



# NORMA CYBER

Annual  
Threat Assessment

2022



The Norwegian Maritime Cyber Resilience Centre - NORMA Cyber - is a joint effort between Den Norske Krigsforsikring for Skib (DNK) and the Norwegian Shipowners' Association and started operations in 2021.

The centre delivers centralised cyber security services to Norwegian ship-owners and other entities within the Norwegian maritime sector. NORMA Cyber aims to be the leading hub for operational cyber security efforts within the Norwegian maritime sector.

NORMA Cyber delivers a wide variety of cyber security services for its members including intelligence, security operations and crisis response.

Our experts work closely with security and emergency preparedness professionals in DNK and the Norwegian Shipowners' Association, both of which are headquartered in the same building. NORMA Cyber also collaborates with other relevant stakeholders such as the Norwegian authorities, other nations' authorities and other 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 first edition of our annual threat assessment. It comes at a time of great uncertainty with a full-scale war in Europe with serious long-lasting consequences for the global security order. As a result, many of our members have experienced significant complications in their operations. The situation is fluid, and the possible outcomes are challenging to predict.

The report gives an overview of the cyber security incidents impacting the maritime industry in 2021 and provides our assessments for 2022. It is exclusively focusing on the digital threats specific to maritime organisations and is meant to complement the threat assessments provided by Norwegian Government entities and other international bodies.

The Norwegian controlled fleet consists of more than 3 000 vessels from all segments and the wider Norwegian Maritime sector also consist of shipbuilders, ports, and various suppliers. The Norwegian maritime sector created values exceeding NOK 150 Bill. and employed more than 90 000 personnel in 2021.

Providing actionable, evidence-based knowledge is demanding during uncertain times, but we strongly believe that it is imperative that decision support is based on verified data and critical analysis.

Enjoy the read!

A handwritten signature in black ink, appearing to read 'Lars Benjamin Vold'.

Lars Benjamin Vold  
*Managing Director*  
Norwegian Maritime Cyber Resilience Centre

# Nation State Threats

## *Espionage*

**The Norwegian controlled merchant fleet is the fourth largest in the world and operate within all segments. The fleet is one of the most modern in the world and the Norwegian maritime sector is a driving force within decarbonisation with future propulsion systems, carbon neutral ships, as well as modern offshore wind solutions.**

The vessels operate in areas of strategic geopolitical importance, like the High North, the Persian Gulf / Arabian Gulf, and the South China Sea. The High North plays a key role in the Russian bastion defense, and China have stated they want to expand their territorial control in the South China Sea. This makes Norwegian maritime sector an attractive intelligence target for nation state threat actors. As an example, it is a stated aim for China to become technologically independent of the West and dominant in emerging technologies.

The Norwegian Intelligence Service and the Police Security Service continue to assess that Russia and China are the most prominent threats to Norwegian interests. In their annual threat assessments for 2022, they highlight the high espionage threat from Russia and China, particularly to organisations working on foreign, defence and security policy, as well as organisations within research and development activities in sectors related to health, defence, petroleum, space and maritime technology.

We assess that Russia-and China-linked threat actors pose a high espionage threat to ship-owners involved in transportation of strategic or sensitive goods, and organisations involved in projects related to critical national infrastructure, energy, or oil and gas.

For example, an AIS track from the Norwegian Coastal Administration shows how the Russian research vessel "Akademik Lazarev" systematically followed pipelines and cables from various Norwegian and British installations and landing sites in 2020-2021.

Nation state actors will likely perform both human intelligence operations as well as open source intelligence operations as part of their initial reconnaissance before conducting

network operations on target organisations. Organisations web sites can provide valuable information about projects and technology as well as details on key personnel, that can be exploited in network operations later.

Nation state threat actors may use a wide range of tactics in their network operations, including brute-force attacks on login services, phishing attacks to fraudulently collect usernames and passwords, spearphishing emails with malicious attachments or links to malicious sites, exploitation of vulnerabilities in internet exposed services or devices, or through supply chain attacks.

Some of the most advanced network operations linked to nation state actors in 2021 involved supply chain attacks or exploitation of vulnerabilities in internet-facing servers.



# Nation State Threats

Supply chain attacks exploit trust relationships between an organisation and external parties. These relationships could include partnerships, vendor relationships, or third-party software. Threat actors will compromise one organisation and then move up the supply chain, taking advantage of these trusted relationships to reach their objective.

### Supply Chain Attacks

In December 2020, the US CISA alerted about an advanced persistent threat actor that had compromised US government agencies, critical infrastructure entities, and private sector organisations through a supply chain attack involving Solarwinds Orion management software. The exact extent of the attack will probably never be known to the public, but the network operation exposed over 18.000 potential victims worldwide, but the threat actor likely only exploited a few victims in highly targeted espionage operations. The US government later attributed this attack to the Russian Foreign Intelligence Service.

Another advanced supply chain attack was reported during the outbreak of the war in Ukraine. An attack on Viasat KA-SAT impacted satellite-based internet communication in Europe. A likely Russia-linked threat actor targeted a Viasat network management partner, exploiting the supply chain to attack the satellite modems. Tens of thousands of active satellite modems dropped off the network and did not attempt to re-connect. The attack primarily impacted modems in Ukraine, and was likely targeting military satellite communication systems. However, it affected a number of modems in Europe, including 5800 Enercon wind turbines in Germany. KA-band satellite communication is rare on vessels, and the attack did not impact maritime SATCOM.

### Exploitation of Vulnerabilities

Vulnerabilities in on-premises Microsoft Exchange have been extensively exploited by nation state threat actors in 2021.

In March 2021, Microsoft released security updates for several vulnerabilities in Microsoft Exchange Server (named ProxyLogon) after de-

tecting multiple zero-day exploits being used to attack on-premises installations in limited and targeted attacks. In the attacks, the threat actor used these vulnerabilities to access email accounts and allow the installation of additional malware to facilitate long-term access to victims' networks.

Microsoft Threat Intelligence Center attributed the campaign to a group assessed to be state-sponsored and operating out of China (named HAFNIUM by Microsoft). The attacks were later attributed by the US government to the Ministry of State Security (MSS) in the People's Republic of China. In July 2021, the US Department of Justice announced criminal charges against four MSS hackers addressing activities concerning a multi-year campaign targeting foreign governments and entities in key sectors, including maritime, aviation, defence, education, and healthcare in at least a dozen countries.

Two weeks after the security patches were released, more than 82.000 internet-facing Microsoft Exchange Servers were still vulnerable to ProxyLogon attacks, and other threat actors, both cybercriminals and nation state, began exploiting the vulnerabilities. 172 Norwegian Exchange Servers were identified to be vulnerable to the ProxyLogon attack, and several organisations were compromised, including one Norwegian shipowner.

In July 2021, Microsoft disclosed three new critical vulnerabilities in Microsoft Exchange Server that were later named ProxyShell, and these vulnerabilities were quickly being exploited by several threat actors, including one ransomware group.

Vulnerabilities in VPN and remote access solutions have also been extensively exploited by nation state threat actors in 2021.



# Regional Conflicts

## Impact on Merchant Shipping

**The Norwegian merchant fleet is operating in areas of strategic geopolitical importance, like the High North, the Persian Gulf / Arabian Gulf, and in the South China Sea.**

Historically there has been significant reporting of destructive cyber operations around the Persian Gulf / Arabian Gulf. There is an ongoing covert cyberwar between Iran and US / Israel. Threat actors have targeted critical national infrastructure in Israel, including systems related to water supply. On the Iranian side, ports, fuel systems, and railway control have been subject to cyber attacks.

Open sources reported on Iran-linked cyber espionage operations targeting US and Israeli defence technology companies, Persian Gulf ports of entry, and global maritime transportation companies with business presence in the Middle East, in October 2021.

Iran-linked threat actors have previously targeted maritime organisations and port infrastructure in Kuwait, likely to gain an insight into the transport of goods, particularly those related to military supply chains. Similarly, major ports in Dubai and the UAE likely present strategic intelligence gathering targets for Iran, given their proximity to Iranian territory and role in facilitating the transport of strategic goods.

We assess that the maritime sector is not a primary target for Iran-linked cyber espionage or destructive operations, however, vessels operating in the area can unintentionally become a target.

China wants to expand its territorial control in the South China Sea and open source reports from December 2021, reported on China-linked cyber espionage operations in the South China Sea, where a threat actor had compromised

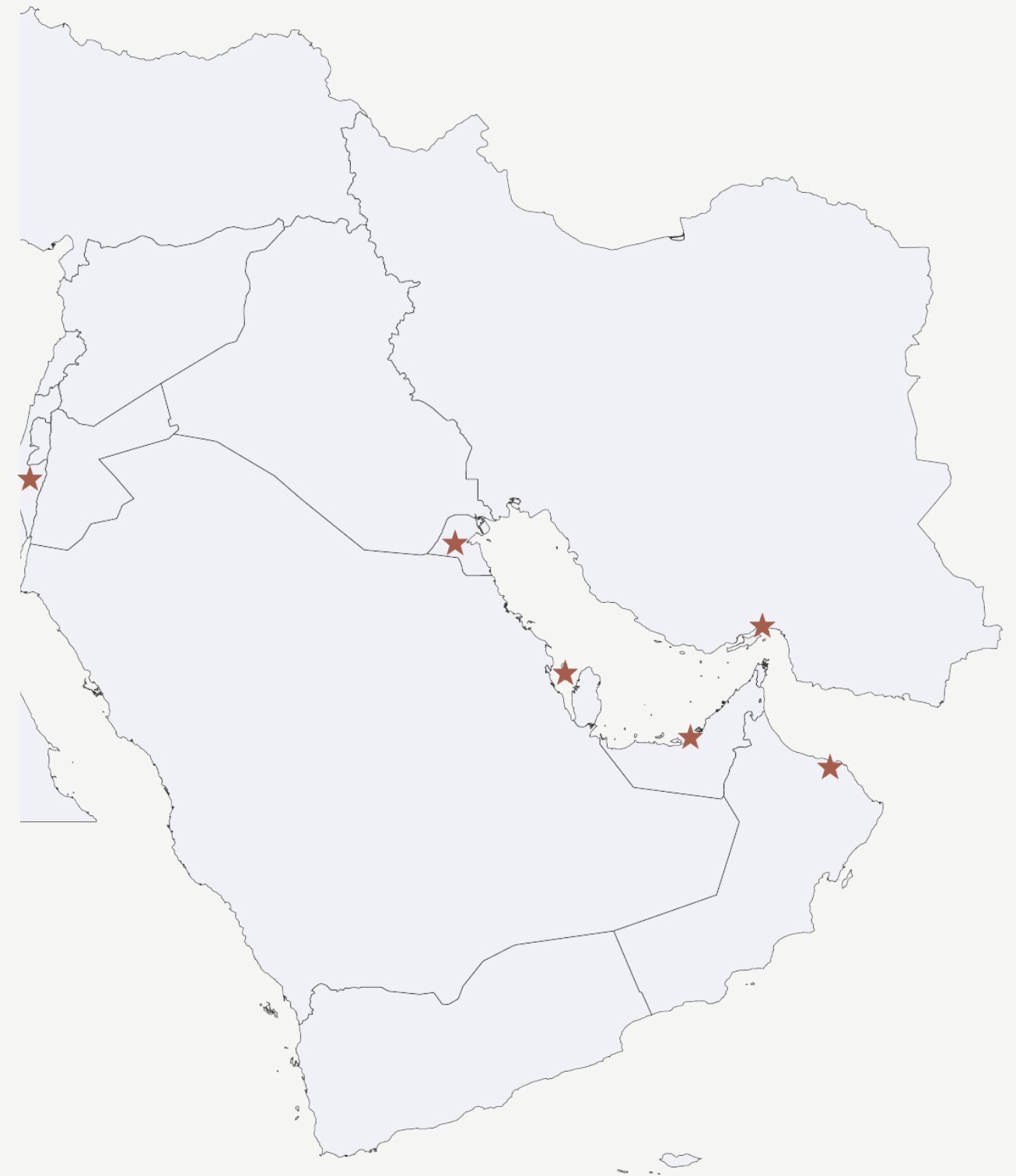
several high-profile military and government organisations across Southeast Asia throughout 2021. The activity included the targeting of Sihanoukville Autonomous Port (PAS), the main deep sea port of Cambodia. The targeting of PAS is likely linked to China's wider strategic objectives under the Belt and Road initiative, as PAS has a high strategic significance given its location along the Maritime Silk Road route.

Open sources reported in February 2021 that a China-linked threat actor had targeted critical infrastructure in India amid heightened border tension. The primary targets in the campaign included power sector organisations and regional load despatch centres responsible for the operation of the power grid. The ports of Mumbai and Chidambaranar were reportedly targeted, but we have not received any reports that this impacted vessels operating in the area.

If China-linked threat actors were responsible for the power outage in Mumbai, and if this is linked to the other publicly reported intrusions across Indian utilities and maritime ports, it reflects a significant shift in China's willingness to leverage disruptive malware against critical national infrastructure (CNI) targets for tactical and strategic signalling purposes. China highly likely retains the technical capabilities to conduct such operations but has to date, unlike Russia, Iran, Israel, and the US, refrained from leveraging these in disputes or political tensions.

We assess that nation state threat actors have identified maritime ports as strategic CNI targets whose disruption can demonstrate a significant signal to an adversary state.

30 to 50 Norwegian owned ships are operating in the Persian Gulf / Arabian Gulf at any given time.



★ = Maritime targets around the Persian Gulf / Arabian Gulf



# GNSS Interference

## Spoofting and Jamming

**Instances of significant GNSS interference have been reported worldwide in 2021. This interference can result in lost or inaccurate GNSS signals affecting bridge navigation, GNSS-based timing, and communications equipment (including satellite communications equipment).**

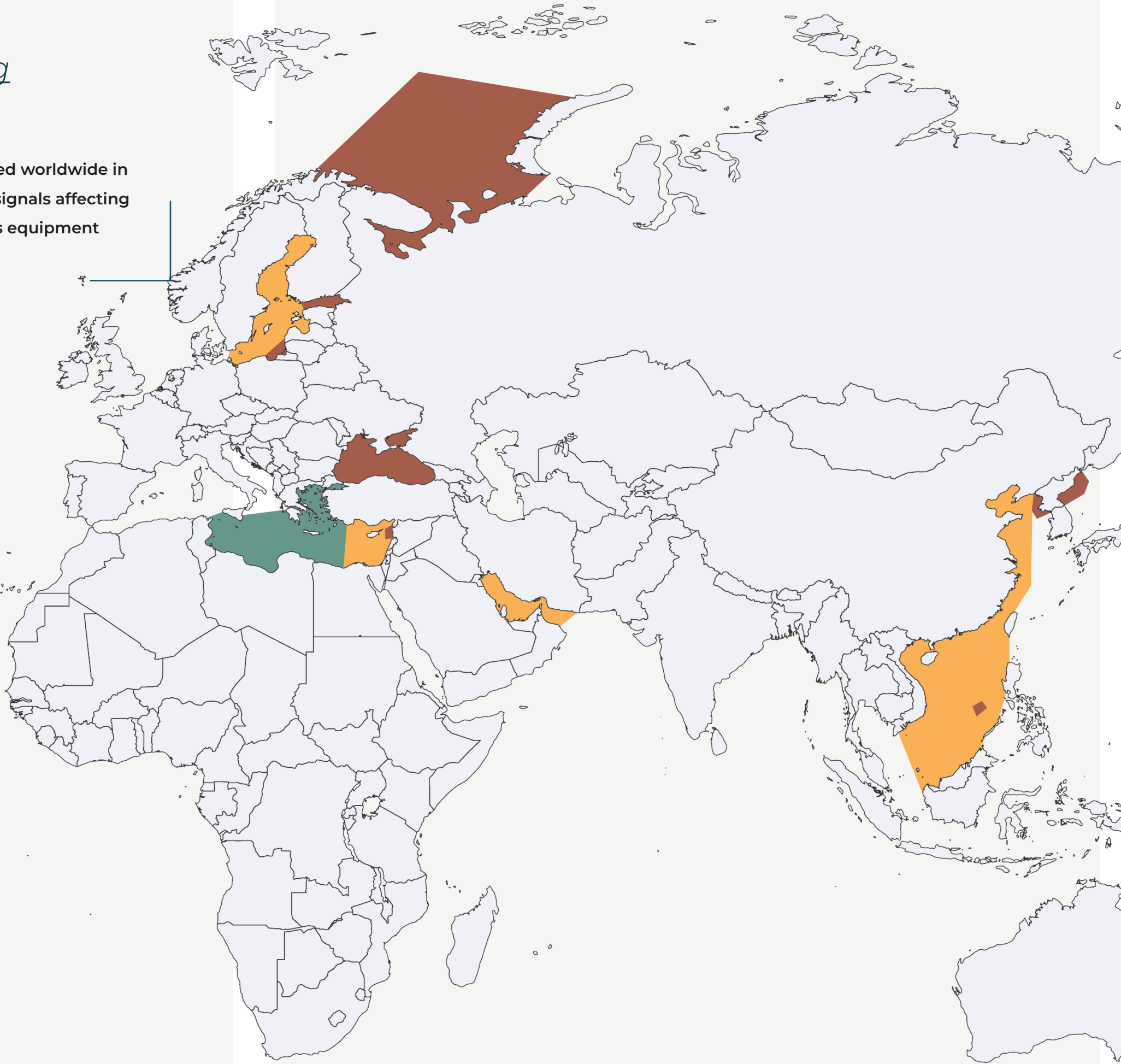
Multiple instances of GNSS interference have been reported in the Baltic Sea, the Black Sea, the eastern and central Mediterranean Sea, specifically in the vicinity of the Suez Canal, Cyprus, Malta, and Istanbul, in the Red Sea / Gulf of Aden, and off the coast of Brazil.

Jamming of GNSS signals requires relatively basic technology, and the general availability of equipment makes these tactics also used by criminal groups and insurgents, particularly over short ranges. Instances of GNSS interference off the coast of Brazil are likely conducted by criminals.

Spoofting of GNSS signals is more complex and is primarily conducted by nation state actors.

Russia has been known to use GNSS spoofing or jamming for the protection of VIPs, strategic facilities, in armed conflicts and military exercises. Other nation states such as North Korea, China and Iran are also possess these capabilities and use these tactics to protect key strategic areas, in harbours or during military exercises.

We assess that this activity will likely continue in 2022. In the Barents Sea and Baltic Sea GNSS interference is more likely to occur during NATO or Russian military exercises.



# AIS Data Manipulation

## in Vessel Tracking Services

**There were several reports of fake AIS data in vessel tracking services last year, particularly in the Black Sea and the Baltic Sea. In all the incidents, the fake data was ingested directly into the vessel tracking service. Considerable care had been taken to produce plausible tracks and the data had been carefully crafted to bypass mitigations implemented in the vessel tracking services.**

In February 2021, the AIS track of nine vessels from the Swedish Navy was manipulated to make it appear that they consecutively left the naval base in Karlskrona late in the evening and sailed south into the Baltic Sea.

In June 2021, the AIS track of two Norwegian Navy corvettes was manipulated to make it appear that the vessels were sailing from Gdynia in Poland and into Russian territorial waters outside the Russian enclave of Kaliningrad.

In September 2021, the AIS tracks of the Russian WARSHIP 545 (a Steregushchiy-class corvette) were manipulated to make it appear that it was sailing from the Russian Baltic Fleet's main naval base in Baltiysk and into Lithuanian territorial waters outside Klaipeda.

The most recent incident was outside Skagen in Denmark in November 2021. Less than three days after the Danish authorities arrested the Russian research vessel Akademik Ioffe on 1 November 2021, a fake AIS track of the Russian WARSHIP 545 appeared. The track displayed WARSHIP 545 approaching the north coast of Denmark, and continuing to sail along the coast of Skagen, well within Danish territorial waters.

In the Klaipeda incident, the fake AIS track was also reported on a fake news site under the headline "Dangerous deception over Russian warships near Klaipeda: there has never been such a provocation against Lithuania".

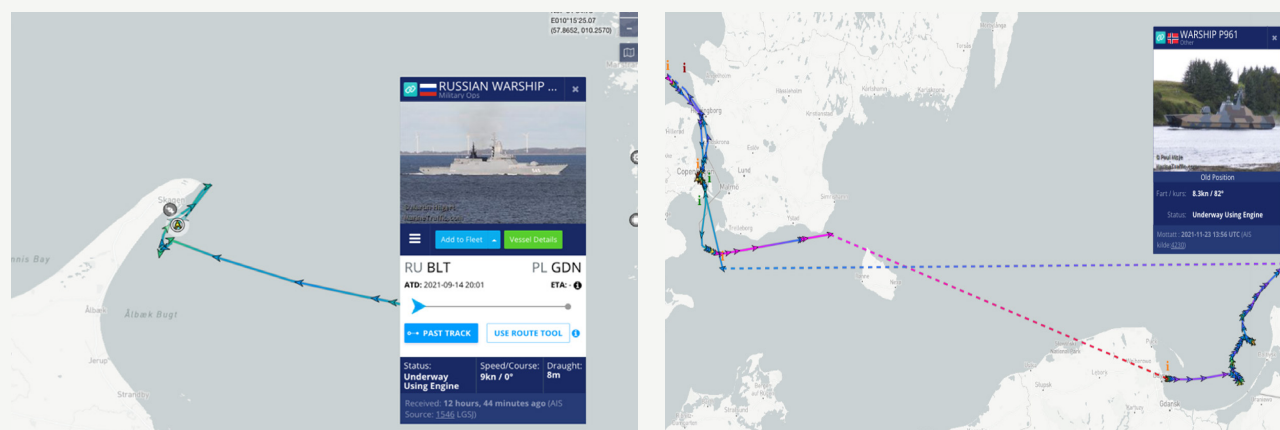
Another incident related to fake AIS tracks occurred in the Black Sea in June 2021, where the AIS track of two NATO vessels was manipulated to make the vessels appear to be outside the Russian naval base in Sevastopol in Crimea, while the vessels were at port in Odesa.

Deliberate manipulation of AIS data in vessel tracking services can serve several purposes. In the case of confrontations at sea, it can be used to cast doubt on who has been where, or as a basis for an accusation of violations of territorial waters. It can also be used as signalling.

The threat actor behind these incidents is unknown, but we assess that particularly the Russian military is continuing to develop and practice the implementation of electronic warfare technologies, focusing on military targets, using traditional GNSS spoofing or jamming techniques; however, these incidents show that vessel tracking services used by commercial or civilian users are also being targeted.

The reported fake AIS data is highly likely a form of information warfare and does not constitute a threat to safe operations of merchant shipping. Nonetheless, AIS data manipulation can have severe legal and financial implications for Norwegian ship-owners if vessels' AIS data is deliberately or accidentally moved into sanctioned areas, since many sanction checking services use AIS data as one of their main sources.

We assess that this activity will likely continue in 2022, particular in the Baltic Sea and the Black Sea, especially during NATO or Russian military exercises.





# Cybercrime

## Gaining Access

The cybercriminal ecosystem is expanding and becoming more professional. Cybercriminal entities will highly likely continue the development towards more specialised roles, enabling effective and increasingly sophisticated operations. One fast-growing, prominent role is that of access brokers.

The number of access brokers has more than doubled between 2021 and 2022 – a trend which is expected to persist. Access brokers monetise by gaining access to companies or services and selling it.

Phishing is one of the primary methods used by criminal threat actors to obtain access to organisations. NORMA Cyber continues to observe phishing campaigns with a maritime theme, often related to port arrival and departure. In addition to this, generic campaigns and phishes related to current events are plentiful. Through 2021, we saw that the most effective phishing emails were those that were sent from the email addresses of a compromised partner. Broadley put; we deduct three fundamental goals with the surveyed phishing campaigns: malware delivery, credential harvesting, or business email compromise.

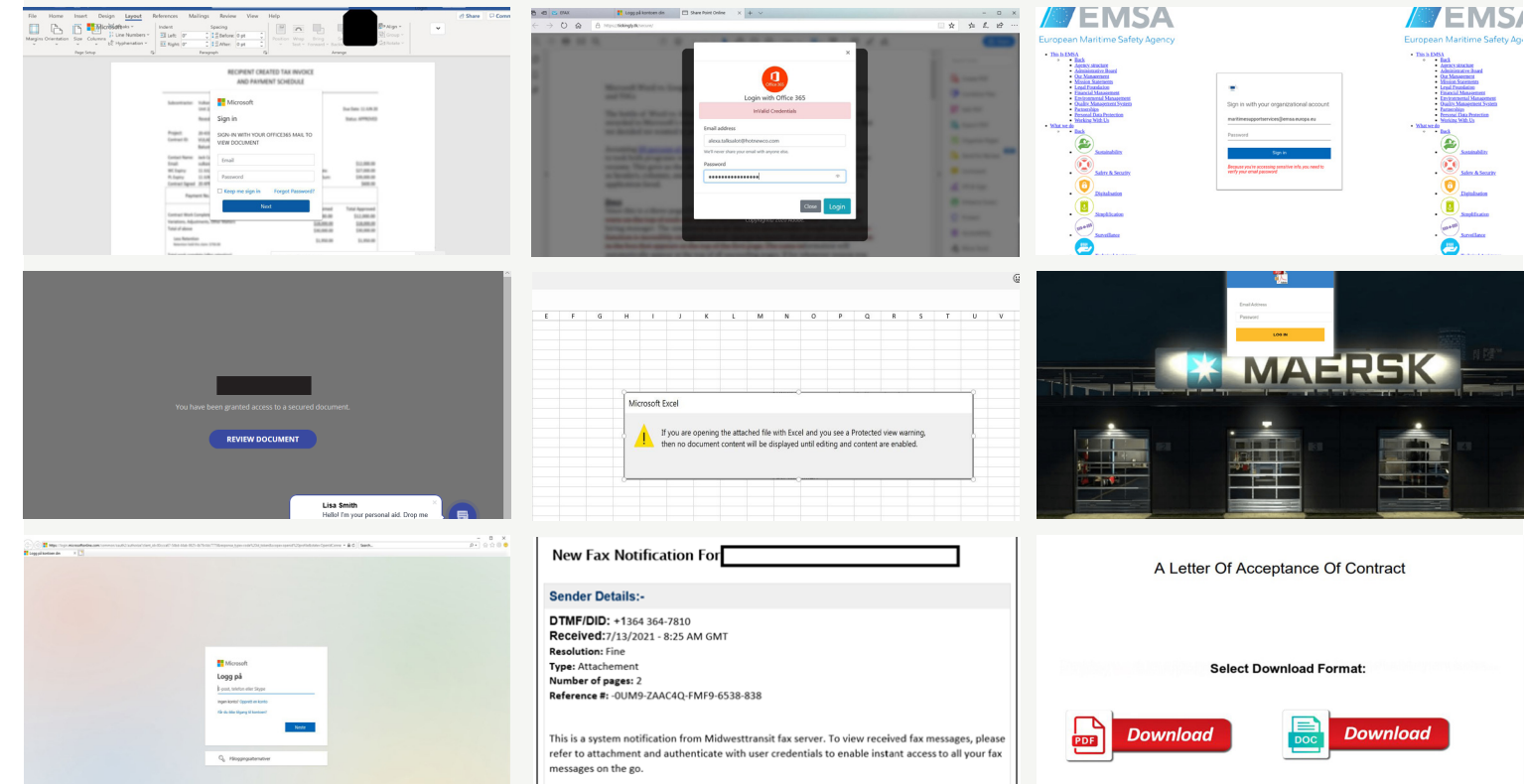
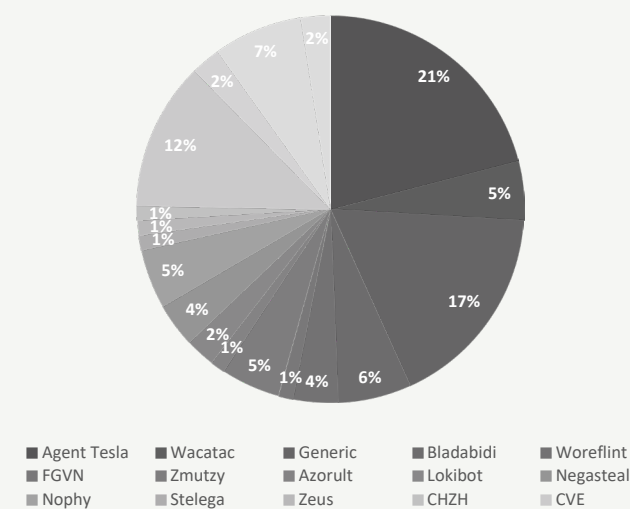
### Malware Delivery

In the coming year, we will likely see the continued development of malware used in the first phases of a compromise. The general goal of initial stage malware is to function as a door into the victim system and exchange information from the victim system to the attacker's infrastructure. Remote Access Trojans, loaders, beacons, and information stealers fall within this category. The most popular malware families in this category are modular with many functions embedded. Threat actors will likely continue to add functionalities and stealth to prominent malware families such as Emotet, QakBot, and BazarLoader. In addition to established malware families, new one continues to be developed and offered for cheap lease, packed with automation and

user-friendly interfaces. We expect to see multiple malware families incorporated into the same campaigns as they have different strengths, and successful deployment of multiple strains increases their persistence on the system.

Between April and December 2021, our monitoring alerted about 216 maritime-themed email phishing campaigns attempting to deliver malware.

**216** Trojanised phishing campaigns April – December 2021



Selection of phishing attempts discovered in 2021.

### Credential Harvesting

The methods applied by threat actors to steal credentials keep evolving, but two approaches we observe frequently are email leading to a website with a fake login prompt and information-stealing malware. In corporate settings, the former appears more frequently. These campaigns routinely start with an email containing a link to a document or service. Since these scams rarely contain any malicious programs, the lures often go under the radar of security mechanisms such as Anti-Virus. Upon clicking the lure, the victim is taken to a web page designed to mimic that of a known service and told that to view the shared contents, the victim must authenticate themselves. Information written into such login forms is often automatically vetted and then sent to the attackers. Multifactor authentication mechanisms are elemental in reducing the risk from such attacks, but threat actors will likely evolve their strategies to include techniques to overcome authentication obstacles.

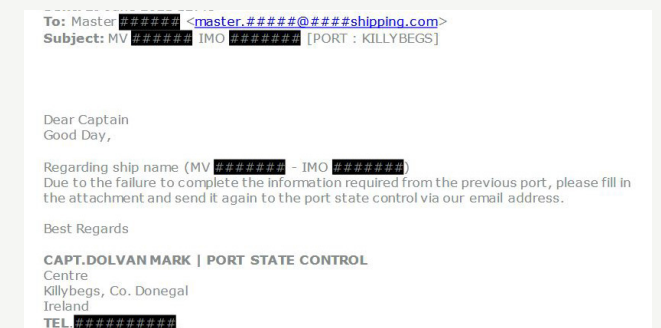
Information stealers are malware that obtain saved credentials and other sensitive information from infected devices and send them in bulk to the attackers. Unlike credential harvesting pages, these generally appear to stem from personal devices.

We assess that credential harvesting, particularly by using well-crafted fake login pages, will increasingly be part of the cyber threat landscape in 2022.

### Inmarsat C Phishing

In 2021, we also identified three Inmarsat C messages, where an unknown threat actor used Inmarsat messages to phish for email addresses, vessel, and crew details. Topics of the messages were related to IMO documents ("IMO General Declaration", "Document of Compliance" and "Safety Management Certificate"), Covid-19 status onboard, and crew lists.

**3** Phishing campaigns over Inmarsat C



We assess that an unknown threat actor has been collecting vessel and crew details, including email addresses to vessels since at least April 2019. The intent is currently unknown, but the email addresses can likely be used for further spear-phishing attacks with malicious attachments or links. Inmarsat C phishing campaigns are likely to occur at low frequencies through 2022.

## Fraud

**Business Email Compromise (BEC) and similar scams use social engineering to manipulate target organisations to send funds to actor-controlled accounts, often in the guise of official transactions. BEC attacks tend to be profitable and do not require advanced technical skills.**

In 2021, several maritime organisations were targeted by criminals impersonating trusted suppliers and partners, seeking to monetise on false invoices. By compromising the email accounts of both the company and a vendor, the criminals were able to craft email threads that appeared authentic, increasing the chance of the victim company believing the lure. Due to the low operational cost and availability of eligible targets, BEC and wire-fraud campaigns continue to pose a high threat to maritime organisations.

of 3.9 million USD in total. Our analysis showed that the perpetrators were Nigerian criminals operating out of Lagos.

Nigeria has an extensive history of cybercrime, which traditionally has been focused on low-sophistication but high volume fraud campaigns. The most prominent groups concentrate on BEC operations and have been known to target industrial organisations, particularly those in the extractive industry. Law enforcement actions towards these groups has had low deterrence success.

### Common clues to look for:

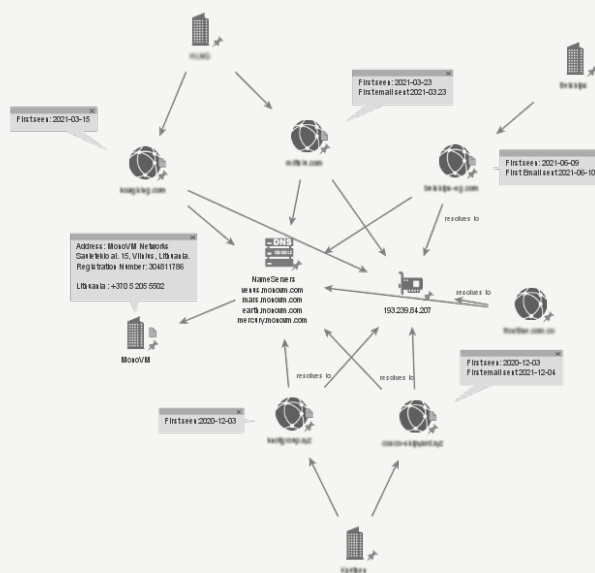
1. Typosquatted/misspelled domains
2. New email archiving or forwarding rules
3. Personas with authority that asks for urgent transactions
4. Sudden change of banking information

In the most elaborate scheme analysed by NORMA Cyber, the criminals compromised email accounts belonging to several members who had a business relationship and created typosquatted domains mimicking each entity. They blended in and hid by hijacking the email thread and creating rules that archived legitimate emails upon arrival. Using false invoices, the criminals tried to elicit a payment

# 3.9

Million USD

Fraudsters tried to elicit at least 3.9 million USD from NORMA Cyber members and their partners between December 2020 and June 2021 through BEC campaigns. They were mostly detected.



## Ransomware

**Ransomware and extortive campaigns will continue to pose a high threat to maritime organisations in 2022. The most prominent ransomware groups combine ransomware with data leak extortion, as the loss of sensitive data is perceived to increase the incentive to pay. Internet-connected IT systems face the highest threat.**

Ransomware – malware that encrypts files on a computer system – is commonly deployed on the victim system as the last step in a multi-faceted attack. Ransomware operations have transitioned from a “spray and pray” tactic to more targeted operations. 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 constantly 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. It is not only the ransom demand itself that leads to high costs; downtime, broken equipment, time spent on incident management, and a potential loss of reputation are all factors that contribute to significant economic losses.

### Law Enforcement

Throughout 2021, law enforcement agencies raided and arrested multiple cybercriminal groups operating in the malware domain. Arrestations affected several notorious ransomware groups and their affiliates. Arrestations were carried out worldwide, Eastern European countries stood out as a key area. Moreover, in January 2022, the Russian Federation's Federal Security Service announced the arrest of individuals allegedly associated with Pinchy Spider's REvil Ransomware-as-a-Service. This is the first known instance of Russia arresting ransomware operators.

The amount of profiled ransomware attacks in 2021 likely led to and aided the increase in law enforcement actions. Although ransomware remains a global concern in 2022, it is unlikely that we will see the same amount of successful arrestations in the coming year due to the ongoing war in Europe. However, ransomware groups continue their high attack frequency.

### Virtualisation

Virtualisation infrastructure is a lucrative target for ransomware groups. Several threat actors were observed targeting services such as VM-Ware vCenter, hereunder the ESXi and vSphere platforms. If successful, these platforms allow the threat actors to attack multiple virtual machines at once, improving the speed of their operation. In 2021, several ransomware groups developed Linux versions of their ransomware, some configured specifically to target ESXi hosts. A common technique to gain access to the virtual environment is to use administrator credentials to log in to vCenter and then enable SSH to permit persistent access. Threat actors will likely continue to explore methods to compromise virtualisation infrastructure.



Images: National Police of Ukraine



# Ransomware in 2021

Known successful attacks towards the maritime sector



# Common Stages of an Attack

Typical events observed in ransomware intrusions

A threat actor gains access to the system. Popular means are phishing, credential harvesting, or using exploits. Sometimes adversaries use multiple attempts to succeed. Many ransomware groups often outsource this activity to specialised access brokers.



Threat actors exfiltrate the data they want to leverage in the negotiation process.



The operability of a computer system post-ransomware depends on the ransomware used as well as affected services. Nonetheless, at this stage, it is all about incident response and deciding what needs to be done next. Having a pre-defined and rehearsed action plan is crucial.



The threat actors responsible for delivering the final blow start mapping out the environment. This includes gaining additional privileges (if necessary), locating sensitive files, disabling security mechanisms, and deciding which systems to target.



Once ready, the threat actors download the ransomware and execute it how they see fit. The binaries used are often freshly compiled for the specific victim.

# Hactivism

## Cyber Activists

**Cyber activists, commonly referred to as hacktivists, are persons who carry out cyberattacks in support of a cause. One of the key pillars of activism is to promote an opinion in a way that the opposition and the public cannot ignore. This is traditionally done through vigorous campaigning.**

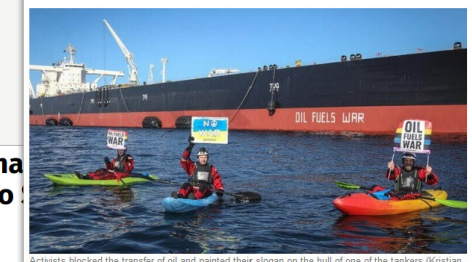
Hactivists use cyberspace to make their point known in some coordinated operations, but signalling in cyberspace have some disadvantages and limitations. It requires some technical skills, it can be easily ignored, and it seldomly has a deterring or hindering effect. Commonly used attack methods are website defacement, Distributed Denial-of-Service (DDoS) attacks, and leaking data. Many of the tactics are considered illegal in substantial parts of the world.

We continue to assess that the hacktivist threat to the maritime sector is low. A significant shift in the public perception of the maritime sector, particularly around issues such as the environment, would result in a likely targeting of the sector by activist groups, but we have yet to see environmentalists resort to cyber attacks. Onshore and offshore assets of maritime organisations operating in geopolitically sensitive regions likely continue to face inadvertent threats from patriotic hacktivist groups, whose pace of operations will be heightened during diplomatic disputes and military confrontations.

### Hactivism and the war

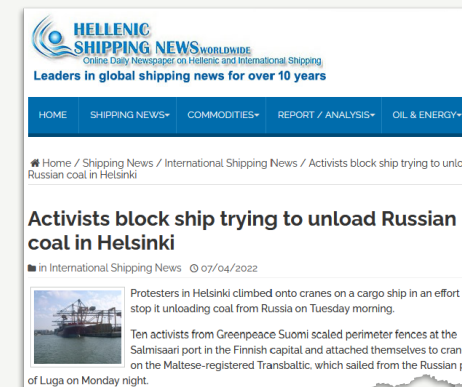
Since the Russian war against Ukraine started, individuals and groups on both sides of the conflict have attempted to disrupt and compromise services and assets belonging to the opposing party. The hacktivists boasted on social media platforms such as Twitter and Telegram about breaching significant entities on the opposing side. Although loud, most of the claims go unverified and the actual impact is difficult to assess. Supporting the combatants by launching whatever attack possible on the rivalling side has been somewhat romanticized by media and patriotic computer literals. However, the hacktivist commitment is expected to decrease as the conflict drags on. Maritime organisations with a strong presence in Ukraine, Russia, the Black Sea, and the Sea of Azov likely face a moderate threat for inadvertent inconveniences caused by hacktivist groups.

### Greenpeace Blocks Transshipment of Russian Oil in Denmark

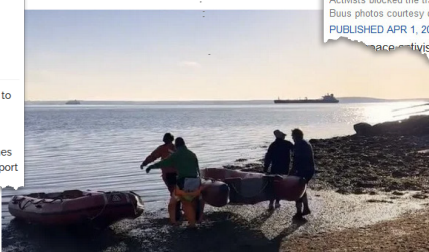


Activists blocked the transfer of oil and painted their slogan on the hull of one of the tankers (Krisitan Bias photos courtesy of Greenpeace)

PUBLISHED APR 1, 2022 5:31 PM BY THE MARITIME EXECUTIVE



### Greenpeace Activists Chain themselves to Tanker to Stop Russian Oil



Greenpeace activists set out to block a tanker waiting offshore with a cargo of Russian jetfuel (Greenpeace)

PUBLISHED APR 25, 2022 2:22 PM BY THE MARITIME EXECUTIVE

In possibly their most daring protest yet against Russian oil, activists from Greenpeace Norway along with the Extinction Rebellion chained themselves to a

### Extinction Rebellion plans to protest arrival of first cruise ship in Victoria



More than 100 protesters are expected to make a statement



# Operational Technology

## State-backed OT threats

Malware continues to pose a threat to operational technology (OT) either by affecting them directly, or through indirect implications such as forcing a victim to shut down OT because of an attack towards IT.

We divide malware that poses a risk to OT systems into three categories based on the perceived attacker motivation: destructive, espionage, and financial gain. Malware designed to aid in destructive attacks and espionage campaigns tends to be developed by nation state threat actors, whereas cybercriminals construct malware used for monetization.

There are no known reported events where OT has been compromised in the maritime sector in the last year. At the start of 2022, there has been a shift in the threat to control systems.

Seven known malware strains are tailormade for industrial control systems, four of those are designed to **disrupt or damage**:



**Stuxnet** disrupted Iranian uranium enrichment at Natanz, destroying more than 3000 centrifuges. Discovered in 2010, assumed developed in 2006.



**Crashoverride/Industroyer** is OT malware used to disrupt Ukrainian Energy in 2016. It utilised several OT specific payloads, and an updated version of the malware - named Industroyer 2 - was recently used in the unsuccessful 2022 attack against Ukrainian Energy.



**Trisis/Triton** targeted the safety instrumented systems (SIS) and caused a plant shutdown in Saudi Arabia in 2017. It was designed to target human life, but the attack failed and caused a shutdown of the plant.



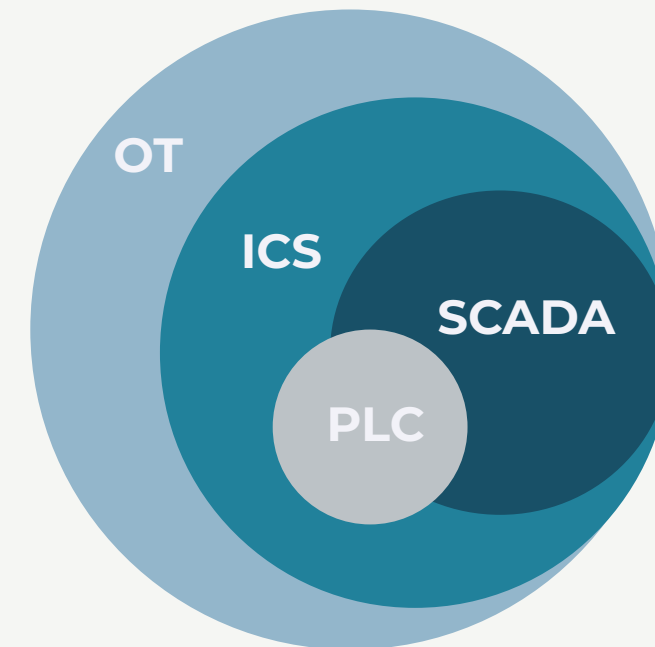
**Pipedream** is the fourth disruptive malware. It was reported to the public by the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and NSA in April 2022. CISA warned of an advanced persistent threat campaign with the ability to gain full system access to multiple industrial control systems. Pipedream and its framework are designed to disrupt or damage industrial control systems, marking yet a significant change in the threat landscape. Although it is likely the work of a state actor, the modular malware reportedly comes with a console which allows a less sophisticated adversary to use the toolset.

The current iteration of the Pipedream framework targets Schneider Electric and Omron PLCs - all are type approved and can be found in the maritime industry. The toolset does not exploit any vulnerabilities to compromise target systems. Instead, it communicates and interacts with Modbus and Codesys, two common industrial protocols. The toolset can reportedly be modified to target other vendors and equipment.

Pipedream has not been observed deployed in the wild, it was discovered by threat researchers before the threat actor was able to launch an attack. Details about the discovery is currently scarce.

# Operational Technology

Different communities use different terms describing computing systems involved in physical operations. Examples of such systems are intergrated alarm, control and monitoring systems, propulsion control, and dynamic positioning systems. We use the terms operational technology (OT) and industrial control systems (ICS) interchangeably.



There are two notable malware families used for **reconnaissance and operational technology espionage**:



**BlackEnergy** was originally used for distributed denial-of-service attacks and malware deployment by cybercriminals. The infamous Russian threat actor Sandworm repurposed BlackEnergy and used it in several attacks. The 2015 cyber attack on Ukrainian power company Prykarpattya Oblenergo is the most recognized. The attack triggered a six-hour blackout and knocked 30 substations offline. BlackEnergy2 and BlackEnergy3 never had an attack capability, they are used as an espionage toolkit.



**Havex** is an older remote access trojan used in espionage campaigns. It is modular and contains plugins to detect network activity using the OPC protocol and to gather information on common OT ports. The malware was delivered in several ways: phishing, waterhole attacks, and was even found embedded in installers. Havex infected more than 2800 victims.

# Operational Technology

## Financial Gain

**No known financially motivated groups specifically target OT environments. 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.**

Several major cyberattacks impacted OT operations over the past twelve months. In all publicly-reported incidents where ransomware directly disrupted OT networks, the affected devices were running on the Windows OS. Reportedly, these attacks did not directly disrupt lowerlevel industrial equipment. Still organisations chose to shut down their OT environments as a precaution

An example of this is the ransomware attack on the Colonial Pipeline Company. They proactively shut down its pipeline system as a safety precaution, which lead to a temporary gas shortage and panic buying of fuel. Shortly after, JBS Foods had their server systems encrypted by another ransomware group, leading them to power off some production systems.

Three known ransomware attacks affected OT in maritime organisations. One ransomware group disrupted the terminal operating system of several African ports in 2021, and in January 2022 port terminals in Germany, Belgium, and the Netherlands were forced to run at a limited capacity following two separate attacks.

Internet-connected OT networks may also be tempting targets for less sophisticated criminals focusing on mining crypto currencies. Many OT networks have significant up-times, which is favourable to coin mining.

Maritime organisations are attractive targets to cybercriminals for multiple reasons:

- ◆ The large and distributed nature of the maritime sector provide adversaries of all types with a large attack surface.
- ◆ Organisations with physical or critical operations traditionally have a low tolerance for down time and therefore are more likely to pay a ransom demand.
- ◆ Organisations with physical operations, particularly in segments such as oil & gas, manufacturing, and technology, are commonly perceived to have high revenues and therefore also able to pay a higher ransom.

OT operations may be impaired by criminals targeting organisations, particularly if malware is released on an improperly segmented and flat network.

# Operational Technology

## 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 1 OT related intelligence report, 49 vulnerability notifications consisting of 458 individual vulnerabilities. The vulnerability reporting criteria is 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 that are used in the maritime industry.

The chart shows that sizable vendors such as Siemens, Schneider Electric, and Mitsubishi are represented with high number of reported vulnerabilities. There are two reasons for this. Firstly, they have an extensive equipment

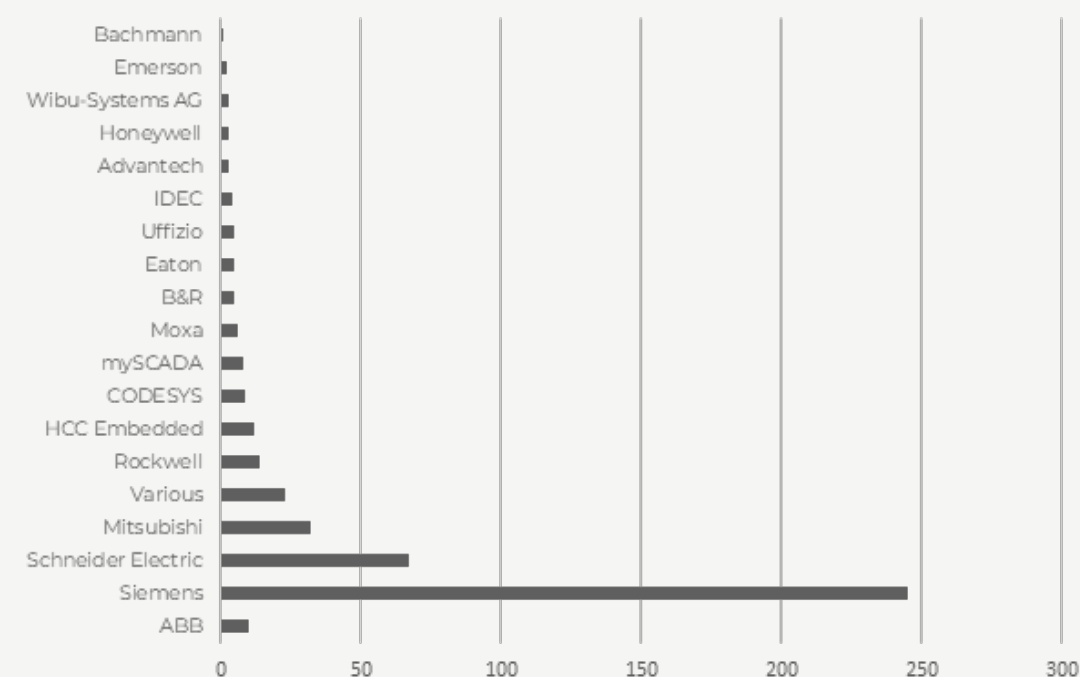
portfolio and deliver components to several industries. Secondly, they are industry leaders in testing their systems and openly report on vulnerabilities.

NORMA Cyber is aware of major vendors in the maritime industry that do not publicly disclose their vulnerabilities, so the overview below may give a wrong impression of the situation. There are different strategies on vulnerability management.

We believes that, in the long run, the most sustainable strategy is to be open about vulnerabilities and how to mitigate them.

## 458

OT vulnerabilities detailed in NORMA Cyber-reports  
April 2021 – April 2022







## 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:**

- ◆ Unauthorized 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 unauthorized 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](mailto:ops@normacyber.no) and be as detailed as possible. Please include full contact information so we are able to take the appropriate action.

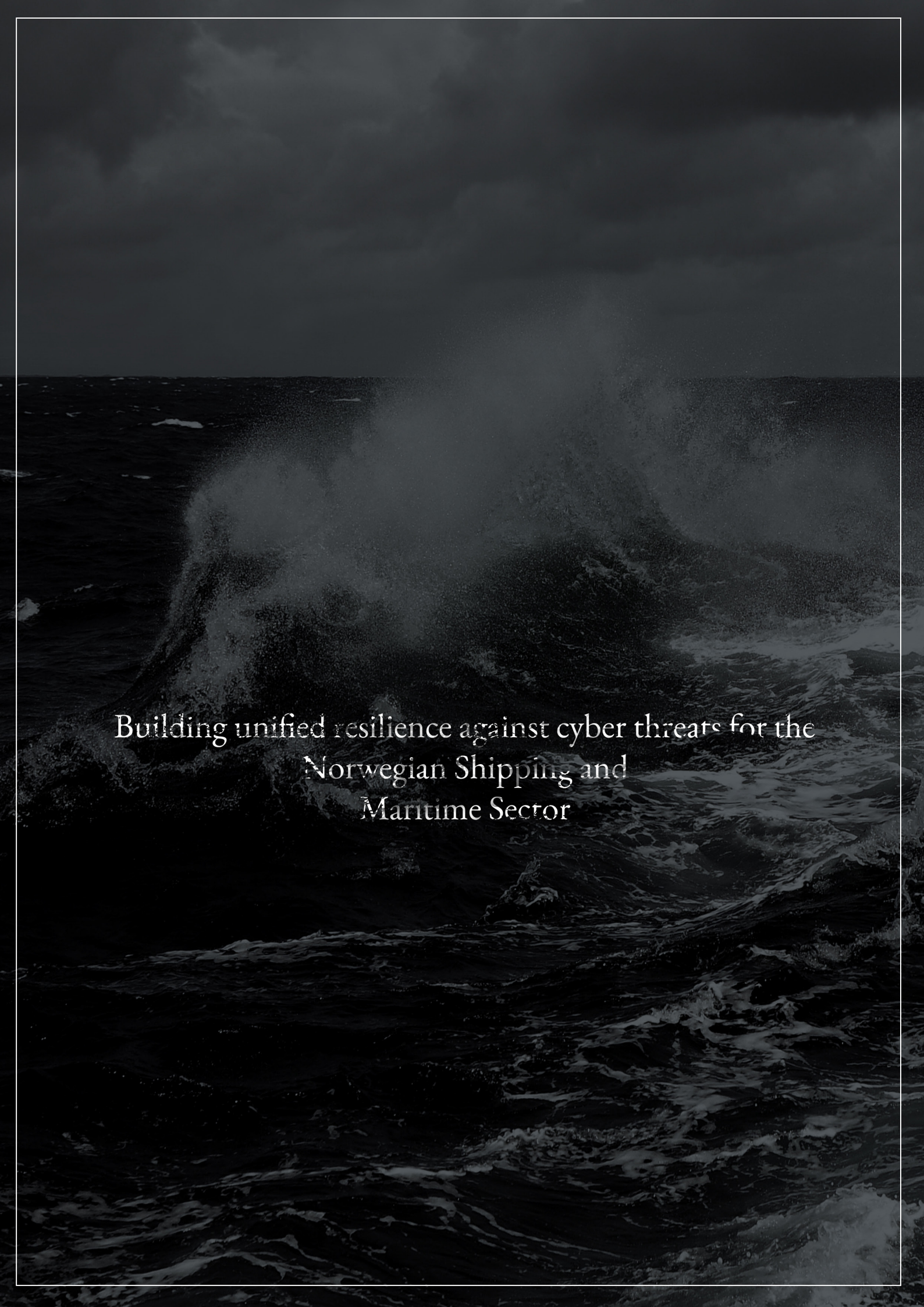
**Key elements to share:** incident data and time, incident location, type of activity and a detailed narrative of the incident.

**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  
Norwegian Shipping and  
Maritime Sector