe. A significant share of the gas consumed in Germany, UK, Belgium, and France comes from Norway. The gas comes from Norwegian gas fields that are connected to receiving countries in Europe through a vast pipeline network. Norwegian-affiliated vessels account for a significant share of the world's total capacity both within transportation of LNG and re-gasification (FSRU). These vessels constitute a strategic capacity to secure Europe's energy supply. Damage to the Norwegian petroleum infrastructure would harm both Norway and the receiving countries in Europe. This makes the energy infrastructure a desirable target for threat actors wanting to hamper European energy supply chains. The energy infrastructure could be subject to accidents, physical sabotage and destructive cyberattacks.

Recent examples of incidents include the attacks against the Nord Stream pipelines in 2022 and the Balticconnector pipeline between Finland and Estonia in October 2023. Sweden and Denmark closed the Nord Stream investigation in February without publicly attributing the attack. The Balcticconnector pipeline was damaged by an anchor dropped from the Hong Kong-flagged vessel NewNew Polar Bear.

This also impacted two subsea telecom cables. Whether these were accidents or deliberate acts of sabotage will probably never be uncovered.

Russia has demonstrated its will and ability to use destructive cyber operations to harm critical infrastructure in situations of conflict. Both before and during the war in Ukraine, Russia has attacked telecom and industrial control systems.

Russia has been mapping Norwegian critical oil and gas infrastructure for years. This mapping is likely still ongoing, both physically and in the cyber domain. Russia employs a high number of civilian ships for intelligence operations, but it is likely that maritime entities involved in projects related to critical subsea infrastructure will be targets for Russian cyber espionage operations.

Norwegian-affiliated vessels are number two in the world in the offshore / subsea segment, with more than 500 highly specialised vessels. In addition to being involved in critical subsea projects, these vessels also operate world leading subsea technology, making the attractive intelligence targets both for Russia and China.

Forest Blizzard

Forest Blizzard (also called Fancy Bear or APT28) is linked to the Russian Military Intelligence Service (GRU). It is one of the threat actors specifically targeting the energy, logistics and transportation sector in cyber espionage operations.

Forest Blizzard conducts extensive network reconnaissance activity, using port-scanning, brute force or password spraying activity to identify vulnerabilities or obtain credentials for further cyber operations.

Forest Blizzard has also used spear phishing emails with malicious attachments, exploiting vulnerabilities in Microsoft or other office application to target entities in the energy sector.

It is likely that Forest Blizzard will continue their activities in 2024 and it is likely that maritime entities in the energy sector will be considered targets for this threat actor.

The espionage threat from Russia is high. Maritime entities involved in energy, critical subsea infrastructure projects, logistics and transportation, will be likely targets of Russia-linked cyber espionage operations.

The war between Israel and Hamas: the Red Sea Crisis

The Hamas terrorist attack against Israel 7 October 2023, and the subsequent war between Israel and Hamas shows that the underlying conflicts in the Middle East persist. The intensive fighting has thus far been confined to the Gaza Strip, however the conflict has spilled over to other areas and affected maritime organisations with kinetic attacks, GNSS interference and cyber-attacks in the Red Sea. Cyber attacks against maritime organisations perceived to support Israel will likely continue in 2024 and GNSS interference will likely persist in the Red Sea.

The Red Sea crisis – kinetic attacks and GNSS interference

Following the outbreak of war, the Red Sea crisis started on 19 October 2023 when the Houthis insurgents in Yemen launched missiles against Israel and started attacking merchant vessels off the coast of Yemen in the Red Sea. The Houthis have attacked merchant vessels with Anti-Ship Missiles (ASM) and Unmanned Aerial vehicle (UAV) as a stated support to Hamas and the Palestinian people.

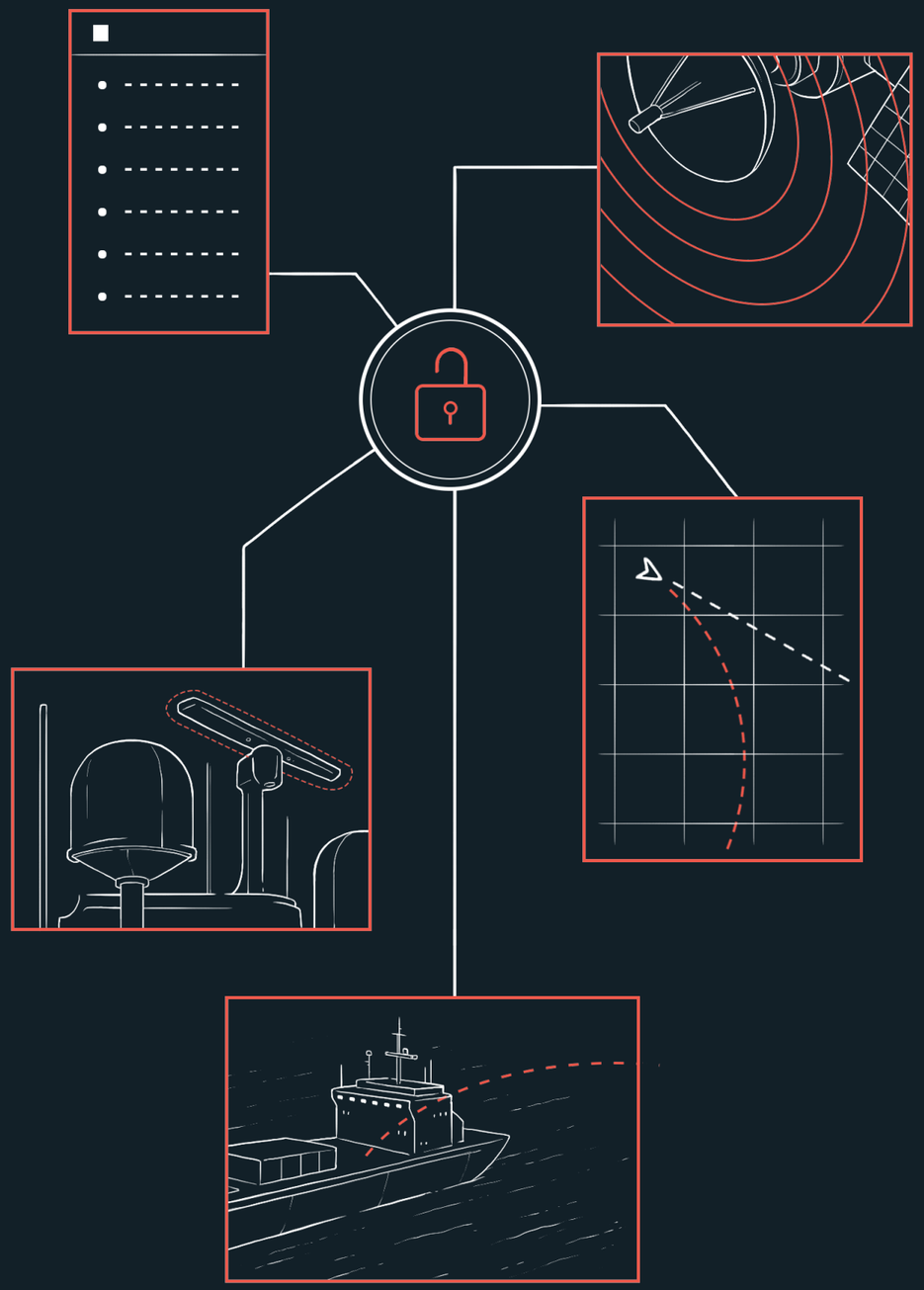
More than 10 merchant vessels have been hit in and around the Strait of Bab al-Mandab, a chokepoint of the global economy, as it serves as the southern maritime gateway to the Suez Canal, and to the Gulf of Aden.

Electronic warfare plays a key role in countering missile and drone attacks, and it is highly likely that Western naval forces operating in the Red Sea to protect merchant shipping operations have jammed or spoofed GPS signals to disrupt missile or drone attacks. GNSS interference has been reported outside the port of Jizan, where vessels have had their position spoofed to a location on the border between Saudi Arabia and Yemen. It is likely that this GNSS interference will continue as long as the conflict persists.

The Red Sea crisis in the cyber domain

The Red Sea crisis is a part of a broader proxy war between the United States and Iran, both in the cyber and physical domain.

The Houthis have primarily targeted vessels affiliated with Israel, the US, and the UK. It is likely that the Houthi, or someone assisting them, have used online vessel tracking services and lists of port calls to identify potential targets for missile or UAV attacks. Vessel tracking services, such as Marine Traffic, provide information about vessel management structure, including beneficial owner, commercial manager, and technical manager.



According to open sources, members of Iran's Islamic Revolutionary Guard Corps (IRGC) have been operating on the ground in Yemen, and it is likely that they have provided tactical intelligence to the Houthis. Iran-linked threat actors have previously deployed malware specifically designed to capture usernames and passwords from SATCOM and vessel tracking services.

In January 2024 the Iran-linked Internet persona YareGomnam claimed to have taken down the TankerTrackers online service, that tracks and report shipment of crude oil, in what was reported as a DDoS attack. The DDoS attack was reportedly timed to coincide with a simultaneous kinetic attack by the Houthis against the Marshall Island-flagged, US-owned, Greek-operated tanker MV CHEM RANGER.

Albeit seemingly unsuccessful, if the information is correct, this was the first example of coordination between targeting of maritime targets in the cyber and physical domain.
Coordinated attacks where cyber capabilities are applied to stage kinetic attacks or amplify the effect of kinetic attacks is likely part of a developing trend in the conflict. The use of cyber capabilities will likely increase in frequency in 2024 depending on the developments in the conflict between Hamas, and Israel and the spillover effects in the Red Sea involving the Houthis. Iran-linked cyber capabilities both state-sponsored hacktivists and other likely pose a potential escalating factor depending on the developments in the Middle East region.

As long as the Red Sea Crisis persists maritime organisations affiliated with Israel, the US, and the UK will likely continue to be targets in Houthi ASM and UAV attacks. Similarly, maritime organisations affiliated with Israel, the US, and the UK will likely be targets in cyber operations. Furthermore, it is likely that there will be an increase in coordinated attacks in the physical and cyber domains given that the situation continues to deteriorate between the parties.

Regional Conflicts

China

China-linked threat actors conduct operations that reflect the Chinese Communist Party's pursuit of global influence. These threat actors continue to carry out sophisticated worldwide campaigns targeting a wide range of sectors, including the maritime sector and nations in the South- and East China Sea. China-linked activity also indicate likely pre-positioning in critical infrastructure in the event of a future geopolitical crisis.

Over the past decade, China-linked cyber operations have matured into a stealthier and more coordinated threat. Chinas cyber capabilities, especially those driven by the Ministry of State Security (MSS) and the People Liberation Army (PLA), represent a significant threat to the maritime sector focusing on espionage, intellectual property theft, and potentially disruptive operations against critical infrastructure.

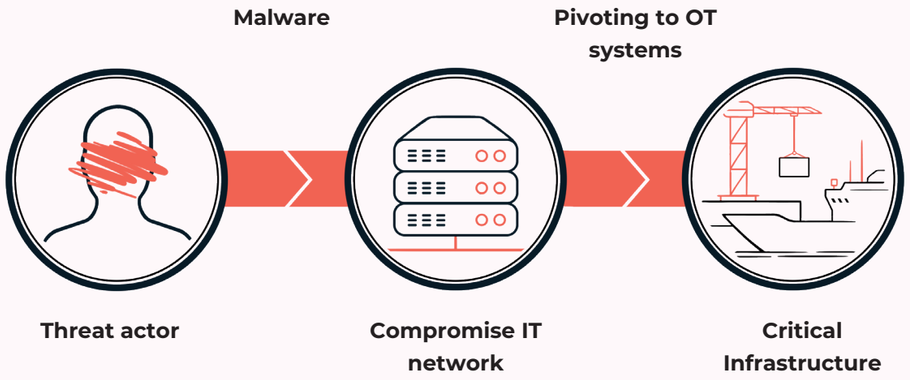
Pre-positioning in critical infrastructure

Mid 2023, government and industry reported that a China-linked threat actor targeted organisations related to critical infrastructure in the transportation, water utility, and energy sectors in the US and the Western Pacific (Guam). The activity likely has a dual purpose, espionage to collect information about organisations involved in critical projects, and prepositioning in critical infrastructure. The latter involves acquiring and maintaining persistent access to potentially execute disruptive or destructive cyber activity when needed. The cyber security industry tracks this activity as Volt Typhoon.

The threat actor has over time built a covert botnet consisting of compromised Small Office and Home Office (SOHO) devices to carry out covert operations in near proximity of end targets. Volt Typhoon gains access to targeted networks by exploiting internet facing appliances, favouring remote access solutions. In certain cases, the precise way these appliances were exploited is unclear, suggesting the actor likely obtain currently unidentified zero-day exploits. After initial access the threat actor lives of the land to acquire administrative privileges and focuses on gaining capabilities to access operational technology (OT) assets, before going dormant.

US government organisations conducted a court-authorized takedown of parts of the botnet, resulting in a swift and intensive comeback by the threat actor to regain access. The takedown reportedly was effective, but it is likely that the takedown had limited effect and will only delay Volt Typhoon operations.

Microsoft has tracked Volt Typhoon targeting of critical infrastructure since 2021. Several of these attacks include targets that do not have obvious intelligence collection benefits. These campaigns likely intended to provide China with the capability to disrupt critical infrastructure or communication between the US and Asia during a future geopolitical crisis.



China-linked threat actors' disruptive capabilities are largely uncertain due to the current lack of destructive attacks attributed to China. However, evidence of research related to electrical power infrastructure and pre-positioning in critical infrastructure indicate a heightened focus on the matter. With the current tension in Taiwan territorial waters and in the East- and South China Sea it is likely that China-linked threat actors will continue to develop contingency access to enhance readiness in handling an escalating situation. It is likely that this targeting includes the maritime sector given the strategic importance of the South China sea as a whole in a future conflict.

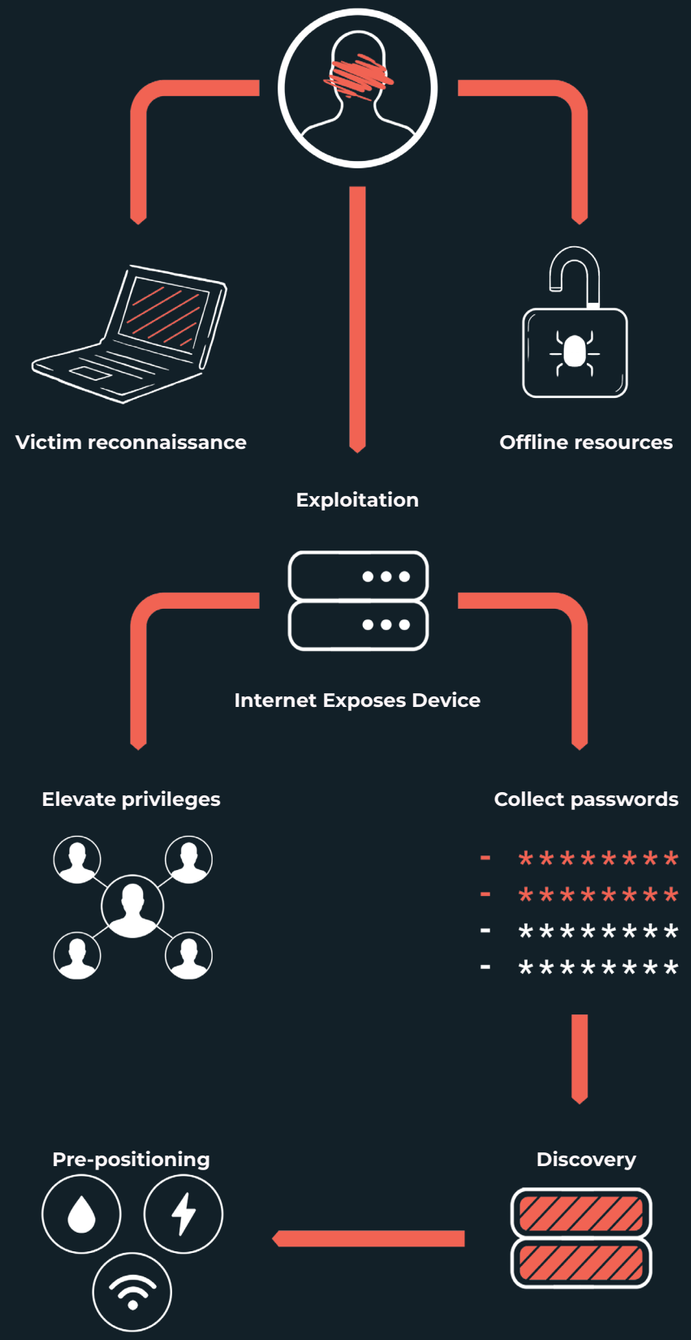
Chinas hegemony in the East- and South China Sea

China-linked threat actors have on several occasions targeted entities to gain insight into ongoing conflicts or tension near their boarders, this activity also affects the maritime sector and will highly likely continue the coming year. Targeted phishing campaigns with a maritime related theme have been used on several occasions. An example of this was in late 2023, when phishing documents crafted by a China-linked threat actor using a maritime theme was used as initial attack vector, to target organisations handling the tension between China and the Philippines.

The document was crafted around the Philippine's proposal to conduct joint patrols in the South China Sea. Simultaneously, there were reports that a China-linked threat actor known as Stately Taurus compromised entities in Philippines's, with espionage intension.

The timing of these campaigns coincides with a period of heightened tension between China and the Philippines, which escalated a few weeks prior. This period was marked by a sequence of confrontational incidents, including a notable standoff at the Second Thomas Shoal. The situation further intensified with the Philippines enhancing its military collaboration with the United States and Australia, coupled with a noticeable reduction in direct communication with China.

These operations likely intend to give Chinese government a deeper understanding of the strategies and response to the maritime dynamic between China and the Philippines. Albeit not a direct target, the maritime sector, particularly organisations with close ties, or cooperation with governmental entities, could likely be collateral targets during cyber operations in geopolitical tense areas.



Due to continuous Chinese claims about territorial power of Taiwan, intelligence collection targeting anything Taiwan related will highly likely remain a long-term intelligence objective for China-linked threat actors. Amidst the heightened political tension of Taiwan's presidential election, a China-linked threat actor compromised a Taiwanese local government entity. This activity coincided with the election where Lai Ching-te, from the Democratic Progressive Party (DPP) advocating for strong ties with Washington, emerged victorious. Beforehand, statements of this outcome from China indicated that a DPP victory could disrupt the peace across the Taiwan Strait.

Taiwanese related maritime organisations have also been targeted with phishing documents addressing information from the "Ocean Bureau of Kaohsiung City (Taiwan)". The targeting of Taiwanese maritime entities supports multiple intelligence requirements, including but not limited to fishery competition, maritime conflict, and merchant shipping. Targeting of maritime interests will likely also include merchant shipping related to China's Maritime Silk Road, a component of the Belt and Road Initiative.

The espionage threat from China-linked threat actors targeting the maritime sector is high. Particularly organisations involved in naval engineering, shipbuilding, subsea technology, and organisations involved in projects related to critical infrastructure or close cooperation with government entities in geopolitical sensitive regions, are likely targets for China-linked threat actors. Organisations involved in mapping or extraction of natural resources, including supply-chain involvement are also likely intelligence targets.

02 Cybercrime

Initial Access

The threat against maritime organisations from economically motivated threat actors will persist in 2024. These threat actors will highly likely strive to innovate their malware strategies and diversifying their delivery methods. The targeting will likely continue to be opportunistic.

Initial access brokers, criminal threat actors specialising in gaining access to companies, will be a prevalent threat to maritime organisations globally in 2024. Access brokers are expected to enable breaches into maritime organisations utilising a combination of standard and customised tools.

The following methods and capabilities will highly likely be key threats against maritime organisations in 2024:

In 2024, threat actors will likely continue to log into business resources using valid credentials. Popular means of obtaining such identities are phishing, using information stealers, and exploiting self-service password-reset portals. Credentials to cloud resources are expected to grow in popularity.

Credentials to corporate Google accounts, AWS, and Entra IDs will highly likely be at the top of threat actors' target lists, as these credentials have the potential to be identity providers for multiple platforms. Commodity malware targeting these credentials poses a threat to shipowners, particularly those who allow employees to sign into their accounts on private or unmonitored devices. Defenders rely on sufficient visibility to detect and mitigate malware threats before the breach is a fact. Threat actors who have stolen legitimate credentials to resources will likely attempt to blend into the compromised environment and can be challenging to detect.

The use of information stealers will likely increase in 2024. An information stealer is a malware designed to covertly gather sensitive information, such as usernames, passwords, and other authentication tokens stored in web browsers. There has been a gradual increase in the distribution of these malware types and their sophistication. While dumping passwords stored in browsers is trivial, prominent stealers contain functionalities that allow them to hijack sessions and exploit vulnerabilities at scale.

NORMA Cyber's deep and dark web monitoring efforts have identified several instances where credentials to access member services are being sold on criminal marketplaces. The intelligence suggests these credentials often come from the personal devices of employees. The information extracted from these devices is typically sold as complete logs, with prices ranging from £3 to £15. While there is significant activity on public forums, it's important to note that more established cybercriminals tend to conduct transactions privately, especially when dealing with high-value access credentials obtained from well-regarded threat actors. This means that valuable and validated access to maritime entities is unlikely to be publicised openly and thus hard to detect by external monitoring.

In 2023, the NORMA Security Operations Centre (SOC) detected and mitigated a large number of compromised accounts where the threat actor had access to valid credentials. The SOC has also observed threat actors utilising compromised accounts to conduct business email compromise (BEC) fraud by sending fraudulent emails to the compromised accounts' contacts, requesting financial transactions, or sending sensitive information disguised as legitimate business requests.

Furthermore, the SOC also handled a significant incident involving an initial access broker affiliated with ransomware groups. The threat actor was removed from the network before the access was listed for sale, and without a timely response, the access broker could have taken serious post-exploitation actions.

Artificial Intelligence

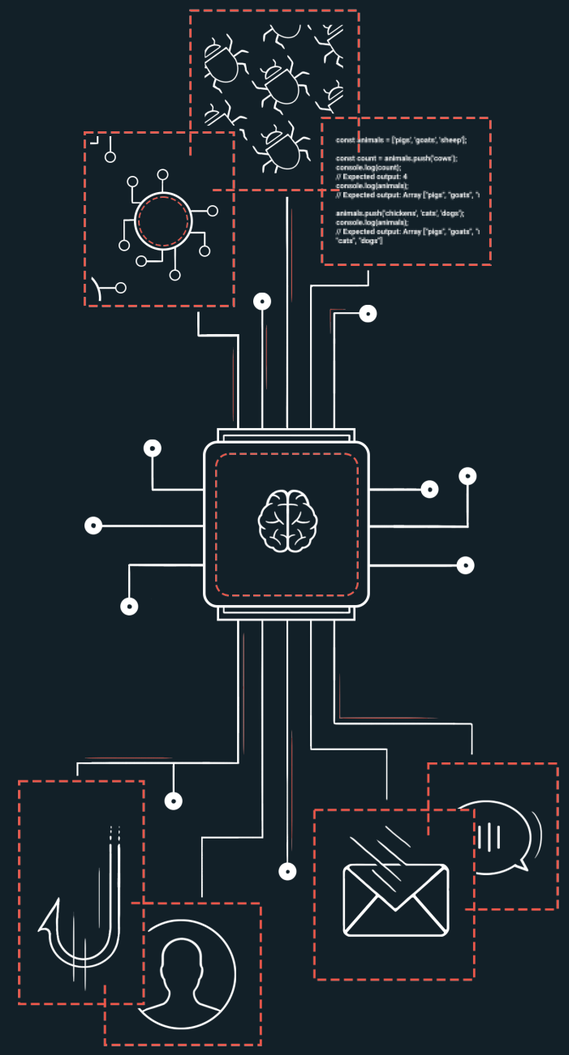
Generative Artificial Intelligence (AI) has levelled the playing field in computing, enhanced the capabilities of threat actors and lowered the barrier to enter the cyber threat landscape for novice attackers.

There are two main areas where generative AI will likely impact the cybersecurity landscape:

Practical Enhancement of Operations: This includes the development and execution of cyberattacks, with AI being used to create scripts or code that could have malicious outcomes.

Social Engineering: Generative AI has the potential to significantly increase the effectiveness of campaigns designed to deceive or manipulate individuals. AI-powered deception can take form in text, speech, images, and video.

Predicting the number of adversaries incorporating technologies like AI into their malicious activities presents challenges. Especially predicting the extent to which these technologies might aid in the development and execution of cyberattacks is challenging. To date, the use of AI during operational phases has been sporadic and difficult to confirm. However, especially in cases pertaining to fraud and social engineering, malicious use of AI will pose a threat to maritime organisations due to its ability to create highly convincing fake communications, such as emails, invoices, and even voice messages that mimic known contacts.



Disruptive Crime

Threat actors focusing on ransomware and extortion attacks will likely continue to expand their operational arsenal. The targeting will likely remain opportunistic. Notable ransomware incidents include attacks on port and terminal facilities and marine technology providers, and the following disruptions have had significant economic implications for shipowners. This trend will likely continue in 2024.

Maritime and shipping organisations are at significant threat of becoming collateral damage in ransomware attacks that affect their supply chain – both physically and digitally. In 2023, several port facilities fell victim to ransomware attacks and closed operations for days, disrupting all operations that relied on the ports. Other likely consequences of attacks against suppliers are leakages of sensitive information and unavailability of digital tools.

2023 was a record year in terms of companies exposed on ransomware Data Leak Sites. NORMA Cyber are aware of 72 instances where maritime organisations have had their data leaked for not meeting ransom demands. In comparison, 52 listings of maritime entities were noted in 2022 and 24 in 2021, showing a steady increase in publicised incidents. The increase is likely due to a combination of a rising number of attacks combined with fewer victims paying the ransom. There are highly likely considerable dark numbers, and victims that pay the ransom are seldomly named on leak sites.

Threat actors will likely increasingly transition to pure data theft and extortion operations, particularly in cloud environments. The cloud is not limited to traditional IT systems but includes systems for extracting and aggregating vessel data.

When faced with cloud environments, threat actors likely find it simpler to steal inadequately protected data, remove the original files, and then demand a ransom for their return. This modus operandi also works against on-prem systems, which means the threat actors adapt a more technology agnostic approach to extortion. It also eliminates the reliance on encryptors that might not always work as intended, and risks damaging files permanently. Although theft and extortion operations are likely to increase, incidents involving malware that encrypt files – ransomware – will highly likely continue to dominate incidents in 2024.

Another anticipated trend is increased targeting of edge devices. Edge devices, such as routers, switches, and remote access solutions, predominantly act as gateways for network entry or exit. As Multi-Factor Authentication becomes more commonplace and user device security improves, edge devices are expected to gain popularity as entry points. Moreover, edge devices tend to be outdated. Threat actors will likely be quick to mass exploit high-reward vulnerabilities in such devices when they become known, requiring shipowners to stay updated on patches to minimise the threat.

Ransomware attacks 2023

Other

Akira - Pilot Thomas Logistics/ Maxum Petroleum (USA)
BlackBasta - ABB (Switzerland)
BlackBasta - GTT Group (Canada)
Cactus - UTC Logistics (USA)
Cyclops - Pechexport (Madagascar)
Darktrace - Port of Naples CO.NA.TE.CO SpA (Italy)
dragonforce - Seven Seas Group (UAE)
Hunters International - Austral USA (USA)
Knight - Transka Tankers/Akbasoglu Holding (Turkey)
Losttrust - Liberty Lines (Italy)
MalaLocker - Harita Group (Indonesia)
Medusa - Aranui Cruises (Tahiti)
Medusa - Gulf American Line (USA)
monti - Superline Logistics LLC (UAE)
monti - Magsaysay Maritime (Philiphines)
Noescape - RS Logistics (Hong Kong)
Qilin - Better Systems (Thailand)
Ransom Cartel - DNV - Shipmanager (Norway)
Ransomware Blog - Kaff Logistics Ltd. (Hungary)
Royal - Livingston International (Canada)
Snatch - Maldives Ports Limited (Maldives)
Stormous - Furuno Spain S.A. (Spain)
Vicesociety - Neptune Lines (Greece)
Vicesociety - SubDrill Supply Ltd (UK)
werewolves - Morsky Bank (JSC) (Russia)
Unknown - Lürssen (Germany)
Unknown - Brunswick Corporation (USA)

8base

Cyberfreight Systems Maritimes Inc. (Canada)
Lysander Shipping (Denmark)
The Integral Port Administration of Quintana Roo (Mexico)

Alphv

Corsica Ferries (France)
IKM (Norway)
Penanshin (Singapore)
Slade Shipping (USA)
Ultrabulk (Denmark)
Yusen Logistics (Japan)

Bianlian

Arab Shipbuilding and Repair Yard Company (Bahrain)
Bolidt (Netherlands)
CMC Marine (Italy)
Flensburger Schiffbau Gesellschaft (Germany)
Nobiskrug (Germany)
Peloindo (Indonesia)

Clop

DESMI (Denmark)
Drydocks World (UAE)
Emerson (USA)
Genesis Energy (USA)
Honeywell (USA)
Hornbec Offshore (USA)
MS Amlin (Canada)
Rhenus Logistics (Germany)
SBM Offshore (Netherlands)
Schneider Electric (France)

LockBit 3.0

AG&P (Philiphines)
AME Offshore Solutions (Australia)
Barchelona Cruise Port (Spain)
BR Logistics USA (USA)
DP World (Australia)
GAC Egypt (Egypt)
Grupo Omega (Brazil)
IPSEN Logistics (Germany)
Melody Shipping Agency (Turkey)
Port of Nagoya (Japan)
Stolthaeven Westport (Malaysia)

Play

Abeko (Netherlands)
Borderlon Marine (USA)
Centek Industries (USA)
Continental Shipping Line (Singapore)
CS Cargo Group (Czech Republic)
Royal Dirkzwager (Netherlands)
Sea Force IX (USA)
Terntank (Sweden)
UECC (Norway)

03 Hacktivism

Hacktivist groups will likely operate as state-aligned proxies and conduct disruptive attacks and information operations in all geopolitical conflicts in 2024. Hacktivists will highly likely target maritime entities in the Nordics.

The hacktivist landscape fluctuates and is highly dynamic. Regional conflict developments will likely drive reactions from hacktivist groups with various skill sets. Maritime organisations who operate in, or have ties to, states or areas with geopolitical tensions face an increasing threat from hacktivists.

The majority of hacktivist groups likely consist of ideologically motivated individuals. The ideology could be political or religious. However, some of the more prominent groups are likely under the influence of states, ranging from state-controlled to coordinated, supported, or influenced. Using hacktivist proxy groups allows states plausible deniability and no direct involvement, thus maintaining the guise of operating within any official agreements they adhere to.

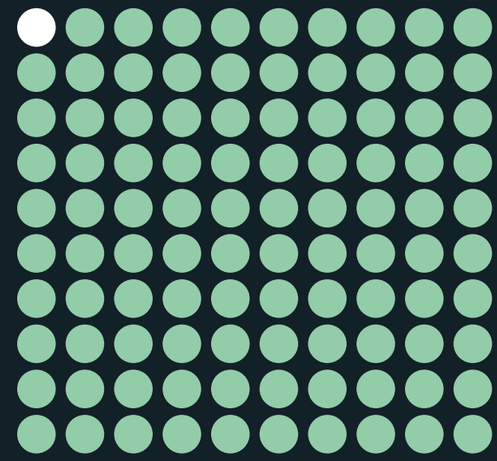
Hacktivists will likely continue to favour basic attack methods that do not require the attacker to be particularly technically apt. An exceeding number of attacks are Distributed Denial-of-Service (DDoS) attacks, where the attackers flood services with requests, creating a traffic jam. This sort of attack does not require any form of hacking or breach into the victim's systems.

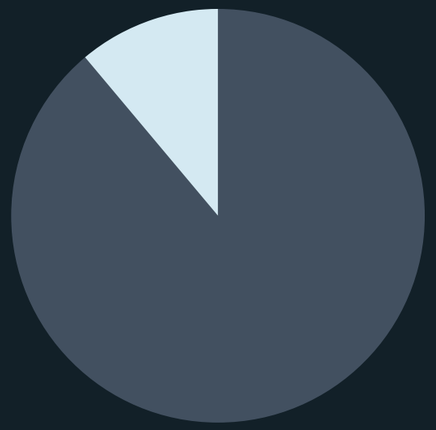
Other attack methods are website defacing, doxing, and obtaining and leaking stolen data. Hacktivists will highly likely boast about and verbally amplify their activities to create publicity.

The amount of DDoS attacks towards maritime entities surged in 2023. NORMA Cyber registered 440 hacktivist attacks towards maritime entities, all but five were DDoS attacks. Four of the remaining incidents were data leaks, and the last was a webpage defacement. The pro-Russian group NoName057(16) was behind 387 of the recorded attacks, but the true number of attacks is highly likely higher.

Hacktivist DDoS attacks will likely have an economic impact on maritime organisations due to operational downtime of services in 2024. Although the attack method is viewed as fairly unsophisticated, hacktivist groups will highly likely increase their capabilities and attack power, making mitigating the attacks harder. Organisations with a low tolerance for resource downtime should implement a layered defence.

98,9%
DDos





NoName057(16) 88%

Other* 12%

***Combined remaining hacktivist group responsible for 0,2-3% each**

In 2023, the NORMA SOC observed DDoS attacks from the NoName057(16) group against multiple members. In response to these incidents, the SOC thoroughly analysed the "Ddosia" botnet client (the software used to perform the DDoS attacks) to better understand its capabilities. With this insight, the SOC could provide advice on mitigation strategies, including specific filtering techniques, by capitalising on errors in the threat actor's programming and their unsophisticated approach.

04 Operational Technology

Hacktivist/state aligned threat to OT

The distinction between state and non-state actors has become increasingly blurred. It is particularly evident in the ongoing Hamas-Israel conflict, where Iran, supporting Hamas, and Israel have extended the conflict to cyberspace. State-aligned actors and state actors masquerading their activities behind hacktivism is an increasing trend. Likely examples have been threat actors taking down fuel pumps at petrol stations across Iran and interrupting water treatment facilities in Israel.

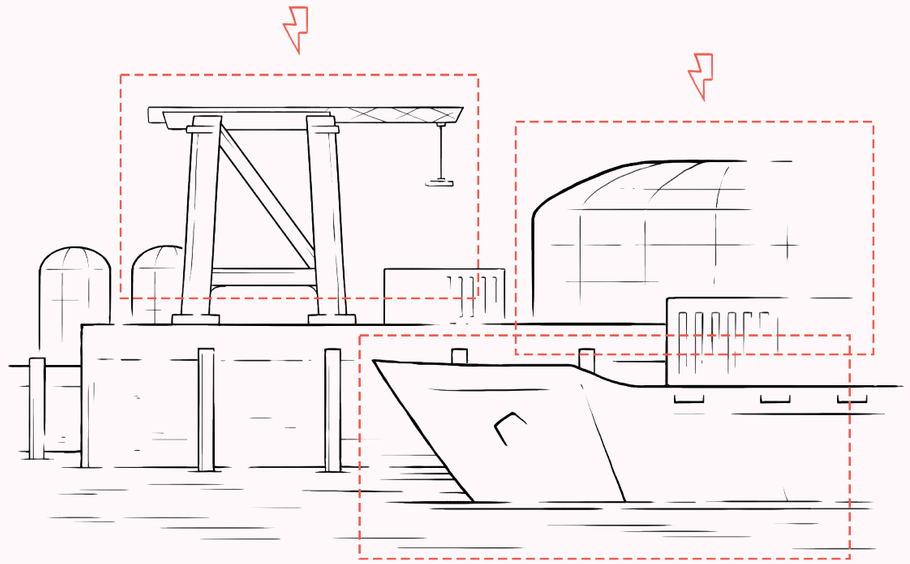
Another trend observed is threat actors publicly claiming their attacks to gain notoriety and recruit followers. The most common attacks are denial of service and web defacements, but there has been an increase in attacks against critical services and industrial control systems.

It is unlikely that hacktivists, state-aligned or not, will disrupt vessel OT. It is highly unlikely that hacktivists have the capabilities to manipulate the control of vessels and perform destructive actions such as groundings or targeted vessel collisions. However, hacktivists will likely take advantage of public-facing vulnerable systems, including maritime entities.

Nation state threats to maritime OT

Government threat actors systematically engage in reconnaissance and pre-positioning activities within critical infrastructure, a tactic yet to be widely observed or reported in maritime environments. As highlighted in threats associated with China, there have been instances where Chinese cyber operations have targeted critical infrastructure within the United States. This behaviour reflects a broader trend where nation-states, amidst escalating global tension, increasingly resort to cyberspace to establish and maintain leverage in case of potential escalation.

In Operational Technology (OT) networks, Shadow Connectivity refers to Crewmembers, Suppliers or Original Equipment Manufacturers (OEMs) having unauthorised or unregulated remote access for maintenance and system monitoring. While such connectivity can be crucial for timely updates and troubleshooting, it poses significant security risks when not properly managed. Shadow connectivity can create hidden entry points into critical infrastructure systems, bypassing standard security controls and potentially exposing these systems to cyber threats.



Reports indicate that IRGC-affiliated threat actors research the potential to disrupt ballast and satellite systems. State-sponsored threat actors are likely to position themselves, perform reconnaissance on maritime equipment and expand their capabilities. There are few reports on impacts to OT networks aboard vessels from this type of targeting. However, the visibility in critical infrastructure to detect these threats is limited. Nation state affiliated threat actors prioritise evasion techniques and persistent access within target networks. This underscores the crucial need for enhanced visibility through logging and monitoring measures within the maritime domain to mitigate potential threats.

It is unlikely that OT networks on vessels will be systematically targeted by nation states in 2024. However, some maritime entities that are of geopolitical importance will likely be targeted. This could, for example, be vessels within the energy sector.

The ransomware threat to maritime OT

The threat from ransomware operators specifically targeting operational technology is low. Although in case an attack against the IT systems of entities with OT systems do occur it will likely affect physical operations. Most organisations will power down OT systems, or operate at limited capacity, until the threat is contained in case of attacks. As reported in the disruptive crime section, over 70 maritime entities have been hit by ransomware in 2023. None of the reported attacks have affected OT networks.

Port facilities have suffered the most significant impact. The entities have had to shut down operations for several days because logistics, billing, etc., have been inoperable. Ransomware is an increasing threat to maritime organisations, but it is unlikely that ransomware will affect vessel OT specifically and impact the ability to control the vessel. However, it is likely that port entities will continue to see larger operational impacts from ransomware in 2024, which likely will have the potential to delay vessel operations.

Vulnerabilities

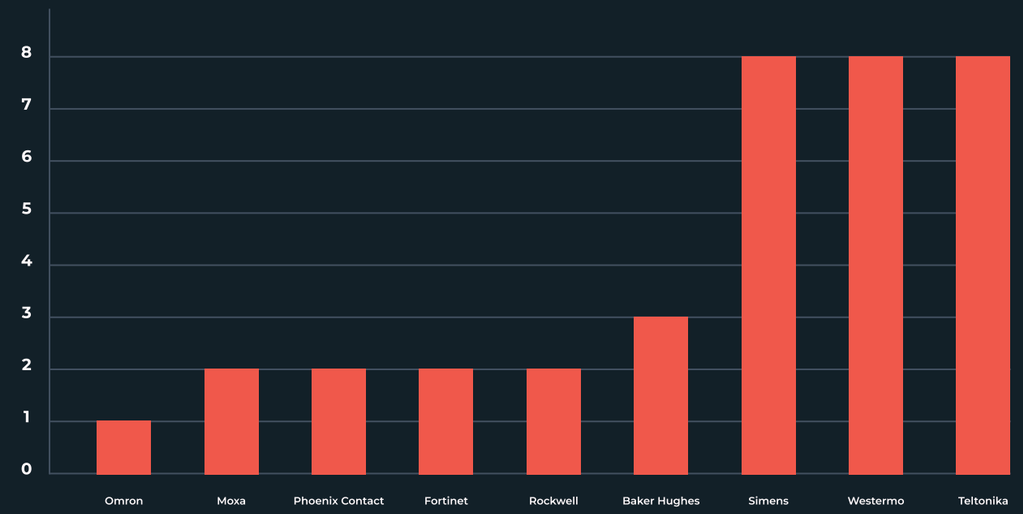
Throughout the year, NORMA Cyber has analysed notable vulnerabilities and movements in the current threat landscape, performed risk assessments of vessel infrastructure and researched methodologies for attacking and defending IT/OT vessel environments.

NORMA Cyber has published ten vulnerability notifications consisting of 36 individual vulnerabilities. The vulnerability reporting criteria are that the vulnerability is rated as high, meaning a score higher than 7.0 as defined by the Common Vulnerability Scoring System (CVSS v3) and that the vulnerability affects devices used in the maritime industry.

The fact that some IT/OT vendors have relatively few reported vulnerabilities does not necessarily mean their products are more secure. It is likely that these products have not been subjected to as much examination by security researchers or that the vendors do not disclose known flaws.

NORMA Cyber is aware that significant vendors are not disclosing their vulnerabilities. As a result, maritime organisations should conduct thorough security assessments of all control systems in use, regardless of the vendor. NORMA Cyber strongly believes in openness and that the most sustainable strategy for everyone is to be open about vulnerabilities and how to mitigate them.

Number of vulnerabilites reported by NORMA Cyber (April 2023 - April 2024)



About NORMA Cyber

About NORMA Cyber and our services

Together Stronger

The Norwegian Maritime Cyber Resilience Centre (NORMA Cyber) delivers cyber security services tailored to maritime organisations.

The center hosts events where members and partners can come together to share best practice and find common solutions. 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 intelligence reporting, incident and crisis response and external monitoring.

NORMA Cyber provides additional services, these are:

- Managed Security Operations Centre services for maritime IT and OT systems, and corporate or cloud infrastructure.
- From 2024 we provide a penetration testing service.

For more information, please see
www.normacyber.no

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

Deep/dark web monitoring and vulnerability scan of internet exposed services. Alerting to members affected.

Network

Competence and knowledge sharing through conferences, webinars and workshops.

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

Penetration Testing

Simulation of cyber attacks against IT and operational technology (OT) systems to identify vulnerabilities and assess the effectiveness of 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 system. There is normally no hardware installation needed or particular types 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 anonymised 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 and 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.

SOC for Vessel Operational Technology (OT)

The SOC team now monitors several vessels OT networks. Through the solutions we are able to:

- Identify assets and create detailed asset lists.
- Identify vulnerabilities and continually evaluate risks.
- Detect anomalies and threats.
- Act on alerts and perform forensic analysis of events.

24/7 monitoring for 100 vessels and

8000 land-based staff in over 19 countries

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 cooperate with the Norwegian Maritime Authority on this assignment.

In January 2024 NCA chose NORMA Cyber 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 when needed 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 crises. This means that each sector is responsible of establishing and maintain the necessary information sharing and response functions. This function is responsible for coordination between stakeholders in the sector and also 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 ICT-security incidents" by NSM.

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 we can make a difference!

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. This information is also critical to identifying trends that can help us to protect our members and the maritime sector.

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

How should you share?
We encourage you to send an email to ops@normacyber.no and be as detailed as possible. Please include full 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.

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 cyber crime or fraud.

Building unified resilience against cyber threats for the Nordic Maritime Sector