NORMA CYBER

Annual Threat Assessment

2023

The Norwegian Maritime Cyber Resilience Centre - NORMA Cyber - is a joint effort between The Norwegian Shipowners' Mutual War Risks Insurance Association (DNK) and the Norwegian Shipowners' Association and started operations in 2021.

NORMA Cyber operates as a non-profit, and the members are organisations in the Norwegian maritime sector. NORMA Cyber currently has more than 90 members represented by more than 2 000 vessels and offshore units.

The centre delivers various cyber security services for its members, including intelligence, security operations and crisis response. NORMA Cyber aims to be the leading hub for operational cyber security efforts 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 Contingency Preparedness Centre. This is a joint centre to support mutual members within complex operations where both physical and cyber threats are prominent. NORMA Cyber also collaborates with other relevant stakeholders, such as the Norwegian authorities, other nations' authorities, and principal stakeholders in the maritime industry.

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

Emergency number: +47 90 98 97 37

Dear Reader,

Welcome to the second edition of the NORMA Cyber Annual Threat Assessment. During the last year, we have seen an increased interest in cyber security among our members and other stakeholders as the threat environment has grown more unpredictable.

This Threat Assessment is based on multiple sources - including Norma Cyber members. This product predicts the development of the maritime cyber threat landscape in the upcoming year using closed and open sources. The target audience for the Threat Assessment is the executive level and decision-makers among our members and other relevant stakeholders. Even though the intelligence is of a strategic nature, we believe that cyber security experts will find the content relevant and that it will increase the dialogue and shared understanding among different branches and levels of our member organisations.

Technological development within the maritime landscape is moving fast. Maritime connectivity is rising quickly; there is an increased demand for live data from critical systems and more complex supply chains. These factors increase the maritime industry's vulnerability to cyber security threats. Meanwhile, the threat landscape is developing and becoming more complex and dynamic.
During such demanding times, approaching cyber security through facts, structured analysis, and knowledge-based assessments are becoming more important than ever.

Enjoy the read!

Lars Benjamin Vold
Managing Director
Norwegian Maritime Cyber Resilience Centre


EVERGREEN
EVERGREEN
MAERSK
SEALAND
MAERSK
SEALAND

Summary

State Actors

Russia and China continue to represent a high espionage threat to the maritime sector. In 2023, the maritime sector will likely see more network reconnaissance and intrusion attempts from Russia-linked threat actors. Organisations involved in sanctions, transportation of sensitive goods, critical national infrastructure and energy face the highest threat. China-linked threat actors are highly likely to conduct cyber espionage operations towards organisations involved in technology development and projects related to critical national infrastructure. Maritime organisations operating in the South China Sea are likely targets.

Cybercrime

The threat from financial fraud and ransomware campaigns affecting entities in the maritime sector is high. In regards to ransomware, members are also at risk of becoming collateral damage if a third party is compromised. Such damage may include leaked documents or disrupted physical operations due to facilities being down. The threat from ransomware operators targeting operational technology specifically is low. Phishing is still the favoured entry point for financially motivated threat actors.

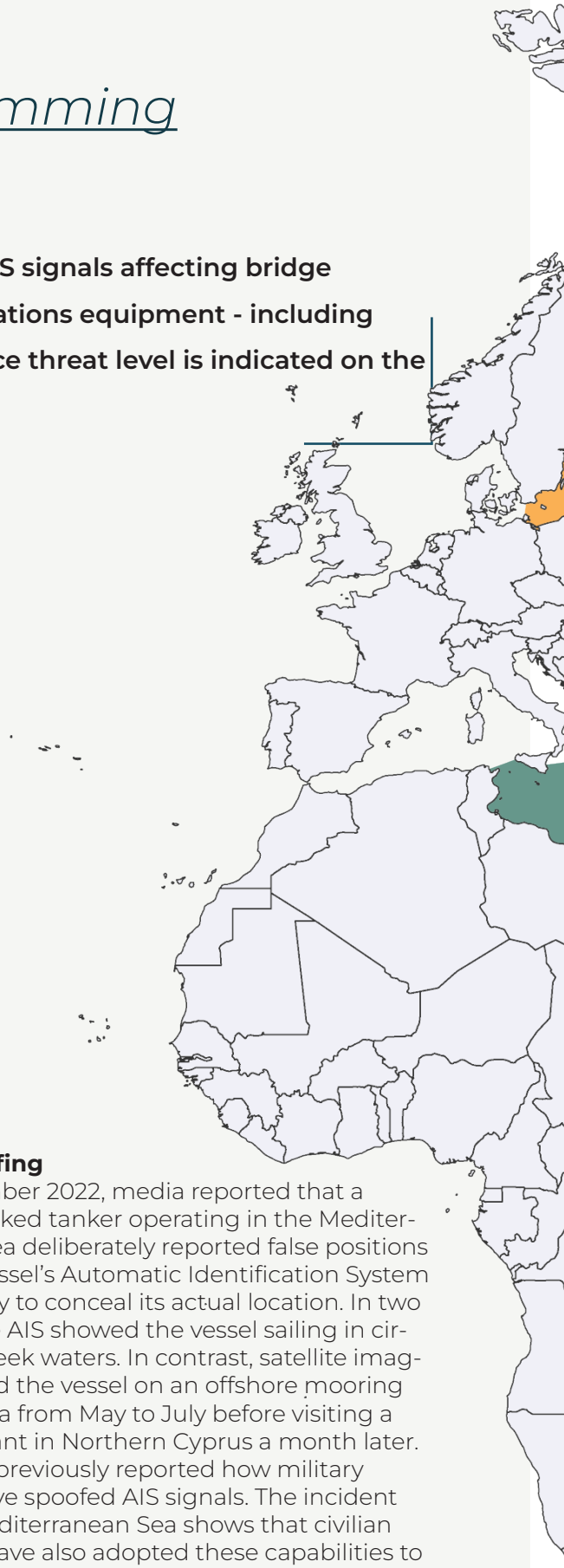
Hacktivism

Hacktivist groups are becoming more structured and professionalised. Maritime entities may become collateral damage in hacktivist campaigns targeting geographical areas and receive attention purely due to their nationality. Hacktivists push the narrative of their cause, and their attacks are highly likely to follow the geopolitical situation and favoured media narration. The threat from hacktivist defacement attacks, data theft, and information operations aimed at the maritime sector is low. The DDoS threat from targeted attacks against European maritime entities is moderate.

GNSS Interference

Spoofing and Jamming

Interference can result in lost or inaccurate GNSS signals affecting bridge navigation, GNSS-based timing, and communications equipment - including satellite communications. The global interference threat level is indicated on the map. The threat is expected to continue in 2023.



Over the last year, GNSS interference has been reported in:

- The Arabian Gulf / Persian Gulf specifically in the Strait of Hormuz and off the coast of Saudi Arabia and Qatar
- The eastern and central Mediterranean Sea specifically in the vicinity of the Suez Canal and off the coast of Libya, Turkey and Israel
- In the Yellow Sea and the Sea of Japan
- In Kattegat and in the Baltic Sea
- In the Black Sea
- Off the coast of Brazil

Jamming GNSS signals requires relatively basic technology. The overall availability of equipment enables criminal groups and insurgents to use this tactic, particularly over short ranges. Criminals likely conduct GNSS interference off the coast of Brazil.

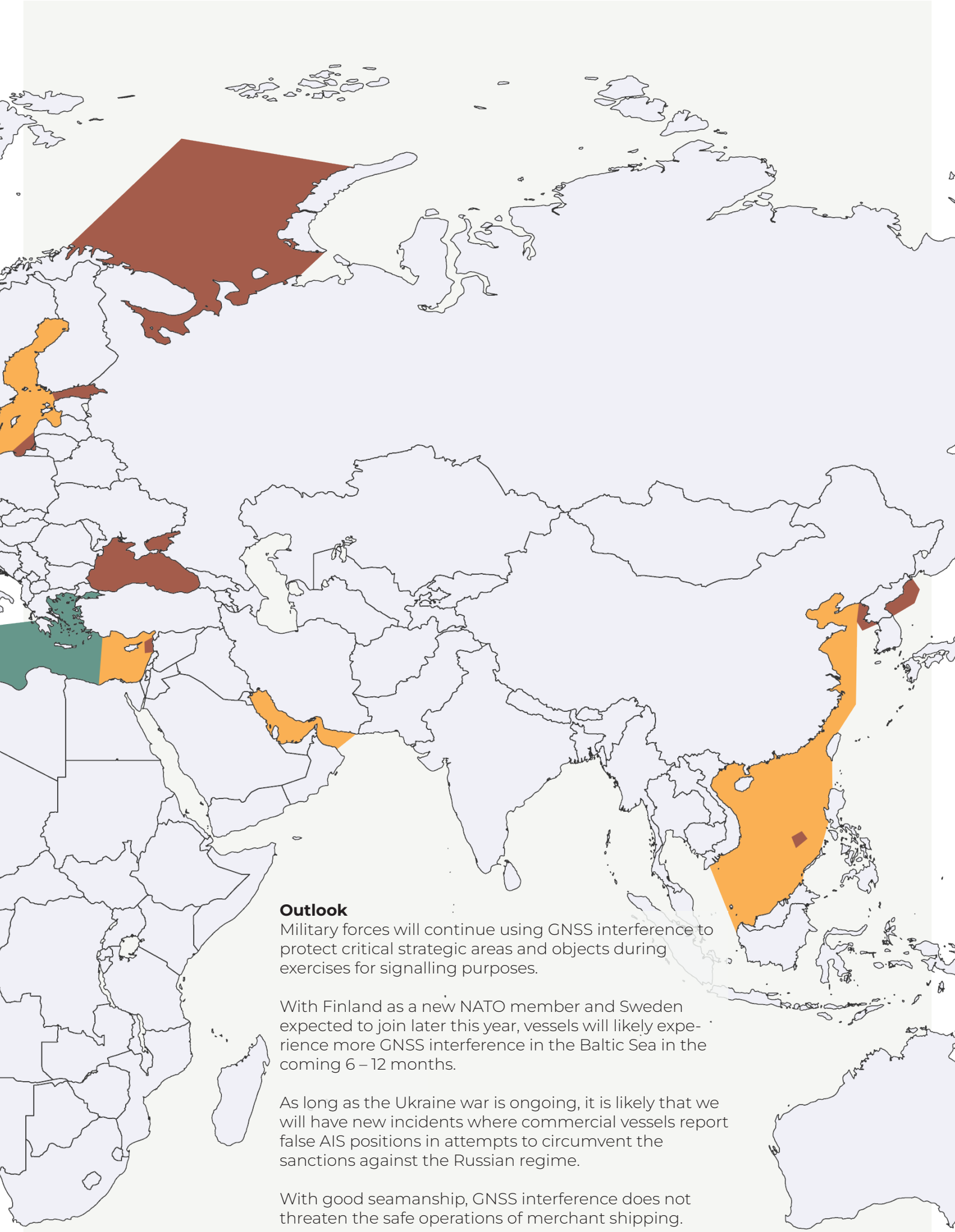
Spoofing of GNSS signals is more complex and is primarily conducted by state actors. Russia has been known to use GNSS spoofing or jamming to protect VIPs and strategic facilities in armed conflicts and military exercises.

Other nation-states such as North Korea, China, and Iran also possess these capabilities to protect critical strategic areas, in harbours, or during military exercises. This activity is likely to continue in 2022.

In the Barents Sea and Baltic Sea, GNSS interference is more likely to occur during NATO or Russian military exercises.

AIS spoofing

In December 2022, media reported that a Russia-linked tanker operating in the Mediterranean Sea deliberately reported false positions via the vessel's Automatic Identification System (AIS), likely to conceal its actual location. In two cases, the AIS showed the vessel sailing in circles in Greek waters. In contrast, satellite images showed the vessel on an offshore mooring near Malta from May to July before visiting a power plant in Northern Cyprus a month later. We have previously reported how military forces have spoofed AIS signals. The incident in the Mediterranean Sea shows that civilian tankers have also adopted these capabilities to blunt western oil export restrictions imposed on Russia.



Outlook
Military forces will continue using GNSS interference to protect critical strategic areas and objects during exercises for signalling purposes.

With Finland as a new NATO member and Sweden expected to join later this year, vessels will likely experience more GNSS interference in the Baltic Sea in the coming 6 – 12 months.

As long as the Ukraine war is ongoing, it is likely that we will have new incidents where commercial vessels report false AIS positions in attempts to circumvent the sanctions against the Russian regime.

With good seamanship, GNSS interference does not threaten the safe operations of merchant shipping.

The Ukraine War

and the impact on the maritime sector

Russia's invasion of Ukraine has dramatically changed the security landscape in Europe, with noticeable effects on the maritime sector. Physical and digital disruptions, side picking, and sanctions - there are many facets, and the threat actors active in the war range from infamous state-sponsored hackers to invested private actors.

Indispensable Energy
Russia used to be a leading supplier of gas to Europe. Their illicit attack on Ukraine has led to extensive European and US sanctions, affecting the energy sector, among others. Following the cessation of deliveries of Russian gas, Norway became the largest natural gas supplier to the European market.

The increased importance of supply security from the Norwegian continental shelf affects the Norwegian offshore fleet. In addition to extensive gas deliveries through pipelines, Norwegian-affiliated vessels account for a significant share of the world's total capacity in the transportation of Liquified Natural Gas (LNG) and Floating Storage and Re-gasification Units (FSRU).

These vessels constitute a strategic capability to secure Europe's energy supply. The Norwegian maritime sector, especially those operating within the energy segment, will likely be attractive intelligence targets for state-linked threat actors, particularly from Russia.

The Norwegian-affiliated fleet includes over 50 LNG tankers and more than 10 FSRUs.

The FSRUs are LNG storage vessels with an on-board regasification plant capable of returning LNG into a gaseous state. The vessels then supply it directly into the European gas network, providing energy to France, Germany, Lithuania, Poland and Latvia.

The Ukraine War

Hacktivism

Pro-Russian hacktivists engaged in the war will likely pose the most significant hacktivist threat to maritime entities in 2023. Following the Russian narrative, the hacktivist will likely continue to react based on how their news feed is presented to them. The targeting will likely persist in being somewhat randomised.

Hacktivism is not what it used to be
Cyber activists, commonly referred to as hacktivists, are persons who carry out cyberattacks in support of a cause. One critical pillar of activism is promoting an opinion in a way that the opposition and the public cannot ignore. This is traditionally done through vigorous campaigning. Hacktivists operate in the same manner in the digital domain.

The Russian-Ukrainian war has helped fuel the transition from loose groups of lone wolfs operating together on a set cause to more organised groups with top-down leadership and military-inspired structures. The most prominent groups in today's landscape have a clear political motivation on which the group members agree, often stated in a manifesto. Noteworthy Pro-Russian groups require potential members to have a minimum skill set and knowledge before being accepted into their ranks. Thus, professionalising the groups.

Some hacktivist groups have been particularly interested in operational technology (OT) systems and claim to have disrupted internet-facing units and systems' operations. Two hacktivist groups have dominated this field, GhostSec and Team OneFist, who both regularly shift causes. Based on their public appearance, both teams are likely devoted to rebelling against oppression and unsolicited power abuse. All of the more publicised OT attacks targeted pro-Russian or Iranian entities. None affected maritime entities.

With the increased professionality, hacktivist groups are venturing into other activities, such as establishing forums, advertising crypto-related services, and moving towards their own solutions for Distributed Denial of Service (DDoS) attacks. Pro-Russian groups such as KillNet and NoName057(16) have also initiated fundraisers and sales of merchandise to help fund operations.

An exceeding number of attacks are 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 on the victim's side. Other attack methods are website defacing, doxing, and obtaining and leaking stolen data. The targeting will likely persist in being randomised, with media exposure in relation to the Ukraine-Russia war increasing the chances of receiving hacktivists' attention. Entities that have been targeted once are more likely to experience repeated attempts.

14 Days of DDoS attacks towards the maritime sector

29 Unique pages affected

11 Of whom belonged to Norwegian companies

Maritime attacks by the Al Tahera Team **1**

Maritime attacks by KillNet **7**

Maritime attacks by NoName057(16) **26**

The Ukraine War

Notable Events

State Actors

Destructive cyber-attack on Viasat KA-SAT satellite broadband

In the early hours of 24 February 2022, just one and a half hours after president Putin announced the start of Russia's invasion of Ukraine, the first major destructive cyber-attack hit Ukraine. A Russia-linked threat actor targeted the Viasat KA-SAT satellite broadband service. The aim was likely to target Ukraine's military satellite communication systems, but it also impacted civilian organisations across Europe. For instance, German Enercon lost connection to 5800 wind turbines, and Norwegian meteorologists on Svalbard and Bjørnøya lost external communication channels for two weeks due to the attack.

The attack consisted of two phases. First, the attackers used Viasat satellite modems in Ukraine to perform a Denial-of-Service attack, temporarily knocking KA-SAT modems offline. Secondly, the attackers exploited a Virtual Private Network misconfiguration to access the management segment of the KA-SAT network. With this access, the attackers sent commands that overwrote key data in the memory on tens of thousands of modems, rendering them unable to access the network but not permanently unusable. A substantial number of the modems were located outside of Ukraine. The cyber-attack on Viasat did not impact maritime satellite communication but demonstrated that satellite systems are vulnerable to cyber-attacks.

24 February 2022

25 February 2022

Criminals and Hacktivists

Ruckus in the underground

Following the invasion of Ukraine, cybercriminals started to state allegiance to either Ukraine or Russia. Most noteworthy was that the most prominent ransomware syndicate at the time, Conti, published a statement on their Data Leak Site (DLS) declaring that they fully supported the Russian government and that any digital attack on Russian entities would be retaliated. Conti later changed the statement to say that they are apolitical and condemn the ongoing war but would still attack any "Western warmongers" that tries to attack Russian critical infrastructure.

The Ukraine War

What is a wiper?

A wiper attack aims to delete or destroy computer or network data permanently. The purpose of a wiper attack is to cause maximum damage and disrupt the system's normal functioning. Unlike other types of attacks, such as ransomware, the goal of a wiper attack is not to extort money from the victim but to cause destruction.

Wiper attacks typically overwrite critical system files, delete data, and disable the operating system. Once the wiper executes on the target system, it spreads rapidly throughout the network.

Russia-linked threat actors used wiper malware against Ukraine as early as January 2022. Since then, they have used more than nine different wiper malwares and two ransomware-like malwares in destructive cyber-attacks against hundreds of systems across the Ukrainian government and critical infrastructure.

Destructive malware

Viasat confirmed that the AcidRain wiper was used in the 24 February attack against the KA-SAT modems.

31 March 2022

27 February 2022

Retaliation leak

Someone leaked over 60,000 internal messages belonging to the Conti ransomware operation, including some of the training material, as a reprisal for the syndicates' outspoken siding with Russia. The leak exposed how the criminal organisation worked, and the Conti brand seized operations not long after.

The Ukraine War

What is network reconnaissance?

Network reconnaissance gathers information about a computer network to identify potential vulnerabilities and plan a cyber-attack. It involves actively probing the network to obtain details about its architecture, operating systems, applications, and network devices such as firewalls and routers. Network reconnaissance aims to get as much information as possible about the target network to identify potential weaknesses and vulnerabilities that can be exploited to gain unauthorised access, steal sensitive data, or disrupt network operations.

Network reconnaissance activity against entities in the LNG segment

NORMA Cyber received the first warning from a partner that Russia-linked threat actors were conducting network reconnaissance against specific entities involved in transporting or re-gasifying LNG.

We established the "**LNG Cyber Security Forum**" in May 2022, where we worked together with members involved in the transportation or re-gasification of LNG to investigate the warning.

18 May 2022

29 June 2022

Emotions leads to actions

KillNet listed 14 Norwegian target domains on their Telegram channel. The post also featured an image of Norway's Minister of Foreign Affairs, Anniken Huitfeldt, as the fictional character Maleficent. KillNet affiliates then shared the post on their Telegram channels. The attacks coincided with attacks on Lithuanian entities and were likely a rebellion against recent sanctions on the transportation of goods to Kaliningrad and Svalbard. Although Norway is not a part of the EU, it applies EU sanctions against Russia. No Norwegian transportation or maritime entities were on the target list.

The Ukraine War

Vessel is hit by a missile in Ukraine, 2022. DNK

1 July 2022

Follow-up

NoName057(16) announced they would continue KillNet's work and took credit for DDoS attacks towards three Norwegian domains. A supportive follower commented the following in their chat:

"In Norway, transport logistics is very developed by means of ferry services, this is perhaps a very serious sector of cargo transportation in Norway (...) A strike on this area will be more interesting than helicopters and mail combined."

3-5 July 2022

"Thanks for the tip"

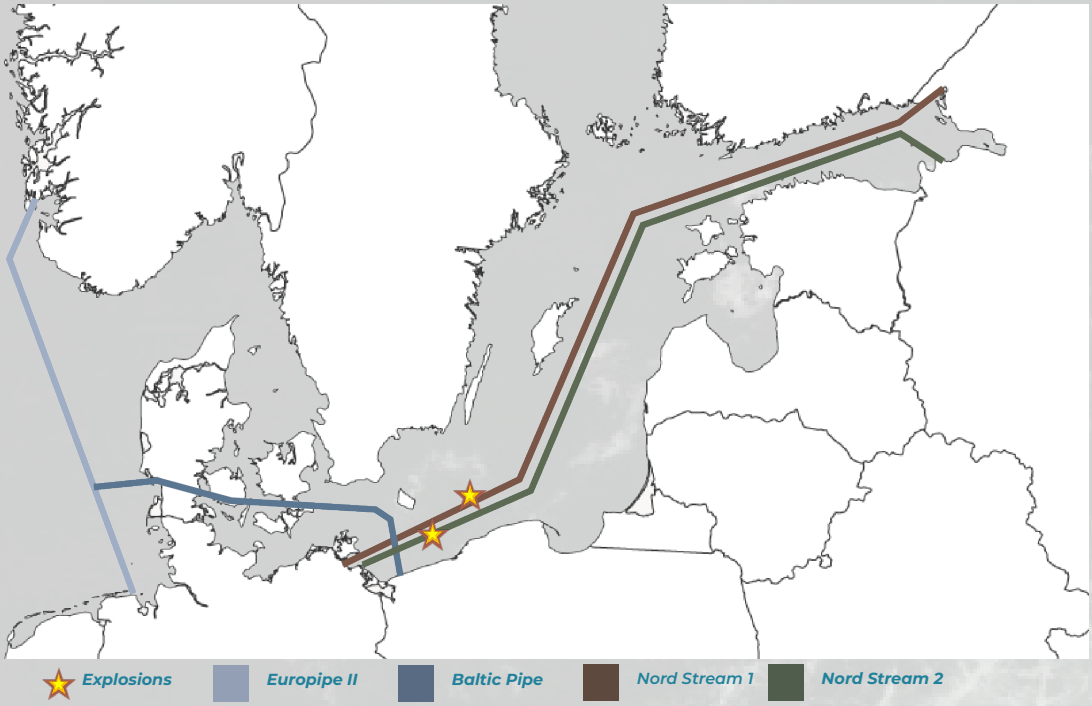
NoName057(16) apparently took note of their fan's suggestion and launched DDoS attacks towards at least eleven maritime domains, most within the passenger transportation segment.

The Ukraine War

Trade stop

Gazprom halted gas flows through Nord Stream, citing issues related to European sanctions imposed against Russia over the war in Ukraine.

2 September 2022



Nord Stream 1 and 2 sabotage

Multiple explosions rendered Nord Stream 1 and 2 pipelines inoperable. The incidents occurred the day after the EU announced the opening of the Baltic Pipe at a ceremony in Goleniów, Poland. The Baltic Pipe will be a pivotal route to carry gas from Norway through Denmark to Poland and neighbouring countries.

The Nord Stream incidents and several reports of unidentified Unmanned Aerial Vehicle (UAV) activity close to offshore installations in the North Sea and critical onshore infrastructure increased uncertainty among the general public. The Norwegian Ministry of Petroleum and Energy decided to strengthen the preparedness related to infrastructure, land facilities, and installations on the Norwegian continental shelf in response to reports of increased UAV activity. In addition, the Norwegian Coastal Administration increased the threat level at 20 port facilities and terminals.

Subsequent investigation of the Nord Stream sabotage confirmed that the damages resulted from deliberate actions. The perpetrators are still unknown.

26 September 2022

Network reconnaissance activity against entities in the oil and gas sector

NORMA Cyber received another warning that an unknown threat actor conducted network reconnaissance against entities in the gas sector. The threat actor likely targeted entities involved in the transportation of LNG. The reconnaissance activity included port scanning, accessing web pages, and automated login attempts (brute-force) to VPN services. This activity was estimated to have been ongoing from June 2022 until September 2022.

Based on similar reporting from other partners, a Russia-linked threat actor likely conducted this network reconnaissance activity, targeting a wide range of organisations in both the government and private sectors. The results from the network reconnaissance could have been used to exploit vulnerabilities in internet-facing servers or remote access with credentials acquired through automated login attempts (password spraying).

13 October 2022

The Ukraine War

Ransomware attacks on transportation and logistics industries

A ransomware-like campaign targeted organisations in Ukraine and Poland's transportation and logistics industries utilising previously unknown ransomware. The ransomware labelled itself as "Prestige ransomware" and was later linked to the Russia-linked threat actor Sandworm, which has publicly been attributed to Russian military intelligence services.

The Prestige ransomware campaign highlighted a shift in Sandworm's destructive attacks, signalling an increased threat to organisations directly supplying or transporting humanitarian or military assistance to Ukraine.

18 October 2022

The Ukraine War

ASSESSMENT AND OUTLOOK

NORMA Cyber assess that Russian-linked threat actors are highly likely to continue to leverage destructive cyber-attacks against Ukrainian critical national infrastructure. Organisations in the energy, utilities, and logistics sectors are likely targets to support kinetic military objectives in the conflict. The threat from Russia-linked destructive cyber-attacks against maritime organisations, ports and terminals outside Ukraine is low.

Russia-linked threat actors are unlikely to perform destructive cyber-attacks outside Ukraine in fear of escalating the conflict and triggering a NATO Article 5 scenario.

The threat from Russia-linked cyber-espionage operations against maritime organisations continues to be high, particularly against organisations involved in sanctions, transportation of sensitive goods, and critical national infrastructure, energy, or oil and gas. The Ukraine war has dramatically changed the security landscape in Europe. In the next 6-12 months, the maritime sector will likely see more network reconnaissance activity and intrusion attempts from Russia-linked threat actors.

Network reconnaissance activity against entities in the oil and gas sector and possibly entities involved in the transportation of LNG

Media services reported on network reconnaissance activity against the Eemshaven LNG terminal in the Netherlands, pointing at Russia-linked threat actors.

The Eemshaven LNG terminal opened in September 2022 and was the first FSRU-based import terminal for LNG in the Netherlands. The terminal was developed to increase supply security and help the Netherlands become less dependent on Russian gas.

25 November 2022

Regional Conflicts

China

China-linked espionage pose a significant threat to the maritime sector. Beijing devotes significant resources to secure advanced technologies, including cyber espionage and theft of intellectual property. In 2022, China's offensive cyber operations maintained a high tempo to gain dominance.

The tension around Taiwan will continue to pose a significant challenge. In late 2022, a China-linked threat actor targeted Taiwanese government organisations to collect maritime intelligence, illustrating how digital espionage can affect maritime entities. Cyber operations will remain China's preferred acquisition method for intelligence collection and insight into current conflicts.

Organisations involved in, or supporting, marine technology development, shipbuilding, renewable energy, naval engineering, and mapping or extraction of natural resources are of particular interest to China. As China continues to pursue dominance in technological industries, the threat of espionage operations towards the maritime sector is likely to persist.

East Asian waters

China has significant strategic and economic interest in the maritime sector in East Asian waters, particularly in renewable energy and natural resources. This has led to several China-linked cyber espionage operations against maritime organisations operating in the South- and East China Sea.

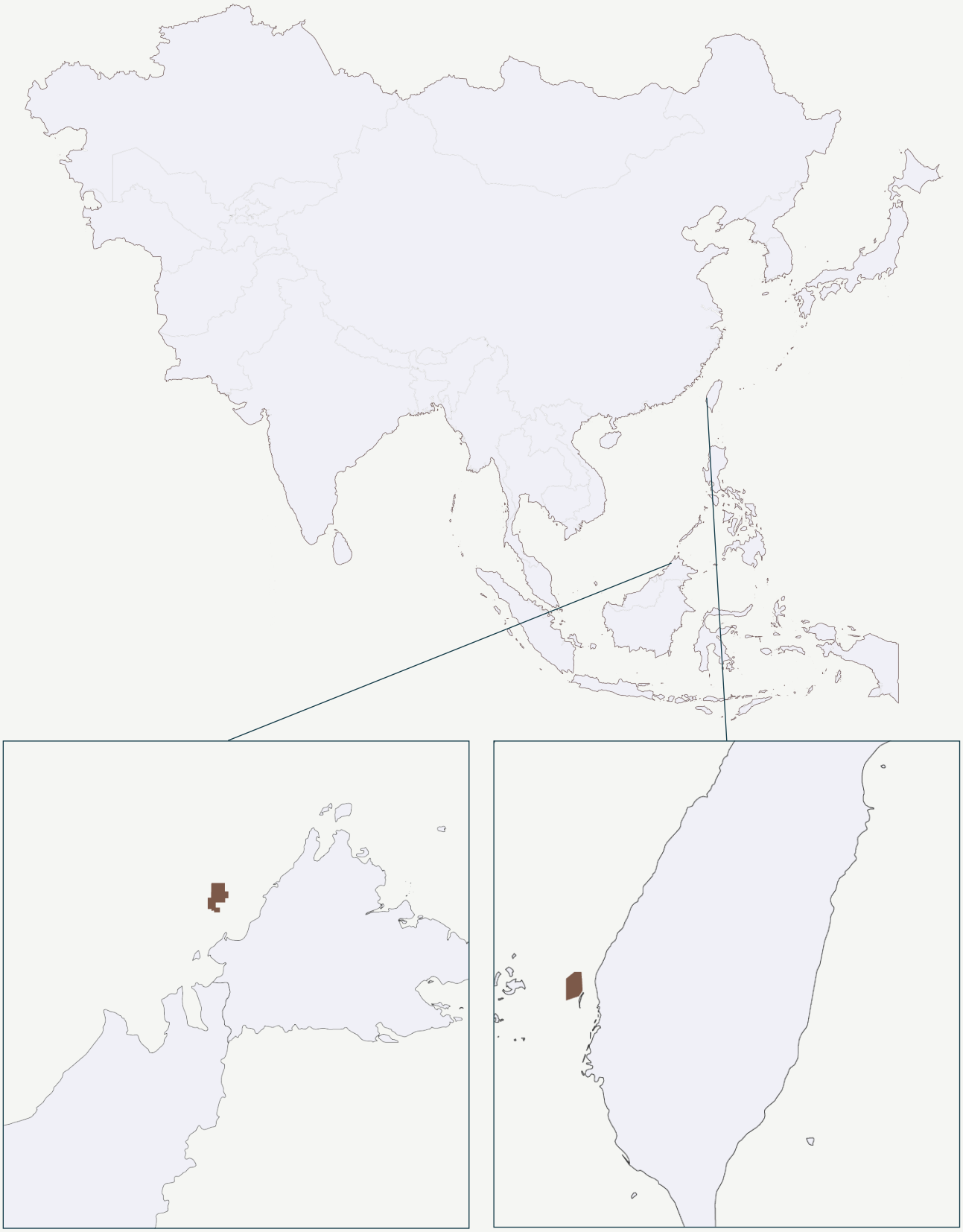
One example of this is the targeting of the supply chain of the Yunlin Offshore Windfarm project in the Taiwan Strait. The project experienced construction delays causing several significant contractors to end their engagement and leave the project unfinished. Coinciding with the project's uncertain future a European manufacturer of equipment used in the construction was targeted by phishing activity. The design of the phishes suggests that the threat actor was attempting to gain information on the project at a crucial time.

Another example is the targeting of companies involved in the Kasawari Gas Project off the coast of Malaysia. From mid-2021 through 2022, various cyber espionage campaigns were observed targeting Malaysia, Australia, and entities operating in the South China Sea. The predominant focus of the campaign was Malaysian companies involved in the Kasawari Gas Project. Four of the eight targeted entities were directly associated with this project.

Shortly after the cyber espionage campaign, the Asia Maritime Transparency Initiative reported disruptions at the Kasawari Gas Project site due to Chinese Coast Guard harassment. While it is impossible to draw a direct correlation between the cyber espionage campaign and the naval intervention, the historic targeting focus of China-linked cyber actors and the subsequent maritime intervention suggest that the project in the South China Sea was a high-priority area.

Both cases have been attributed to the China-linked threat actor APT40. Information suggests that the threat actor behind this campaign operates out of Hainan Island in China. The US Department of Justice has indicted APT40 for providing long-term support to the Hainan Province Ministry of State Security. The Department has also noted that APT40 has historically focused on intellectual property related to naval technology developed globally by federally funded defence contractors.

The examples demonstrate the cyber threat posed by China to the maritime sector in East Asian waters and how they utilise cyber operations for intelligence purposes. China-linked threat actors are highly likely to continue to conduct cyber-espionage towards the maritime sector globally.



The Kasawari Gas Project, Malaysia

The Yunlin Offshore Windfarm, Taiwan

Cybercrime

Initial Access

Employees' inboxes are still the favoured entry point into organisations. Criminals use phishing emails to steal credentials, inject themselves into conversations, and deliver malware. Other means of initial access include exploiting vulnerabilities and public-facing applications. This will likely persist.

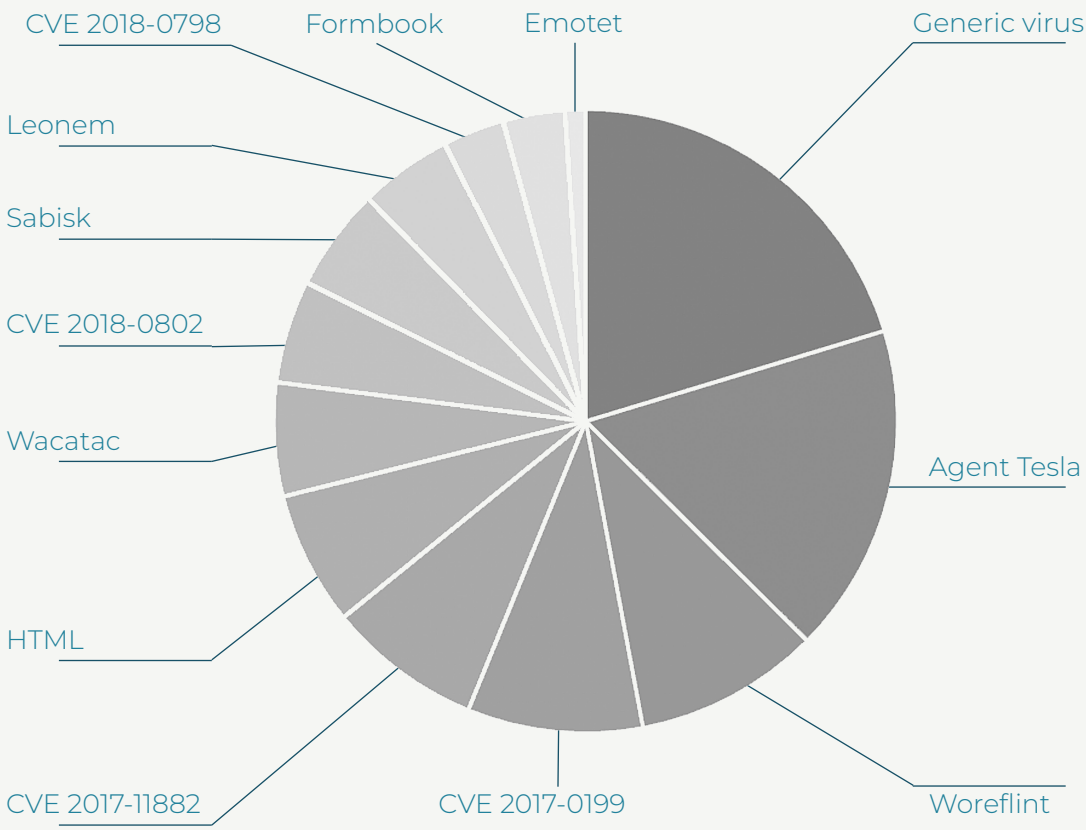
Phishing is one of the primary methods criminal threat actors use to obtain access to organisations. NORMA Cyber continues to observe phishing campaigns with a maritime topic often related to port arrival and departure. The campaigns we monitor all contain malware or leverage known exploits, often as attachments, relying on user execution. An exploit is a way of using a vulnerability to enter or compromise digital assets. Several exploits can exist for one single vulnerability.

When Microsoft announced a shift in their macro policy in the spring of 2022, threat actors started to explore new delivery vectors, such as using Windows shortcut files containing PowerShell scripts, Microsoft Excel Add-in files, and OneNote documents, to name a few. We also noticed a considerable increase in HTML phishes when the change was attempted to be enforced. HTML phishes sent users to fake login pages, often mimicking Office365 sites.

At least

188

Weaponised phishing campaigns with a maritme theme



At least

208

Credentials to member portals posted for sale on underground marketplaces

192
Listings said they had the username

197
Listings said they had the password

28
Listings said they had the cookie

Information Stealers

NORMA Cyber regularly observe credentials and system details obtained by information stealers sold on dark web marketplaces. Our monitoring shows that data collected from devices used to access member resources periodically are part of these sales listings. The data consist of usernames, passwords, and, occasionally, session cookies used to access web-based resources.

An information stealer is a type of malware developed to steal sensitive information, often usernames, passwords, and other available authentication tokens saved in browsers. There is a steady rise in the distribution of information stealers and stolen information being sold on dark web markets. Information stealers can also be used to exfiltrate other data, e.g. files and system information, and stage further attacks.

Norma Cyber's deep and dark web monitoring has seen several actors selling credentials to member resources on criminal marketplaces. Based on the content of the logs, these credentials generally stem from employees' personal devices. Information collected from the browser of personal devices is commonly sold as is, where one listing contains the entire log. These logs are sold for between $3 and $15, depending on the forum, stealer used, perceived quality, and seller's reputation. Although there is a lot of open trading on underground forums, many prominent cyber criminals transact goods, including access, privately. This is especially true for high-value access obtained by threat actors with a good reputation and established relationships with other criminal groups.

Access brokers will likely carry on professionalising their business. As the cybercriminal ecosystem continues to develop specialised roles, skilled access brokers will likely become partners of ransomware groups and their affiliates. Lower-tier access brokers, such as those selling logs in bulk on forums, will likely continue to depend on information-stealing malware and maintain a high operational tempo.

Artificial Malevolence

Q4 in 2022 saw the beginning of a race building and publishing Artificial Intelligence bots with natural language processing capabilities. The service ChatGPT by OpenAI kicked off the ball, and the big tech companies have announced that they will publish their alternatives in 2024, speeding up their development. Although these services have security controls that aim to prevent malicious use, researchers have already managed to trick services into creating scripts and phishes for nefarious purposes.

The emergence of AI services with natural language processing capabilities will likely lower the bar for less skilled threat actors to get started. It is also likely that threat actors will use the services to develop functionalities that will increase the success rate of their malware.

Cybercrime

Fraud

Business Email Compromise (BEC) and similar scams employ social engineering to deceive organisations into transferring funds to accounts controlled by the attackers, often under the guise of legitimate transactions expected by the victim. Fraud campaigns continue to pose a high threat to maritime organisations.

The scammers often compromise email accounts and impersonate legitimate entities. BEC attacks are typically lucrative and do not necessitate advanced technical expertise. They often use phishing to gain access, and once in, they read up on the inbox's contents.

The criminals strive to craft email threads that appear authentic, thus increasing the chance of the victim company believing the lure. Due to the low operational cost and high availability of eligible targets, BEC and wire- fraud continue to pose a high threat to maritime organisations. It is highly likely that members will encounter fraudulent invoices in 2023.

Prominent threat actors will likely advance their operations and employ techniques to bypass multifactor authentication (MFA). Some common MFA bypass techniques used in BEC attacks are MFA fatigue and session hijacking.

Nigeria has been identified as a source of many BEC scams due to its large population of technologically apt young adults and weak regulatory environment. The most distinguished groups concentrate on BEC operations. Law enforcement actions towards these groups have had low deterrence success.

Common clues to look for:

1. Typosquatted/misspelled domains
2. New email archiving or forwarding rules
3. Personas with authority that asks for urgent transactions
4. Sudden change of banking information

Example attack

The scammers pretend to be a trusted source and send phishing emails with links.

When clicking the link, the victim is taken to a website mimicking a legitimate service and required to log in.

The scammers validate and steal the entered credentials.

The scammers can now log into the victim's email account.

If MFA is enabled, experienced scammers might attempt to bypass it using techniques such as MFA fatigue.

Many scammers spend some time reading correspondence and learning what is normal. They then inject themselves into the conversations.

When they have gained trust, they send fraudulent invoices or change the bank details on existing invoices.

Ransomware

Ransomware attacks continue to be opportunistic. Notable ransomware incidents include attacks on port and terminal facilities, shipbuilders, and marine technology providers. The operational tempo of influential ransomware groups will highly likely fluctuate slightly through the year and between years, but the threat remains high.

Ransomware – malware that encrypts files – is commonly deployed on the victim system as the last step in a multifaceted attack. The most active ransomware groups continue to decrease the time spent on noisy operations on the victim system by locating and stealing the files believed to be most valuable to the victim and tuning their ransomware to encrypt files faster. In addition to reaching their objective swiftly, this reduces the time available for defenders to detect them. On average, threat actors spend between two and five days on a compromised system before encrypting it.

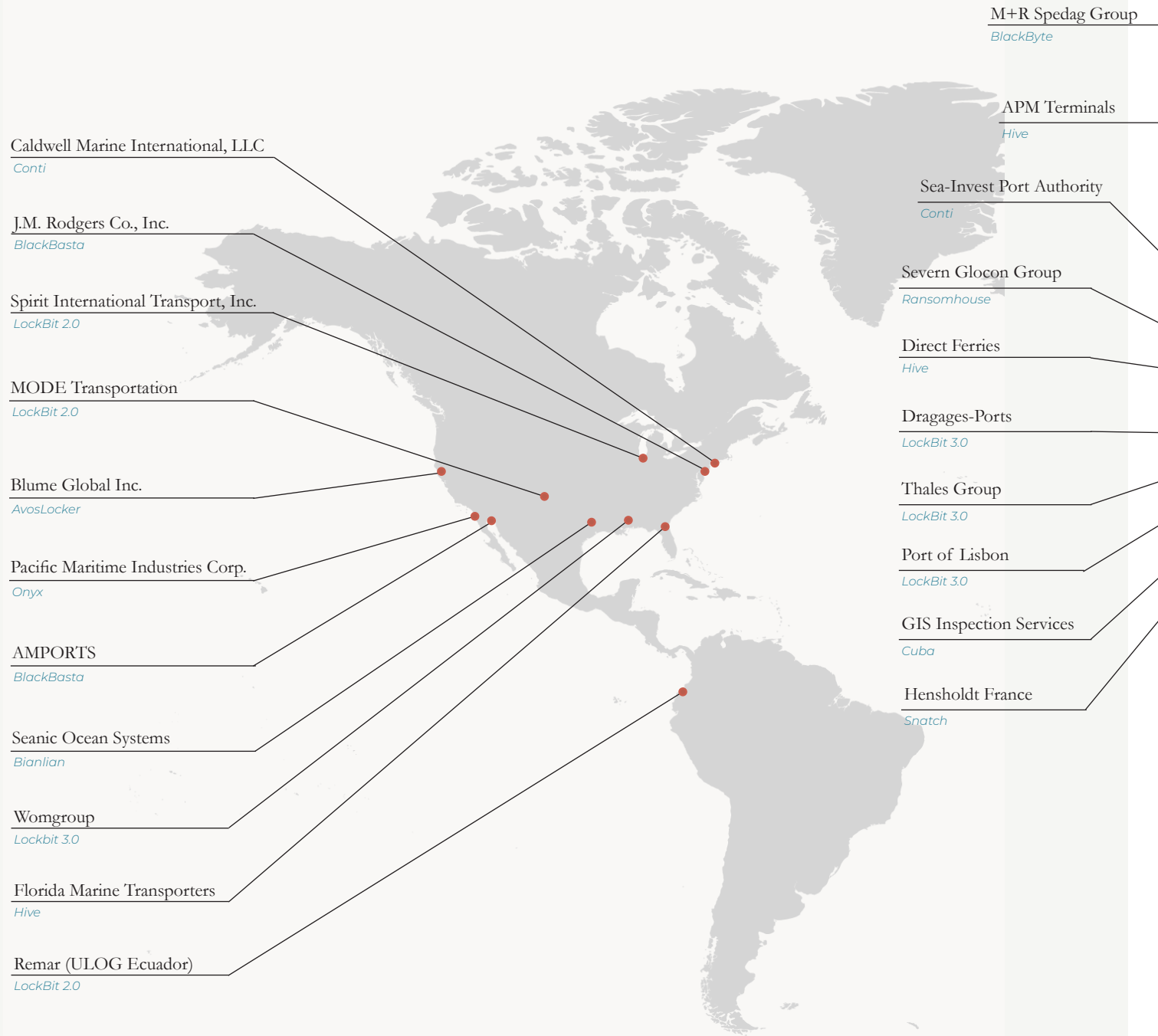
NORMA Cyber are familiar with 23 successful ransomware attacks towards maritime entities in 2021 and 49 successful attacks in 2022. This does not necessarily mean that maritime organisations are targeted more by threat actors than previously, but merely that more oganisations were attempted shamed on various Data Leak Sites. There are likely considerable dark numbers, and victims that pay the ransom are seldomly named on leak sites.

Although only one of the maritime ransomware victims in 2022 was explicitly Norwegian, members can become collateral damage. For instance, Belgic Sea-Invest had to seize all operations due to a ransomware attack, which impacted ports in Europe and Africa.

The Singaporean shipbuilder Sembcorp Marine, who also builds vessels for Norwegian shipowners, had detailed design drawings leaked. The majority of attacks impacted businesses in the freight forwarding and logistics segment.

Most ransomware attacks affect shore-based IT infrastructure, but there are occasional incidents where vessel IT infrastructure is encrypted. The reason for this is likely the difference in attack surface, with shore-based IT infrastructure being larger and more diverse. To date, no financially motivated ransomware groups have demonstrated the capability or intent to target OT environments directly. Despite the lack of direct OT targeting, such systems are still vulnerable to financially motivated attacks as a disruption to the environment can create a loss of digital control and visibility into operations.

We maintain that the ransomware threat to the maritime industry is high. Maritime and shipping organisations likely also face a high threat from inadvertent disruptive ransomware operations against organisations in their IT supply chains. Other likely consequences of attacks against suppliers are data leakages of sensitive information.

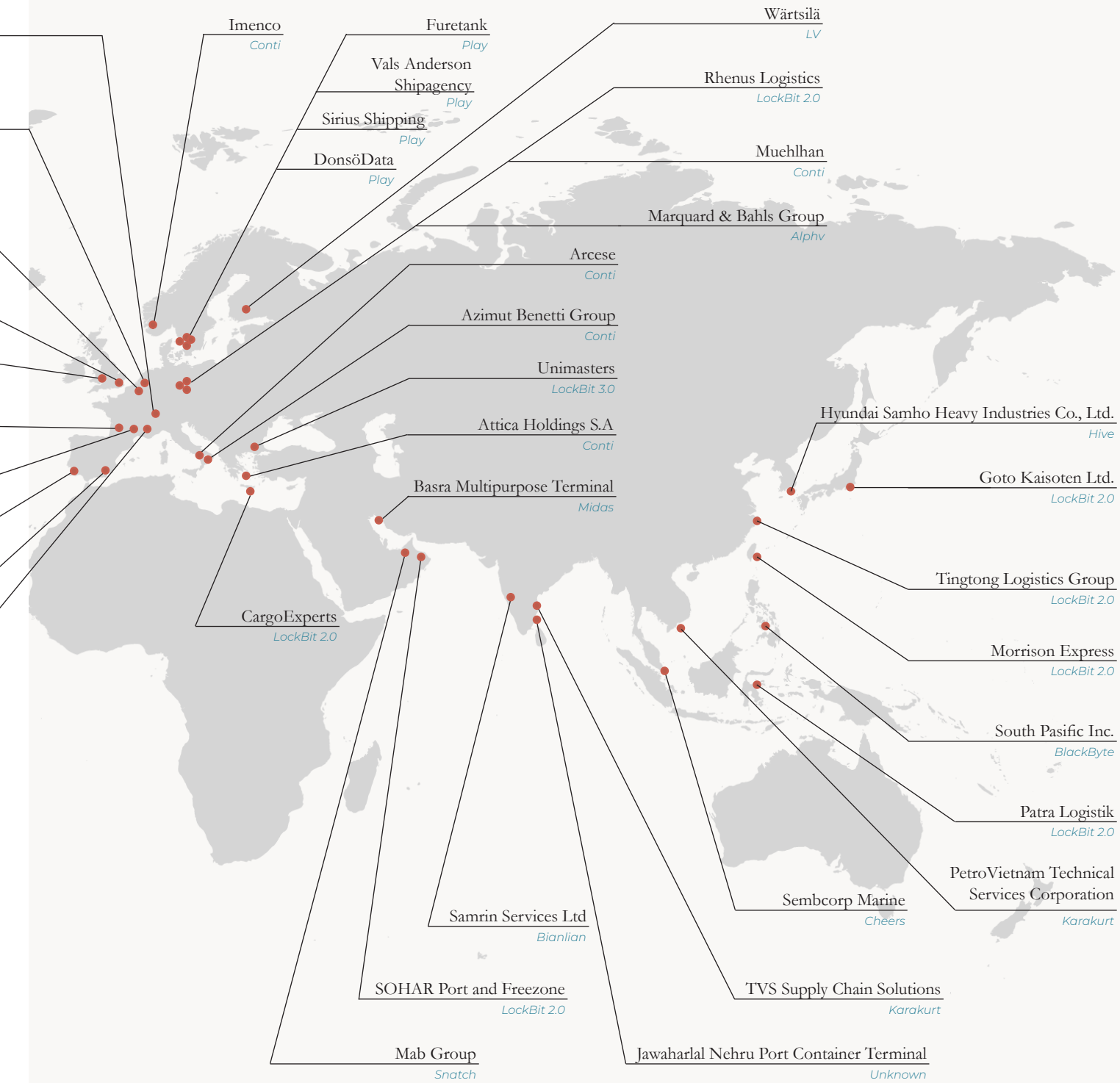


Known ransomware attacks on the

Maritime Sector

January 2022 - December 2022

49
publicised
incidents
globally



Illustration

Malware in the Engine Control

The nature of maritime operations with remote locations and limited access to external resources justifies the usage of USB devices. Some threat actors adapt to this, using external devices to access peripheral IT and OT systems.

At the end of 2022, NORMA Cyber was informed about an incident on an offshore supply vessel operating in the South China Sea. Malware was detected on an engine control room machine, and the infection stemmed from a USB device. Artefacts from the malware behaviour indicated it could spread to other USB devices connected to the infected machine, making this a self-propagating threat.

Technical indicators and behaviour from the incident align with a campaign from 2020 dubbed “KillSomeOne” and attributed to China by Sophos. NORMA Cyber observed an uptick in malware samples related to the campaign submitted to public malware repositories in the last quarter of 2022.

The campaign is likely still active because of the USB-stick malware propagation capabilities. It is unlikely that the compromised offshore supply vessel was targeted by recent efforts – the malware appears to have been a lingering artefact from the 2020 campaign.

Utilising USB devices as an attack vector enables access to non-internet-facing systems that might not be reachable through normal network operations. This is likely part of a dual-attack vector campaign. The threat actor distributes malware with USB propagation capabilities to the target system or waits for the desired type of system or organisation to be compromised before engaging selected systems for further actions.

USB sticks are a favoured method for delivering data to offline or air-gapped systems, both for benign use and malicious actions. They are convenient to attackers as they allow them to dispense malware directly into the host. Malware that self-propagates through USB sticks has a long lifespan, and instances of leftover malware from threat actor campaigns are likely to occur sporadically. The threat from USB stick malware or espionage campaigns is low. Entities relying on USB sticks for updates and who operate in areas or projects with political tension face the highest threat.

Operational Technology

Vulnerabilities

Throughout 2022, NORMA Cyber has analysed notable vulnerabilities and developments in the current threat landscape. Vulnerability is a collective term for weaknesses that an attacker can exploit. All analysed vulnerabilities are in systems type approved for the maritime industry.

NORMA Cyber has published 18 vulnerability notifications consisting of 98 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.

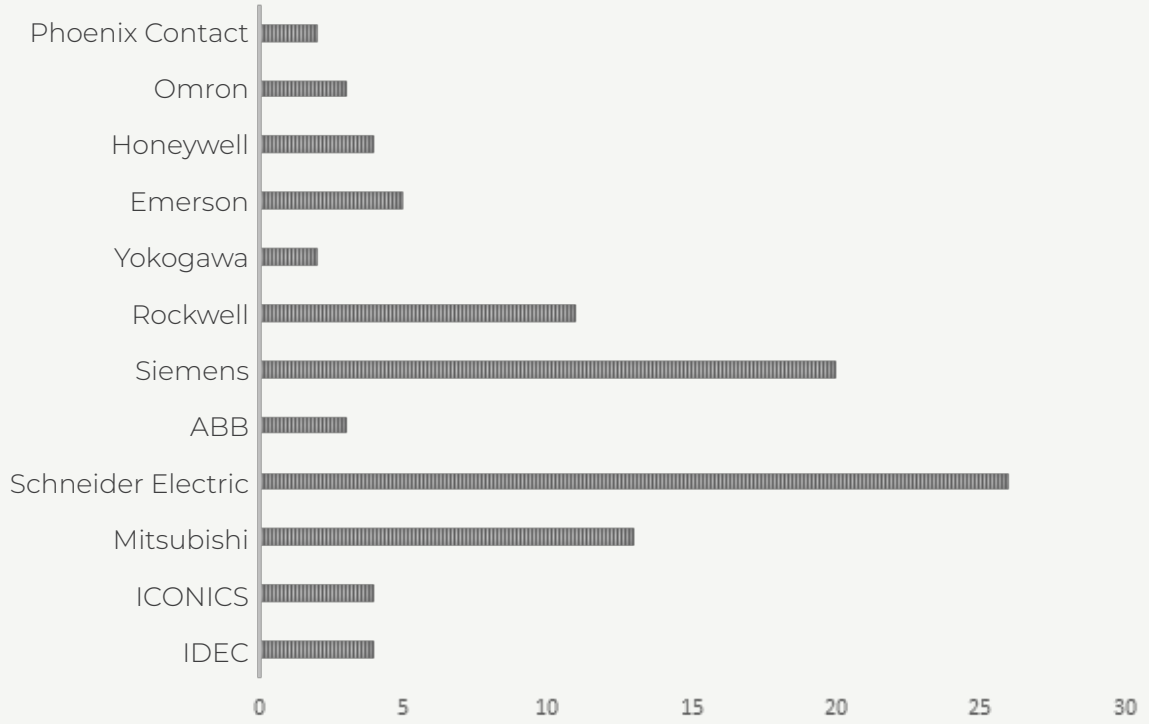
The fact that some IT/OT vendors have relatively few reported vulnerabilities does not necessarily mean their products are more secure. It could reflect that these products have not been subjected to as much scrutiny by security researchers or that the vendors do not disclose known flaws. NORMA Cyber 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 believes that the most sustainable strategy for everyone is to be open about vulnerabilities and how to mitigate them.

98

OT vulnerabilities detailed in NORMA Cyber-reports

April 2022 – April 2023



Membership Services

Together Stronger

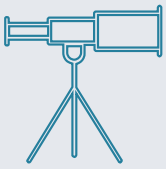
The Norwegian Maritime Cyber Resilience Centre (NORMA Cyber) delivers a wide variety of cyber security services for its members, including intelligence, security operations and crisis response. More than 90 Nordic companies have joined in on the initiative.

Our inhouse intelligence team consist of capable analysts that leverage proven intelligence methodologies and an all-source approach to collect and analyse information. The team focus on threats that might impact the maritime sector and provide members with reports tailored to meet their information requirements. They also hold briefings and webinars, and maintain a database of indicators of compromise, which members can access.

This framework provides effective intelligence and information sharing to and from NORMA Cyber and its members, but it should also facilitate sharing between members directly. We strongly encourage members to share relevant data about potential threats detected in their systems.

For more information, please see www.normacyber.no

Intelligence & Sharing



Decision Support

- Effective information sharing to/ from members
- Monthly Threat Assessments
- Intelligence reports
- Tippers
- OT Vulnerability notifications
- Mitigation advice
- MISP portal – indicators of compromise sharing

Monitoring & Detection

External Monitoring

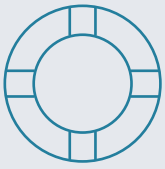
- Deep/dark web monitoring
- Vulnerability scanning of internet facing systems
- Warnings/Alerts

Security Operations Centre

- Vessel IT/OT infrastructure
- Land-based infrastructure
- Cloud infrastructure
- 24/7/365 - Early alerts

**Additional Service – extra cost*

Response



Member Support

- Mitigation advice
- Crisis response advice
- Coordination between members, authorities and other stakeholders
- Provide and manage recourses
- Participate in exercises and provide scenarios

- Available analysts
- Member portal
- Webinars and Seminars
- User Council

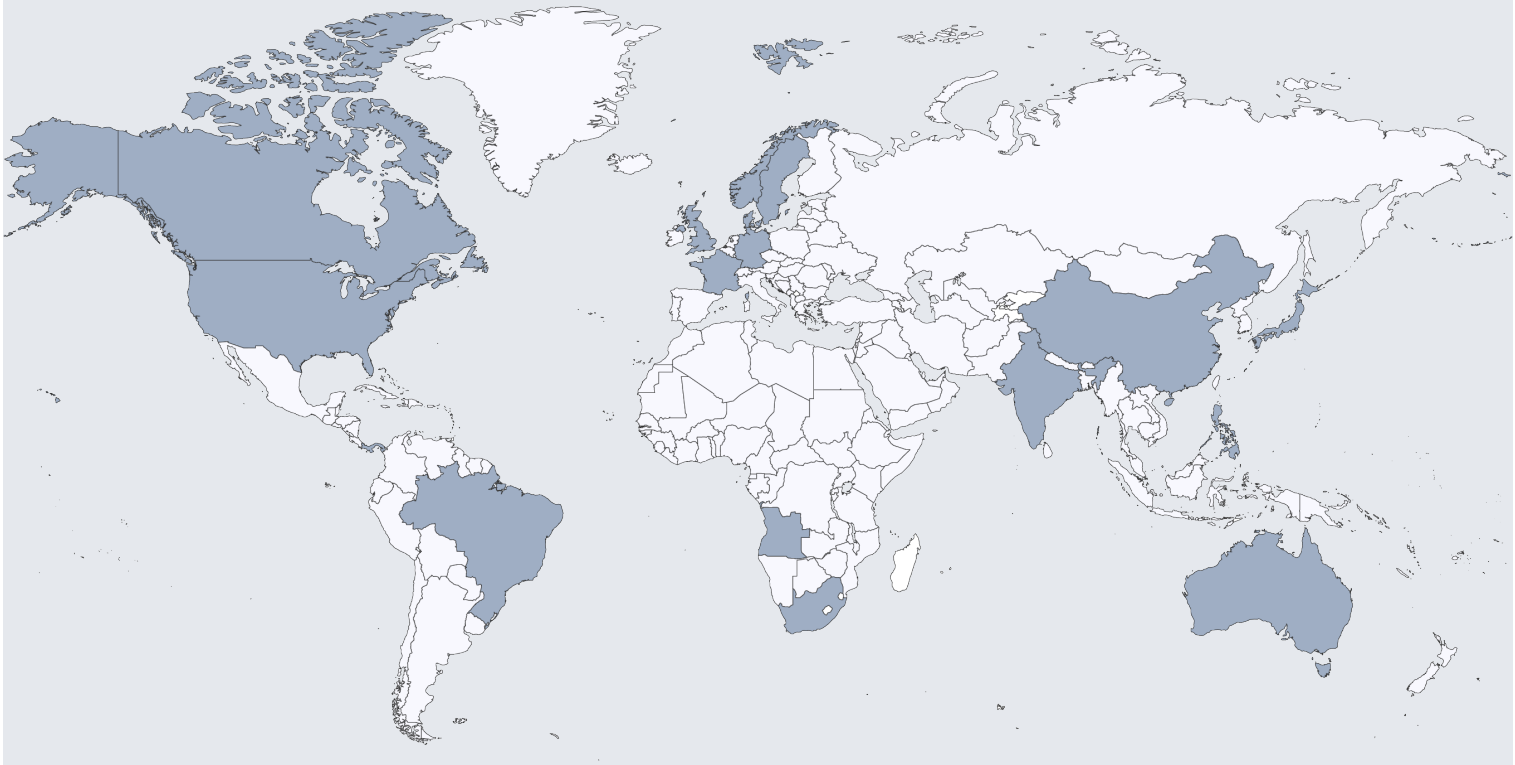
Security Operations Centre

What we do

The NORMA Cyber Managed SOC monitors members' systems 24/7. The SOC consists of technical solutions, competent personnel, and procedures to continuously monitor IT & OT systems, conduct analysis, respond to, and notify members when cybersecurity-related incidents are detected.

The NORMA Cyber SOC aims to monitor, detect, investigate, and respond to cyber incidents in our members' infrastructure. The SOC collects data from our members' land-based IT infrastructure, IT & OT infrastructure on vessels, and cloud services. This data is unified in our Security Information and Event Management (SIEM) system, which gives our SOC analysts a single-pane view of our members' security posture. NORMA Cyber follows a technology-agnostic approach when implementing new members into the SOC. The SOC tailors the services to each member's existing technology and infrastructure and is not committed to specific vendors.

The SOC performs threat hunting in close cooperation with the intelligence team. We proactively search for activity related to threat actors, specifically those known for targeting the maritime sector. Furthermore, the SOC regularly search for known indicators of compromise, such as file signatures for malicious files, domains tied to malicious activities or email addresses used in phishing campaigns, across all the collected data.



24/7 monitoring for **100** vessels and **4000** land-based staff in over **19** countries

Security Operations Centre, OT

Staying ahead of the game

The growing use of connected cyber-physical systems in ports and vessels creates an ever-expanding threat landscape, adding to the many challenges faced by the maritime industry. As a result, the need for risk management, asset visibility, and threat detection increases.

NORMA Cyber is dedicated to creating the next-generation converged IT\OT SOC. NORMA Cyber is building a security operations centre with our members and security solution vendors to monitor threats across IT and OT domains. Increased visibility improves threat intelligence and strengthens the incident response.

NORMA Cyber monitors several vessels' OT networks through our monitoring project. With our solution, we are able to:

- Identify assets and create detailed assets lists
- Identify vulnerabilities and continually evaluate risk
- Detect anomalies and threats
- Act on alerts and perform forensic analysis of events
- Scale up for the entire fleet

OT monitoring requirements
Two things are required to perform network security monitoring; a sensor which analyses traffic and a stream of network traffic to analyse. A sensor can be installed as a physical device or deployed virtually on existing hardware.

Network traffic can be sourced using either port mirroring or a network tap. Port mirroring, also known as port monitoring or SPAN (Switch Port Analyser), involves configuring a network switch to copy all traffic from one or more ports to another designated port for the sensor. Network taps are physical devices that are inserted inline on a network cable. They passively monitor and copy all network traffic passing them to the sensor.

Significance
Focusing purely on the maritime sector reduces the scope and makes it easier to become highly competent in the equipment and vendors used in our industry. This increases the success and professionalisation of subject matter experts within maritime OT, its vulnerabilities, and industry-specific requirements.

By leveraging network security monitoring, vulnerability management, and threat intelligence with automation and orchestration tools, NORMA Cyber streamline a cybersecurity solution designed for the maritime industry and coming regulations. As a next-generation SOC, a focus on developing and retaining skilled security personnel is essential for NORMA Cyber. This involves investing in training and development programs, creating career paths for security professionals, and developing a strong security culture within the organisation.

Sharing cyber event information with NORMA Cyber

Sharing cybersecurity information is essential to the collective defence and strengthening the cybersecurity within the maritime sector. NORMA Cyber encourage our members to voluntarily share information about cyber-related events that could help mitigate current or emerging cybersecurity threats. This also 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 this information to render assistance and provide a warning to prevent other members or entities from falling victim to a similar attack. 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 so we are able to take the 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 the victim of cybercrime or fraud.


Building unified resilience
against cyber threats for the
Norwergian Maritime Sector