**Cyber Crimes**

  10th February 2020

Introduction

Maritime cyber-crimes are illegal actions undertaken against ships or critical infrastructures through computer channels. Attacks can have a wide variety of purposes, including to damage, destroy or hijack IT (Information Technology) or OT (Operations Technology) systems.[1](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-1-33)

Multiple different targets, forms of attacks, motivations, and perpetrators can be involved in cyber-crimes.

A large crane on the water

Description automatically generated with medium confidence

*Port, by*[*Bill Dickinson*](https://www.flickr.com/photos/skynoir/16005967512/in/photolist-qooLv7-3hMqP-UxuNsY-4BWbGQ-7ayuC-2ngNmeL-53qCMK-boPkHz-9eFiDs-5NjkKP-2cRM1iV-mDjjP-4Lymp-4LymQ-5Pzde4-iufdec-61PEFm-54VT7k-5F7C2q-8GvzH2-4Lymc-7sq8r-dp9NN-X8cNZj-3pAjHR-2jh4gHz-BoyjAA-27ek55A-MXJVpE-ChHg4J-6ykQvN-bpTmEp-kPjTY4-5XQmKj-b7FRav-cu4tVj-7cqXMz-ogXxK-EybyB3-5XsXgb-4Kf8Pa-Nu3vGg-a5np3M-4V7Frr-2hMKxA3-HQhYcJ-HE6V1r-Mqic8Z-zd7iWD-6r2YM)*Attribution-NonCommercial-NoDerivs 2.0 Generic (CC BY-NC-ND 2.0)*

Characteristics

*Targets*

Not all cyber-crimes discussed in this entry specifically target the maritime sector, but may instead aim to infect as many systems as possible.[2](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-2-33) As such, there is a distinction between targeted and untargeted attacks.[3](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-3-33) Even so, cyber-crimes pose an increasing risk to the maritime sector, even when untargeted. This is due to the specific dynamics of the sector’s critical infrastructure.[4](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-4-33)

For example, the movement of ships across international boundaries exposes their systems to a larger number of unknown IT networks.[5](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-5-33) Because many ships are relatively old (the average age of ships is over 20 years),[6](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-6-33) they often have a mix of old and new systems, some of which may be obsolete. Many ships (including naval vessels) cannot upgrade these easily due to outdated hardware.[7](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-7-33) Tam and Jones argue that the design cycle of newer ships is of a duration that means this problem will likely continue to exist.[8](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-8-33)

Other reasons ships are particularly vulnerable to cyber-attacks are their differing systems, the duration of their voyages which create large windows of opportunity for cyber-attacks, a nominally low bandwidth while at sea, and alternating between extreme isolation and global connectivity at international ports.[9](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-9-33) Because ships often change crews, it can be difficult to ensure that all crews are aware of cyber-vulnerability, meaning human failure can also be significant risk factor for ships.

Ships are increasingly connected to networks through very-small-aperture terminals (VSAT), and their bandwidth capacity is increasing. This means they can access networks with greater regularity and share more information, making them more susceptible to cyber-attack.[10](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-10-33)

Shipping is also increasingly reliant on networked systems for its operation.[11](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-11-33) Navigation depends on electronic systems such as ECDIS, GNSS, VDR and Radar/ARPA, as well as the un-encrypted Automatic Identification System (AIS) network.[12](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-12-33) In some cases, ships are unable to sail without these systems; many are designed to be paper-less and are therefore dependent on digital means of navigation.[13](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-13-33) Propulsion too is increasingly automated, especially power control systems, and is often networked through integration with navigation.[14](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-14-33)

Ports are also at risk of being targeted. Computer systems undergird the global flow of maritime commerce. Ports incorporate a variety of networked OT systems, including modern gantry cranes, and scanning systems.[15](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-15-33) The advent of ‘smart ports’ means more of the day-to-day operations are automated, increasing vulnerability.[16](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-16-33) Port operators and agents also rely on IT for their management, such as freight management, operations data, traffic control communications, financial data, and corporate systems.[17](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-17-33)

These infrastructures are often connected, with data flowing between a large number of actors from across the globe.[18](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-18-33) This means that a cyber-attack targeting or impacting on one actor can quickly spread to other actors and different infrastructures.[19](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-19-33)

*Types of attack*

Cyber-attacks can take multiple different forms.[20](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-20-33) In order to provide a simplified overview, these will be explored through the effects they have – firstly, those that impact directly on operations, and secondly, those that are used to facilitate other forms of criminality.

The first type of cybercrime stops or limits operations, generally through a direct attack that damages systems or makes them either inaccessible or limited in such a way that continuing operations in ports or onboard ships and offshore infrastructure would be impossible or unsafe. Autonomous shipping, port services, navigation aid systems, offshore platforms and marine traffic control centres are all potential targets for these kinds of crimes.

Cyberattacks of this type can include mechanisms such as malware, software designed to damage systems, ransomware, software that blocks access to systems or publishes data unless a ransom is paid, and Distributed Denial of Service (DDoS – the flooding of a network with data to make it inaccessible). The Baltic and International Maritime Council (BIMCO) report a case where a shipowner opened an infected email attachment sent from two unwitting ship agents which made systems inaccessible until a ransom had been paid.[21](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-21-33) Similarly, a large-scale destructive malware attack was targeted at the Maersk line in 2017.[22](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-22-33) This saw malware spread across up to 76 ports causing widespread system outages. Both of these examples shut down operations by making information systems inaccessible.

Ships are also at risk from these forms of attack. In 2016 in South Korea 280 ships had to halt operations due to problems with their navigation systems.[23](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-23-33) Viruses and malware have been shown to contribute to these issues, causing stoppages in operations due to safety concerns and an inability to navigate effectively.[24](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-24-33) While these navigation systems were connected to the internet, even air-gapped systems (those not physically connected to an external network) have been shown to have dormant viruses.[25](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-25-33)

Many of these attacks are likely to have been untargeted. However, analysis by BIMCO suggests that targeted attacks are more sophisticated, because specific tools and techniques will be created for targeting the company or ship. These might include the manipulation of insider individuals; brute force (where many passwords are tried); and DDoS attacks.[26](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-26-33)

Spoofing is a targeted form of attack that has become a concern for ship navigation.[27](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-27-33). Spoofing involves convincing the positioning systems of the ship into believing a counterfeit signal in order to make unintentional course corrections.[28](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-28-33)

One study conducted by Trend Micro demonstrated an ability to recreate a VHF frequency on AIS that could simulate a “ghost ship” in a nearby port, which would alert vessels they were on a collision course and change their path.[29](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-29-33) In a further study the University of Texas-Austin were able to effectively take remote control of a yacht in the Mediterranean by overpowering the onboard GPS.[30](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-30-33) Spoofing can also cause ships to misreport or lose their own position, as occurred in the Black Sea in 2017 in an incident that impacted over 20 vessels.[31](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-31-33) The diversion of ships through spoofing impacts negatively on operations, requiring the them to right the course manually or halt altogether until the issue is resolved.[32](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-32-33) Jamming can also cause such issues by causing failures in navigation systems.[33](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-33-33)

Data loss and theft resulting from hacking can be a serious targeted cyber-crime. In a case against an Iranian Shipping Line, for example, data loss relating to delivery and locations of containers meant that cargo containers could not be identified or located, causing financial loss.[34](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-34-33) There have also been cases where companies have been extorted into paying hackers so that confidential business information is not released.[35](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-35-33)

A second type of cybercrime aims to facilitate other maritime crimes such as drugs trafficking, piracy, and fraud though various forms of cyber-attack, for example by hacking port systems that control and track container movement in order to hide shipments of illicit goods. An indicative case was the hacking of the Port of Antwerp’s digital container tracking system in 2013.[36](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-36-33) Containers trafficking drugs could be released without port authorities becoming aware, and traffickers could reach containers before their legitimate owners.[37](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-37-33) Initially this was done through the cultivation of insiders in the port system, which then allowed hackers to re-enter electronic systems remotely. In other cases, traffickers have been able to discover which containers are under suspicion in order to avoid collection, as occurred in Australia in 2012 [38](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-38-33)

Robbery and piracy can be facilitated by cybercrimes. By hacking a system, attackers can browse cargo and container lists to identify the most valuable goods for black markets, to then be stolen in the port or targeted for future piracy attacks when the ship is at sea.[39](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-39-33) Between 2010 and 2011, for example, a Greek Shipping Company was targeted by pirates in the Gulf of Aden after hackers had gained access to route timetables and ship vulnerabilities.[40](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-40-33) It has been suggested that spoofing can also make piracy easier, by making the ships appear to be elsewhere – either leading them into more dangerous areas or making rescue difficult.[41](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-41-33)

Cyber-fraud, too, is an increasing problem. A number of maritime bunkering and fuel services have fallen victim to such frauds, including World Fuel Services, who were defrauded of $17.9 million by a faked order.[42](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-42-33) Criminals were able to create a fake fuel supply tender, which led to a ship-to-ship transfer. When they attempted to bill the agency in the documents, however, there was no record of the transaction. Vulnerabilities are increased because many transactions occur over email.[43](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-43-33)

*Perpetrators*

Some attacks are undertaken by independent individuals and are relatively minor in scale and effect. These may be carried out by hackers outside of the system or disgruntled employees.[44](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-44-33) The motivation for such attacks may be economic gain, but non-financial reasons such as a desire to cause vandalism, leak information, prove cyber skills and enhance reputation in the wider community, or even ideological motivations when wanting to damage operations to protest for an activist cause.[45](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-45-33) Within these relatively small activities some may be opportunistic rather than planned and be undertaken without specialist knowledge of techniques and tools.[46](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-46-33)

Other cybercrimes are more organised. In the cases of trafficking facilitation above for example, there were links to South American organised criminal groups. Corrupt employees can also be implicated in such attacks. Attackers often need an in-depth knowledge of port systems and infrastructure, as well as expert knowledge of the techniques and tools for cyberattacks, both of which demand sophisticated organisational capacities.

Other groups engage in corporate or industrial espionage. [47](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-47-33) These can include corporations seeking to create competitive advantage .[48](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-48-33) They may act directly or through third parties with the aim of harming a rival by collecting business intelligence, stealing intellectual property, or disrupting operations to cause financial or reputational loss.[49](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-49-33)

Not all organised cyber-crimes are targeted or have a financial motivation. For example, the Maersk case discussed above was well-orchestrated, but seems to have been aimed at disruption as much as financial gain. This has led to a recognition of a distinction between vandalism, which is relatively small scale and disorganised on the one hand, and well-organised and intentional sabotage on the other.[50](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-50-33)

A final difficulty is distinguishing between acts undertaken by criminal groups or independent hackers, and those carried out by states. State-led cyber-crimes tend to be viewed as issues of national security. Cyber-attacks are increasingly difficult to attribute,[51](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-51-33) especially if they are undertaken by perpetrators with less clear state-sponsorship. Some of these criminal acts are thought to be undertaken by states due to the targets involved and the sophistication of the attacks. In 2020 for example, a cyber-attack in Iran’s Shahid Rajaee port terminal – thought to have been conducted by Israel – halted operations.[52](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-52-33) There are also increasing concerns that terrorist groups could engage in cyber-crimes.[53](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-53-33)

Scope

There was initially criticism that the frequency and potential of cyber-attacks was been overestimated.[54](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-54-33) In response, sources such as CyberKeel and Maritime Cyber Emergency Response Team produce bulletins identifying maritime cyber attacks when they take place.[55](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-55-33) BIMCO also collect this information.[56](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-56-33)

Despite these efforts, the scope of cybercrime in the maritime sphere is not well understood. There is no centralized reporting mechanism and there has been some degree of confusion whether channels for reporting emergencies include cybercrimes.[57](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-57-33) This has led to calls for an accessible and streamlined reporting process.[58](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-58-33) However, such systems are limited because cybercrimes are sometimes not disclosed by those targeted due to concerns over reputational loss the exposure of flaws in their IT infrastructure, or misclassification as technological error.[59](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-59-33)

Even so, it is clear that cybercrimes in the maritime sector are on the rise and that many more attacks occur than are made public.[60](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-60-33) Cybersecurity consultancy Naval Dome for example reported a 400 per cent increase in their detected attempted attacks between February and May 2020.[61](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-61-33) The COVID-19 pandemic is thought to have had an impact on this increase, because more systems are became digitally connected out of necessity.[62](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-62-33) Overall, Safety at Sea and BIMCO report 31 per cent of companies surveyed reported an attempted cyber attack in 2020.[63](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-63-33)

Impact

The kinds of attacks described above have a number of tangible impacts. There are also hypothetical impacts should some (so far unsuccessful) cybercrimes to be successful.

First, paying ransoms or dealing with operational shutdowns has an economic impact. The attack on Maersk for example, is argued to have cost as much as $300 million in lost revenue and costs associated with re-building compromised networks.[64](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-64-33) Systems may also be damaged or destroyed. Theft facilitated by cybercrimes also causes a significant economic impact.[65](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-65-33)

Reputation damage, while negative in itself, might also have an economic impact by limiting future revenue.[66](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-66-33) There are concerns that if ports were disrupted by cyber-attacks, the zero-inventory just-in-time nature of many economies would see commerce severely disrupted.[67](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-67-33) This would have a severe economic impact for workers, business revenue and also the shipping lines themselves as goods would have to be diverted.

Cyber-crimes that facilitate drug trafficking undermine enforcement efforts and the rule of law. They also contribute to income for illicit organised groups. In the wake of the Antwerp case discussed above, over $365 million of drugs were seized – demonstrating just how profitable the operation was to the organised gangs.[68](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-68-33)

Cyber-attacks may impact on the physical safety of ships, crews and others. Disrupting navigation could lead to ship-on-ship collisions or even cause ships to collide go aground.[69](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-69-33) As yet, this remains only a hypothesised outcome, but the growing reliance on automated shipping means it is a possibility based on the successful spoofing attacks that have occurred so far. Undetected attacks on Mobile Offshore Drilling Units have the potential to cause oil spills or loss of life through explosions.[70](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-70-33) If OT systems in ports were compromised, it could lead to injury or death due to the dangerous natures of the cranes and ship movement.[71](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-71-33) There are also serious security and safety implications of having queues of ships outside of a port entrance in the case of a shutdown.[72](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-72-33)

Finally, Kramek hypothesises that some cyber-crimes could also impact on military operations, and therefore have a significant national security dimension.[73](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-73-33) In his analysis of the Port of Beaumont, through which much of the US Army’s logistics run, he argues that any attack there could impact the military’s ability to respond to crisis or conflict.

Linkages & Synergies

Cybercrime is most often linked to illicit trafficking, given traffickers’ past usage of cyber to facilitate the movement of cargo through ports. It is also linked to piracy, as information gained through cyber-attacks has been used to inform pirate attacks in the past.

Responses

Responses to cybercrime in the maritime sector have been slow in coming, though there is a movement towards improved guidelines for maritime stakeholders.

Most evidence suggests that ports and shipping lines are under-prepared for cyber threats [74](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-74-33) due to a lack of awareness about cyber-security among management and stakeholders, and a belief that the prospect of an attack is either unlikely or theoretical.[75](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-75-33). There may also be a confusion of responsibility for cyber security between port authorities and IT providers.[76](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-76-33) Kramek demonstrates that most ports in the US did not claim Port Security Grant Program funds (which could be used for any aspect of port security) for cybersecurity purposes.[77](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-77-33) Most did not have cyber incident response plans. These factors have led some to argue that the maritime industry is 10-20 years behind comparable industries in addressing cyber security challenges.[78](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-78-33)

*International*

A number of international organisations have released guidelines for shipping companies and ports, including BIMCO, the International Maritime Organisation (IMO), the European Union Agency for Cybersecurity (ENISA), International Association of Ports and Harbors (IAPH),[79](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-79-33) and EUROPOL.

The expected outcome of these guidelines is a greater awareness amongst stakeholders of the issues, leading to better cyber security policies and training for staff.[80](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-80-33) Such training is important due to the ‘insider threat’, where employees may unwillingly contribute to cyber-attacks through their own lack of awareness.[81](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-81-33)

Insurance companies have played a role in raising awareness, especially as many exclude cyber-attacks from their policies and therefore increase risk (the Institute Cyber Attack Exclusion Clause).[82](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-82-33)

International guidelines also suggest security audits and assessments,[83](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-83-33) penetration testing, network segmentation, regular network scans, multi-factor authentication, identification of stakeholders, the creation of a security operations centre with a dedicated cybersecurity officer, and physical security assessments.[84](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-84-33) Relatively basic guidelines include the need to employ antivirus and encryption measures, frequent password updates, and electronic data backup, as well as limiting the use of USB devices by employees.[85](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-85-33)

In their Interim Guidelines in Maritime Security Cyber Risk Management, issued in 2017, the IMO proposes an approach based on five functional elements: identify, protect, detect, respond and recover. Shipping companies had to come into compliance on the 1st of January, 2021.[86](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-86-33)

*National*

National guidelines have also been implemented. Examples include two sets of codes of practice from the UK’s Department for Transport (Cybersecurity for Ships, and the Cyber Security Code of Practice for Ports),[87](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-87-33), France’s Critical Infrastructures Information Protection Law,[88](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-88-33) and the German IT-Grundschutz.[89](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-89-33)

While preventative guidelines to cyber-threats are increasingly common, strategies for actually responding to cyber-attacks are less well-developed. Reporting attacks to national jurisdictions when underway remains problematic, for example.

Some countries have delegated cyber-security to a specific agency or department in order to build stronger cyber resilience. In the US for example, the US Coast Guard is charged with protecting the maritime sector from cyber-crimes. They send out monthly notices to the maritime community in the United States with links to cybersecurity awareness bulletins, training, tools, and alerts.[90](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-90-33) However, coordination with other relevant agencies has sometimes been problematic.[91](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-91-33) Coordination challenges have also been recognised within the EU. The European Union Agency for Cyber Security (ENISA) for example argues that ‘the fragmentation of European maritime policies brings difficulties for the clear definition of responsibilities and roles to be taken regarding cyber security matters in this sector.’[92](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-92-33)

Coordination and information-sharing between state and private stakeholders such as shipping agents and port authorities can also be difficult. This is problematic when these stakeholders share access to the same systems and networks.[93](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-93-33) One port can incorporate up to 900 different stakeholders for example.[94](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-94-33) Some may use different IT systems with different technical support teams behind them. As ENISA argues, ‘this [port] ecosystem is built from companies of various sizes, with various levels of cybersecurity capabilities and can even be direct competitors among themselves’.[95](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-95-33) Efforts are underway to solve this problem – Port Information Sharing and Analysis centres, for example, aim to establish public-private partnerships and are predicated on trust-based networks that allow for secure information-exchange.[96](https://www.safeseas.net/evidence/2020/02/10/cyber-crimes/#easy-footnote-bottom-96-33)

List of References

1. [Alcaide & Llave 2020](https://www.sciencedirect.com/science/article/pii/S2352146520302209)
2. [MARLINK 2018](https://marlink.com/resources/); [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
3. [MARLINK 2018](https://marlink.com/resources/); [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
4. [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20); [2019](https://ieeexplore.ieee.org/document/8899382)
5. [Tam and Jones 2018](https://ieeexplore.ieee.org/document/8560690); [2019](https://ieeexplore.ieee.org/document/8899382)
6. [Statista 2022](https://www.statista.com/statistics/1102442/age-of-world-merchant-fleet-by-vessel-type/)
7. [Goldman 2015](https://money.cnn.com/2015/06/26/technology/microsoft-windows-xp-navy-contract/index.html); [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20); [2019](https://ieeexplore.ieee.org/document/8899382)
8. [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20)
9. [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20)
10. [MARLINK 2018](https://marlink.com/resources/)
11. [Balduzzi et al. 2014](https://dl.acm.org/doi/10.1145/2664243.2664257); [Driva 2016](https://womencourage.acm.org/archive/2016/poster_abstracts/womENcourage_2016_paper_10.pdf); [Hareide et al. 2018](https://www.cambridge.org/core/journals/journal-of-navigation/article/abs/enhancing-navigator-competence-by-demonstrating-maritime-cyber-security/AF9FD35689C5B5F879B2446722B5CA1B); [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20); [2019](https://ieeexplore.ieee.org/document/8899382); [Tam et al. 2021](https://www.scirp.org/journal/paperinformation.aspx?paperid=113658)
12. [Marsh 2014](https://www.marsh.com/pr/en/industries/marine/insights/risk-of-cyber-attack-to-maritime-sector.html); [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=); [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
13. [Tam and Jones 2018](https://ieeexplore.ieee.org/document/8560690)
14. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=); [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
15. [Kramek 2013](https://www.brookings.edu/research/the-critical-infrastructure-gap-u-s-port-facilities-and-cyber-vulnerabilities/); [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
16. [Chelin & Reva 2020](https://issafrica.org/iss-today/security-vs-efficiency-smart-ports-in-a-post-covid-19-era); [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector); [Bagwandeen 2022](https://www.ntu.edu.sg/cas/news-events/news/details/development-of-smart-ports-in-africa)
17. [Kramek 2013](https://www.brookings.edu/research/the-critical-infrastructure-gap-u-s-port-facilities-and-cyber-vulnerabilities/)
18. [Loomis et al. 2021](https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/); [Kessler & Shepard 2022](https://www.garykessler.net/MaritimeCybersecurityBook/index.html)
19. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
20. [Kessler & Shepard 2022](https://www.garykessler.net/MaritimeCybersecurityBook/index.html)
21. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
22. [Mathews 2017](https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/?sh=2bb5f2914f9a)
23. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
24. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
25. [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20)
26. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
27. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
28. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
29. [Ferran 2013](https://abcnews.go.com/Blotter/guys-make-oil-tankers-disappear-virtually/story?id=20565851)
30. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
31. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
32. [Hareide et al. 2018](https://www.cambridge.org/core/journals/journal-of-navigation/article/abs/enhancing-navigator-competence-by-demonstrating-maritime-cyber-security/AF9FD35689C5B5F879B2446722B5CA1B)
33. [Homeland Security 2016](https://info.publicintelligence.net/DHS-SeaportCyberAttacks.pdf); [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
34. [Cyberkeel 2014](https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cyber-Crime-10-2014.pdf); [Kapalidis 2020](https://link.springer.com/book/10.1007/978-3-030-34630-0)
35. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
36. [EUROPOL 2013](https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf)
37. [Cyberkeel 2014](https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cyber-Crime-10-2014.pdf)
38. [Kotchekova 2015](https://www.kaspersky.com/blog/maritime-cyber-security/8796/)
39. [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
40. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships); [Kessler & Shepard 2022](https://www.garykessler.net/MaritimeCybersecurityBook/index.html)
41. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
42. [Bunker Index 2016](https://bunkerindex.com/news/article.php?article_id=17335)
43. [Ship & Bunker 2014](https://shipandbunker.com/news/am/171559-recent-cyber-attacks-highlight-bunker-industry-vulnerability)
44. [Department for Transport 2017](https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice); [2020](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf); [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
45. [Department for Transport 2017](https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice); [2020](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf); [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=); [Loomis et al. 2021](https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/)
46. [Department for Transport 2017](https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice); [2020](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf)
47. [Newberry 2015](https://www.semanticscholar.org/paper/Maritime-Critical-Infrastructure-Cyber-Risk-Newberry/222bae0f01661a9a3293b5dc887ee72a88a26ba5)
48. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
49. [Department for Transport 2017](https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice); [2020](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf); [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
50. [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
51. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=); [Fahey 2017](https://blogs.icrc.org/law-and-policy/2017/12/07/combating_cyber-fatigue-in-the-maritime-domain/)
52. [Warrick & Nakashima 2020](https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html)
53. [Kramek 2013](https://www.brookings.edu/research/the-critical-infrastructure-gap-u-s-port-facilities-and-cyber-vulnerabilities/); [Newberry 2015](https://www.semanticscholar.org/paper/Maritime-Critical-Infrastructure-Cyber-Risk-Newberry/222bae0f01661a9a3293b5dc887ee72a88a26ba5); [Tanti-Dougall 2014](https://www.lexisnexis.com/legalnewsroom/public-policy/b/public-policy-law-blog/posts/cyber-terrorism-a-new-threat-against-the-maritime-industry)
54. [Jensen 2015](https://timreview.ca/sites/default/files/article_PDF/Jensen_TIMReview_April2015.pdf); [Cyberkeel 2014](https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cyber-Crime-10-2014.pdf)
55. [Maritime CERT n.d.](https://www.maritimecert.org/); [Cyberkeel 2014](https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cyber-Crime-10-2014.pdf)
56. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
57. [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20)
58. [Silverajan & Vistiaho 2019](https://ieeexplore.ieee.org/document/8826949); [Loomis et al. 2021](https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/)
59. [Ahokas et al. 2017](https://www.econstor.eu/bitstream/10419/209316/1/hicl-2017-23-343.pdf); [Cyberkeel 2014](https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cyber-Crime-10-2014.pdf); [Jensen 2015](https://timreview.ca/sites/default/files/article_PDF/Jensen_TIMReview_April2015.pdf); [Larsen & Lund 2021](https://ieeexplore.ieee.org/document/9585112); [Loomis et al. 2021](https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/)
60. [Kessler 2019](https://commons.erau.edu/publication/1318/)
61. [Maritime Executive 2020](https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent)
62. [Khun et al. 2021](https://link.springer.com/article/10.1007/s13437-021-00235-1)
63. [Safety at Sea & BIMCO 2021](https://cdn.ihsmarkit.com/www/prot/pdf/1020/Safety-at-Sea-and-BIMCO-Cyber-Security-White-Paper-2020.pdf)
64. [Kessler 2019](https://commons.erau.edu/publication/1318/)
65. [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20)
66. [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20); [MARLINK 2018](https://marlink.com/resources/); [Alcaide & Llave 2020](https://www.sciencedirect.com/science/article/pii/S2352146520302209)
67. [Kramek 2013](https://www.brookings.edu/research/the-critical-infrastructure-gap-u-s-port-facilities-and-cyber-vulnerabilities/); [Khun et al. 2021](https://link.springer.com/article/10.1007/s13437-021-00235-1)
68. [Kapalidis 2020](https://link.springer.com/book/10.1007/978-3-030-34630-0)
69. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=)
70. [Belmont 2015](https://maritime-executive.com/blog/maritime-cyber-attacks-changing-tides)
71. [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
72. [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
73. [Kramek 2013](https://www.brookings.edu/research/the-critical-infrastructure-gap-u-s-port-facilities-and-cyber-vulnerabilities/)
74. [Ahokas et al. 2017](https://www.econstor.eu/bitstream/10419/209316/1/hicl-2017-23-343.pdf); [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
75. [Cyberkeel 2014](https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cyber-Crime-10-2014.pdf); [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector); [Khun et al. 2021](https://link.springer.com/article/10.1007/s13437-021-00235-1)
76. [Kramek 2013](https://www.brookings.edu/research/the-critical-infrastructure-gap-u-s-port-facilities-and-cyber-vulnerabilities/)
77. [Kramek 2013](https://www.brookings.edu/research/the-critical-infrastructure-gap-u-s-port-facilities-and-cyber-vulnerabilities/)
78. [Caponi & Belmont 2014](https://maritime-executive.com/article/Maritime-Cybersecurity-A-Growing-Unanswered-Threat-2014-10-24)
79. [IAPH 2020](https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf)
80. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships); [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector); [Khun et al. 2021](https://link.springer.com/article/10.1007/s13437-021-00235-1)
81. [Tam & Jones 2018](https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20); [Fitton et al. 2015](https://ssg.lancs.ac.uk/wp-content/uploads/oliver-the-maritime.pdf)
82. [Marsh 2020](https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/silent-cyber-changing-ins-markets-slides.pdf)
83. [BIMCO 2021](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships); [Chelin & Reva 2020](https://issafrica.org/iss-today/security-vs-efficiency-smart-ports-in-a-post-covid-19-era); [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
84. [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector); [Department for Transport 2017](https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice); [2020](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf)
85. [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
86. [Daum 2019](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=); [Petta 2021](https://cimsec.org/the-imos-2021-cyber-guidelines-and-the-work-that-remains-to-secure-ports/)
87. [Department for Transport 2017](https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice); [2020](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf)
88. [ANSSI n.d.](https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/)
89. [ENISA n.d.](https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_it_grundschutz.html)
90. [USCG n.d.](https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/)
91. [Kramek 2013](https://www.brookings.edu/research/the-critical-infrastructure-gap-u-s-port-facilities-and-cyber-vulnerabilities/)
92. [ENISA 2011](https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport)
93. [ENISA 2011;](https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport)[ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
94. [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
95. [ENISA 2019](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector)
96. [USCG 2015](https://homeport.uscg.mil/Lists/Content/DispForm.aspx?ID=45422&Source=/Lists/Content/DispForm.aspx?ID=45422); [Larsen & Lund 2021](https://ieeexplore.ieee.org/document/9585112)