Stormy seas ahead
Cyber-security guidance for the maritime industry
The world’s most critical industry needs to update its cyber-defences to protect global economies.

MDR Cyber’s work with maritime clients has reinforced research showing an industry that is underprepared to deal with cyber-security issues. A survey by IHS Markit/BIMCO found that over a fifth of respondents had experienced a cyber incident. Attackers may be deliberately targeting the industry, due to the nature of its operations and assets, or via ancillary exposure (e.g. a supplier or client experiences a cyber attack).

Given the threat landscape, leaders in the maritime industry need to better inform themselves of what the risks are, and what may lie ahead. They also need to be aware of regulation governing cyber-security management, and take key steps to protect their assets from risks.

Modern commercial seafaring is characterised by a heavy reliance on shipborne technologies. The shipping business, in general, increasingly depends on digital technology for tasks spanning navigation to container tracking, and a host of other business operations. Although technology has revolutionised safety and efficiency in shipping, it has also created vulnerabilities to safety and operations.

The maritime industry plays a critical part in both the United Kingdom and global economies. The world shipping fleet comprises 93,161 vessels worth over USD 819Bn, and there are many more vessels to add to that figure, ranging from pleasure to military craft.

The UK and shipping
As an island nation, the UK sees its economy directly affected by the maritime industry, whether through passenger/freight services and port services or shipbuilding and the supply chain. Every day, ships are responsible for providing the UK with a mechanism to trade with other countries, and to support a large proportion of the economy.

In 2016 the shipping industry contributed EUR 145Bn to the EU GDP, plus EUR 41Bn in tax revenue and 2.3m jobs. According to the Organisation for Economic Co-operation and Development, for every GBP 1m the shipping industry contributes to the GDP in Great Britain, another GBP 1.6m is created elsewhere in the economy.

In this context, a disruption to shipping will result in disruption and financial consequences for the wider economy.

Stormy seas ahead Cyber-security guidance for the maritime industry
The changing nature of the threat

The nature of the cyber threat affecting the maritime industry today reflects that of many other industries, affecting IT systems and back office functions. However, looking to the future, there is growing concern of the possibility and impact of more sophisticated threats affecting shipborne technology.

According to a 2018 survey of more than 350 individuals working in the maritime industry, over a fifth of respondents (22%) reported experiencing a cyber incident in the past 12 months, with 72% of these stating that it related to their own company. Although currently the main threats reported in this survey (93%) related to IT systems, rather than operational technology (OT) or navigation systems, there was an overwhelming perception among respondents that shipborne systems, particularly navigation systems were the most vulnerable to attack.

### Format of System Affected

- IT 92%
- OT 7%
- Navigation 7%
- All 2%

### Incident extent

- Affecting IT performance
- Loss of corporate data
- Financial loss
- Affecting shipborne system performance
- Commerce
- Other

Source: Fairplay and BIMCO Maritime Cyber Security Survey 2018
Vessels and their risks
Across the global maritime community, the increased digitalisation has proven to be beneficial to the industry in terms of productivity, efficiency and performance optimisation. But this consistent connection with the cyber world also imposes serious threats.

As a result, all maritime vehicles have vulnerabilities and potential consequences that define the approach needed to confront and tolerate their cyber risks.

Yachts
Yachts contain high-value assets: the rich and super-rich individuals who own and operate these vessels. They face a particularly high risk of cyber attacks that might facilitate hijacking and piracy.

Piracy is an ongoing concern in many parts of the world, and most pirates would seize an opportunity to capture and ransom a high-value target. Subversion of navigation and security systems to facilitate the capture of passengers is entirely possible.

Cyber attacks that could facilitate such activity include tactics to take remote control of a vessel, or to force a vessel off course into vulnerable waters. This might occur via the transmission of false GPS signals designed to guide a ship off course. This would likely be accompanied by attacks on communications and the like, leading to the conclusion that yachts require a strong combination of redundancy and resilience in their communications and navigation systems.

Passenger ships
Cruise ships today can carry thousands of passengers and an array of on-board systems to support day-to-day operations, communications, safety, and entertainment.

Although piracy is a potential issue for such vessels, commercial disruption is more likely. Potential threats include attackers who can either redirect ships and disrupt their schedules or disrupt onboard operations via the hijacking of ship systems.

Effects could range from a temporary loss of systems, which would likely affect reputation and service to passengers, to serious disruption to the ship’s course and/or damage to the ship itself. At worst, there could be mass loss of life if a ship was destroyed at sea in any way.

To address this, passenger-heavy cruise ships need to ensure that their navigation systems and non-critical onboard systems (those important for passenger comfort and experience) are well protected.
Large vessels
Often holding large volumes of hydrocarbons or other liquids and gasses, tanker ships are subject to a wide range of potential risks, which can be exacerbated by cyber-security risks. Dangerous cargo relies on a range of systems for secure storage and transport, and in modern tankers these systems involve OT components that control general automation and ship operations.

Cyber attackers aiming to cause disruption, significant property damage, and even loss of life can attack these systems to potentially release dangerous cargo within the ship. They could similarly aim to hijack cargo for military reasons, such as to disrupt trade routes to restrict an adversary’s ability to produce energy or manufacture goods.

Maintainers of these large vessels focus on the systems controlling their cargo environments, as well as the integrity of their ship protection systems which are aimed at preventing hijack and piracy.

Container ships
Often carrying huge amounts of valuable cargo, container ships face several risks associated with a breach of their cargo management systems. It has already been proven that criminals can hack into systems to gather intelligence that will support their activities: stealing cargo at sea or tracking cargo to optimise criminal operations once it has arrived at port.

Without effective security measures to prevent and detect unauthorised access and changes to data, systems may be used to facilitate the tracking, theft, or destruction of cargo, depending on the threat actor’s motives.

Container shipping must focus more attention on ports than vessels. Although the security of electronic tags is important for the integrity of the shipping process, the port shipping systems hold the core of the data criminals seek to access.

Autonomous vessels
Seen by many as core to the future of maritime shipping, autonomous vessels will bring considerable opportunity for cost savings and potential increases in safety, but will come with their own challenges with respect to cyber-security.

The lack of a crew to take local control of issues will complicate the handling of any cyber-security incidents that arise; controls and remediation plans will need to address this aspect of potential incidents. On the other hand, improved remote visibility and monitoring capabilities may facilitate a quicker response, and vessels designed from the ground up to function autonomously can also be designed from the ground up to be secure. As always, factoring in security earlier is cheaper than attempting to work it in later.

Autonomous vessels will rely heavily on navigation, communications, and monitoring capabilities so will need to ensure that cyber-security incidents do not arise. All of these systems will need to be robust and resilient to any attacks by criminals or pirates wishing to hijack the vessel or its cargo.
<table>
<thead>
<tr>
<th>Mariners and Bridge Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated Identification System (AIS)</strong></td>
</tr>
<tr>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td><strong>Known vulnerabilities</strong></td>
</tr>
<tr>
<td><strong>Risks / Impacts</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Radio Detection and Ranging (Radar)</strong></td>
</tr>
<tr>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td><strong>Known vulnerabilities</strong></td>
</tr>
<tr>
<td><strong>Risks / Impacts</strong></td>
</tr>
<tr>
<td><strong>Global Navigation Satellite System (GNSS)</strong></td>
</tr>
<tr>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td><strong>Known vulnerabilities</strong></td>
</tr>
<tr>
<td><strong>Risks / Impacts</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Communications</strong></td>
</tr>
<tr>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td><strong>Known vulnerabilities</strong></td>
</tr>
<tr>
<td><strong>Risks / Impacts</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Cargo Movement / Management

**Objective**
- Monitor the status and manage the movement of cargo on board ships

**Known vulnerabilities**
- Network vulnerabilities have led to known instances of data theft via unauthorised access to systems

**Risks / Impacts**
- Risk of cyber enabled information loss leading to theft
- Monitoring of cargo status leads to target for piracy
- Insurance risks

### Deck Machinery

**Objective**
- Machinery enables efficiency of on ship tasks such as heavy loading or basic ship functionality

**Known vulnerabilities**
- Increasingly IP enabled so reliant on network
- Autonomous ships would have less ability for manual override

**Risks / Impacts**
- Health and safety incidents
- Disruption of ship machinery

### People

**Objective**
- Operate the ship, ports, shipping company and enforce security measures

**Known vulnerabilities**
- Security not necessarily a specialism or priority

**Risks / Impacts**
- Ineffective security measures and response to incidents
Hull Systems

Mooring systems
Objective
— Promotes physical safety and efficiency during the ship docking process, can be remotely controlled via radio signals

Known vulnerabilities
— Networking and radio vulnerabilities

Risks / Impacts
— Denial of service and delays
— Destruction to ship / port

Sensors and sensor systems
Objective
— Data on temperature, humidity, position, speed, weight, etc.

Known vulnerabilities
— SONAR detects objects underwater but has had problems with signal congestions

Risks / Impacts
— IP enabled SONAR management systems could be flooded with data to cause congestion and potential destruction of the ship
Maritime has fallen victim to multiple cyber attacks, resulting in severe consequences to finances and operations.

Nation states

Nation state intelligence-gathering operations are highly likely to target maritime entities connected to disputed waterways and regions, or areas of strategic military importance. There is evidence that nation states are testing offensive cyber techniques to disrupt shipping operations. These kinds of attacks will likely remain rare but deliver a considerable impact, particularly if coupled with traditional military operations.

Nation state cyber threat actors typically gather intelligence (‘cyber-espionage’) to support political, military or economic goals. Their targets include intellectual property, commercial details, defence plans, and personal data on individuals of interest. For example, in March 2018, the ‘Leviathon’ cyber-espionage group was discovered engaging in network intrusions targeting information held by engineering and maritime organisations connected to the South China Sea[1]. This area is of strategic focus for the Chinese government, which seeks to assert dominance through their territorial claim; the disputed waters are also claimed by multiple other nations in the region.

Although Leviathon’s exact motive was not made clear in public reporting, presumably the targeted information provided a strategic advantage to the nation state sponsoring the group. Around GBP 2.33tn of shipborne trade passes through the South China Sea each year; that, coupled with possible reserves of oil and natural gas and rich fishing grounds, make it an extremely valuable asset to national economies[2].
1. INITIAL ACCESS
Technique
The Leviathon group sends emails impersonating legitimate entities to potential victims and includes malicious file attachments/URLs; this is known as spear phishing.

Mitigation
Without appropriate anti-virus protection and email/email attachment protection mechanisms, organisations face a serious threat from phishing attacks like these.

2. EXECUTION
Technique
Email attachments and malware delivered by malicious pop-up “warning dialogues” sent from attacker-controlled websites launch their code on the victim’s devices, leveraging administrative tools in the process.

Mitigation
User awareness is often the best protection against this stage; avoiding strange attachments and links can make a great difference. Further local controls to restrict use of administrative accounts would assist in preventing this execution of code.

3. PERSISTENCE
Technique
Further management applications within Windows are used by this group to execute code which embeds the group within the compromised systems, ensuring that a simple reboot will not remove their code.

Mitigation
Advanced Windows management tools should be carefully controlled, and remote access to them blocked whenever possible.

4. PRIVILEGE ESCALATION
Technique
This group uses tools which automate different password combination requests to “crack” user logins and gain access to systems with higher levels of access to the victim’s systems.

Mitigation
Strong passwords, password failure limits and the avoidance of duplicated passwords across systems will greatly complicate this stage of an attack.

5. DEFENSE EVASION
Technique
Attackers made use of stolen code-signing certificates to make malicious code appear trusted. Further to this, code is encoded in such a way that its contents are hidden, and only revealed when additional malicious programs decode the malicious content for execution.

Mitigation
Tools that restrict code execution and unexpected system calls can be used to hamper collection activities, catching both unauthorised applications and subverted applications exhibiting strange behaviour.

6. DISCOVERY
Technique
Malware is used to discover file directories and listings on compromised systems, identifying data and IP of interest to the attackers.

Mitigation
Restricting the behaviour of applications through the control and monitoring of system calls can restrict the ability of malware to locate valuable data, and improve chances that this data discovery is detected.

7. COLLECTION
Technique
Malicious code collects a range of materials for relaying to attackers, including discovered files, screen dumps, emails, and video/audio from the area around a compromised host.

Mitigation
Tools that restrict code execution and unexpected system calls can be used to hamper collection activities, catching both unauthorised applications and subverted applications exhibiting strange behaviour.

8. EXFILTRATION
Technique
To complicate detection, data removal by the attackers is performed using a different communications protocol from the main channel used by the attackers to connect to their software.

Mitigation
Filtering of communications protocols at the firewall level can complicate data exfiltration. This can be combined with the use of the application whitelisting tools mentioned in earlier steps to further complicate attempts to move data.

9. COMMAND AND CONTROL (C2)
Technique
Leviathon uses tools to copy or upload files from one system to another to command staged operations. Communications can involve user profiles on legitimate web services such as Github that are used to issue commands to malware.

Mitigation
Careful limiting of the websites and other communications mechanisms which users are allowed to use in their day to day activities will cut down on the channels available to malware, complicating the command and control of infected devices.
In addition to the general threat of network intrusions, there is a growing concern that hostile nation states may also seek to target maritime entities in ‘offensive’ cyber operations aimed at warfare and disruption.

In June 2017 the Russian military was suspected of testing a new system to misdirect onboard GPS in the Black Sea[3], which left at least 20 ships whose navigation systems showed their locations as 32km inland. The same year, South Korean officials complained to the United Nations that North Korea had used GPS jamming attacks against civilian ships[4]. This kind of attack can enhance traditional military interventions and will likely be used in tandem in future conflict.

**Cybercrime**

Although most cybercrime affecting the maritime industry has not been through direct targeting, there are examples of organised criminals and pirates doing so. With an increased prevalence of piracy specifically targeting the petroleum and gas industries (‘petro-piracy’), it is a realistic possibility that cyber attackers will begin to favour maritime targets.

The maritime industry has been subjected to cybercrime much like other industries, although in most reported incidents the targets were not the industry itself; rather, some companies indiscriminately became victims. In 2017 Maersk experienced a destructive attack using the ‘NotPetya’ ransomware, not because of the nature of the business but because Maersk used specific Ukrainian accounting software targeted by the attackers[1], (see timeline on Page 11).

On rare occasions, organised crime groups (OCGs) have taken a direct interest in targeting the maritime industry, particularly ports[2]—a nexus point for the illegal smuggling of people and drugs. In a now-seminal example of cyber-attack techniques enabling conventional organised crime, between 2011 and 2013 drug traffickers recruited attackers to breach IT systems that controlled the movement and location of containers. The system access gave the attackers the location and security details of containers, allowing the traffickers to send in drivers to steal cargo before the legitimate owner arrived[3].
Piracy continues to present a significant problem to mariners, and can incorporate cyber attack techniques. In 2016 investigators reported that pirates had used information stolen from a global shipping company’s servers to target and capture cargo ships[4]. With bill of lading information obtained via a web-borne attack on the company’s content management system, the pirates pinpointed valuable cargo quickly before disembarking.

Piracy is particularly a concern in the Gulf of Guinea (GOG) surrounding West Africa. In the first nine months of 2018, of the 156 piracy incidents reported to the International Chamber of Commerce, 57 were reported in the GOG region[5]. The West African peninsula is likely to be a central focus for the oil and gas industry – as well as organised criminal elements. Continued insecurities across this region have enabled a steep rise in petro-piracy, and there are new projects to extract some of the estimated 15tn cubic feet of recoverable gas from the West African coastline[6]. Not only are shipments likely to be the targets of increasing criminal hostility, but the production and drilling centres are, in their own right, attractive to criminals.

What form attacks will take is unclear; however, it is not beyond reason to foresee scenarios where cyber techniques could facilitate conventional organised crime and piracy targeted at the maritime transport of oil and gas. One such feasible scenario is a targeted ransomware attack halting or significantly damaging production and transport of oil and gas, by blocking access to one or all relevant computer systems. Similarly, the use of GPS jamming or spoofing by pirates could present an entirely new set of economic opportunities for pirates wishing to board ships before interdiction vessels arrive.
The maritime targets of hacktivism are likely to be those involved in controversial industries, such as whaling. Companies associated with fishing, marine farming, and natural resources transportation could also feasibly find themselves at the centre of unwanted attention, due to environmental protest. Typical tactics include unsophisticated denial of service attacks, website defacements, data leakage and ‘doxing’ (making private information available online).

The low threat hacktivists present to the maritime industry can be attributed to their limited technical capabilities and low intent. They have targeted shipping companies, but the impact has been minor. In 2015 a hacktivist group claimed to have attacked the website of an Icelandic fishing company in protest of its alleged involvement in whaling[1]; there was no business disruption, but negative press coverage did arise.

Hacktivism

Although the threat to the maritime industry from most online activists ('hacktivists') is low, more committed and capable vigilante attackers represent a significant threat.

Hacktivists are ideologically motivated threat actors who usually seek to draw public attention to causes through cyber attacks. Hacktivists can be self-identifying groups or lone actors and they typically have an overt internet presence, using social media to publicise campaigns. Causes adopted by hacktivists can include anti-corruption, human rights, animal rights, or environmental or political issues.

Some businesses that are seemingly unrelated to hacktivist issues have found themselves victims of attacks. A cyber attack on Nissan in 2016 was attributed to the company being Japanese and in protest to nations penchant for whale hunting in the Antarctic. The attack affected their customer-facing online services and was despite the company seemingly having no connection to whaling[2].

A few online vigilantes have proved more sophisticated capabilities, making them an existential threat to certain businesses. Although not linked to the maritime industry, 'commercial spyware' providers are among the tools available to hacktivists that pose a potential threat to maritime entities. A hacktivist calling them self 'Phineas Fisher' has conducted attacks in protest of services provided to alleged unethical government regimes. In 2015 the hacktivist operated commercial spyware against one Italian company, publicly releasing a huge amount of sensitive company information and causing a devastating impact on its reputation and operations[3].

Issues such as the environment may provoke hacktivists into pursuing targets involved in the transport of oil and gas. One long-running hacktivist campaign, known as OpGreenRights, has motivated attacks on companies seen as responsible for pollution and climate change. In November 2018 attackers claimed to have defaced various Italian entities in the name of the campaign.
The reported risks in the maritime industry are almost exclusively focused on financial loss for shipping businesses. Although there is worry about the potential for negative impacts stemming from cyber issues with shipboard systems, these have yet to occur in a measurable way. The industry is stuck between two areas of risk focus – those involving ports/cargo terminals and those involving vessels – and we feel they should be tackled in different ways.

Many of the best cyber-security practices today rely on threat intelligence and an analysis of the risk posed to a specific system. Impact is often thought of as a business event, causing loss of revenue and reputation or an increase in costs. This largely works for non-operational outcomes, but does not translate well for physically based risks.

This section discusses key risks inherent to the threats outlined above, looking at land and sea operations, and proposes recommendations to address these risks.

Risks to ports and cargo terminals
Central shipping locations have always been a focus for criminals. Whether the aim is theft, smuggling, or fraud, the asset-rich and chaotic port environment presents opportunities for illegal profit. Our research shows that criminals often target companies that process a high volume of business-related transactions, and often focus on a particular sector or industry to increase returns on their investment of time and resources; shipping businesses are as likely as any other to be a target.

Incorporating digital tools into the day-to-day activities of cargo management has not removed the threat of crime, but has simply shifted criminals’ focus to digitally enabled activities. We have seen cases of a shipping entity’s systems facilitating a smoother process for high-seas piracy, where technology has created more efficient processes for drug smuggling, and where new communications channels have enabled a more straightforward means of conducting fraud. The crimes have not changed, but the tools that make operations run more smoothly have made crime more efficient.

Most systems in ports and terminals match those of any commercial office: email, telephony, and other standard IT elements form the backbone. Maritime businesses’ additional vulnerability is found in the systems responsible for planning and tracking voyages and cargo. Terminal Operating System (TOS) software tracks cargo from the point it arrives at a port until the time it leaves, maintaining a view of loading and unloading, cargo movements through customs and any inspections, and the collection or deposit of cargo by a customer or third-party shipping company. This centralisation of information brings smooth and integrated operations, along with a target for criminals wishing to manipulate cargo contents. A shipping company’s marine fleet-management software also provides tracking information that can be a rich source of data for pirates and criminals attempting to track goods between ports.

Criminals have already manipulated shipping technology to favour illegal operations

Berthing fraud
In 2017 an MDR Cyber shipping client was targeted by email invoice fraud as part of the berthing process. One of the company’s ships had made a port call to discharge cargo, and commercial agents had been appointed. As cargo was being discharged, emails that had been created to mimic those of the operations team were used to alter bank account details for berthing payments. This led to a loss of approximately USD 100,000.

The global nature of the shipping supply chain presented issues in this matter; as it required law enforcement involvement in multiple countries. Our investigation uncovered a campaign with 25 targets across the shipping sector. The attackers were well versed in the processes used in shipping; they targeted a variety of agents, fuel providers, and engineering firms with whom shipowners and operators would interact. We attributed the attacks to locations in the UK and also found links to Nigeria.
Smuggling
Ports have always had to work hard to prevent smuggling, but cyber-enabled criminals have found ways to make illegal shipments harder to catch. The systems now used to track and manage cargo through the shipping lifecycle gather in one location all data relating to a shipment. Criminals who access that data gain a complete view of the cargo in port, and can plot a safe path for smuggled goods through the customs inspection process. Such an outcome, if unaddressed, could lead to a strained relationship between ports and customs / law enforcement. It could also potentially lead to liability issues if a port’s cyber-security protection was judged to have been inadequate to prevent crimes.

Cyber piracy
Piracy has occurred in coastal areas for as long as there has been shipping on the high seas; cyber-enabled piracy is just a new development in this age-old problem. The IT systems that track cargo are centralising data that could be of value to pirates. Pirate groups that access the data contained in a shipping firm’s container management system could use it to identify particularly valuable cargo, and then target that cargo while the containers are at sea. Such an attack could erode trust in a targeted shipping firm over time, leading to business loss and increased insurance premiums.

Fraud
Fraudsters are particularly attracted to financial transactions that involve substantial regular transfers in a fast-moving environment. The introduction to financial systems of insecure communication protocols, such as for email, has led to considerable fraud. Criminals can impersonate parties in transactions, and, if unchecked, can exploit communication channels to extract funds from organisations, such as during the process of paying mooring fees.

Significant business disruption
The increased reliance on the availability and integrity of new technology systems and controls leads to a clear risk for ports, and on ships. Without easily deployed manual backups, any attack able to disrupt a system – such as for container management – could bring operations to a standstill. The fall-out can include significant financial effects on the terminal operator, as well as on all clients and shipping operators that depend on it for their own operations.
Risks to vessels
Risk profiles for vessels are dynamic and depend on cargo, geographic position, shipborne technology, and competence of the crew. Carrying a cargo of fish in the English Channel carries with it a very different risk than carrying hydrocarbons through the Strait of Malacca.

Large vessels are similar in size and operational complexity to many land-based businesses; they could be considered ‘floating enterprises’. Unlike offices and factories, however, their cargo can vary and they can move through geographic regions that present different and changing risks.

This complexity can be daunting, especially because few vessels regularly carry cargo that would justify expensive cyber-security tooling and operational processes. Maritime leaders need to identify a realistic level of expenditure for their tooling and cyber-security processes, or risk becoming an industry where every vessel is prepared to handle any cargo.

Risk of damage to ship
- AIS data is compromised and subtly changed over time so that the ship is gradually steered off course and other ships appear untrue in digital maps
- Over reliance on digital navigation and data results in the ship crashing, especially in narrow channels such as Panama canal, causing damage to ship, injury and financial impacts

Risk of ceasing imports
- Targeted malware attacks bring down port facilities and operators
- Ships unable to dock and offload cargo
- Serious risks to UK economy after three days

Risk of cyber enabled financial fraud
- Threat groups spoof emails to shipping companies fraudulently posing as port companies requesting payment for docking
- Shipping companies lose significant amounts of money impacting profits and reputation

Risk of theft
- Cargo tracking systems first compromised and criminalised to target cargo which can have high value on black market e.g. pharmaceuticals

Risk of Piracy
- Not only can cargo tracking systems be compromised to identify that a ship is carrying high value goods, such as gold; but also
- Pirates will be able to spoof the position of target ships who respond to ships in distress take longer to locate ships under attack

Fruit & coffee
Pharmaceuticals
Branded clothes
Gold & precious metals
Cars

Salvador, Brazil
Lagos, Nigeria
Al Faw, Iraq
Plymouth, UK
Los Angeles, US
Hong Kong

Higher risk of cyber attack/ cyber facilitated crime.
Additional measures should be in place to address these risks
The risks faced by vessels are as diverse as the systems needed to maintain them, as can be seen in the figure above. Some particular risks deserve more immediate attention, due to a combination of exploitability, criticality, and known attacks; they are described as follows.

**GNSS/GPS disruption**

In oceangoing vessels, the technologies used for navigation and timekeeping are of particular concern for two reasons: the ease with which they can be disrupted, and the almost complete reliance on them to navigate, particularly by younger mariners.

GPS has been in use for more than 40 years, and the vast majority of vessels now rely on it. Although manual tools exist, they are rarely used.

This heavy adoption poses a risk that has manifested in several instances; a GPS or Global Navigation Satellite System (GNSS) can be spoofed or blocked, seriously disrupting navigation and leading to such outcomes as: extended transit times; violations of maritime borders, resulting in the detention of vessels; and, in extreme cases, even the grounding of vessels. Backup navigation capabilities are critical. Nations such as South Korea and the United States are working to deploy coastal navigation eLoran beaconing systems, but these will not assist mariners out of coastal range. Mariners must be aware of that and capable of undertaking manual navigation when necessary; celestial navigation skills need to be practised to be maintained.

**Automatic identification system compromise**

Automatic identification systems (AIS) are used for global-level vessel tracking and local navigation, making them an ideal target for disruption by attackers. In low-visibility conditions, AIS and radar can be critical for preventing accidents in busy waters; relying solely on compromised AIS information could result in ship collisions, leading to cargo loss, ship damage, and even loss of life.

As with GNSS/GPS, the mechanisms involved in AIS message delivery are designed for simplicity and resilience, not security, and there is demonstrable scope for attacks. Attention has been focused on the security of this system for many years, and practical attacks have been demonstrated.

**Mariners’ narrow skillsets**

A significant element to the risks faced by the maritime industry lies with the mariners. As the industry has evolved, they have become more and more reliant on technology; these are highly skilled and specialised workers who have not, until recently, had to worry about cyber-security risks at sea.

As a result of this reliance, newer maritime staff may struggle to handle cyber incidents that disrupt relatively new services and tools. We have found through interviews and discussions that there is a perception among industry experts that younger mariners rely heavily on technology with no consideration to the wider risks. It is believed by these industry experts that they can demonstrate less initiative to question unusual GPS signals and are less likely to use manual means to navigate when there are doubts regarding the accuracy of the GPS service.

---

...a GPS or Global Navigation Satellite System (GNSS) can be spoofed or blocked, seriously disrupting navigation and leading to such outcomes as: extended transit times; violations of maritime borders, resulting in the detention of vessels; and, in extreme cases, even the grounding of vessels.
Increasing regulatory requirements across the maritime industry will pile the pressure on.

The maritime industry is facing a gradual increase in the level of cyber security governance and regulation. This was prompted by an awareness of the criticality of maritime services, combined with a greater understanding of the vulnerabilities in many of the technologies used by the industry, which has raised alarm bells. The increase has been gradual, initially driven by the need for physical security when piracy was a particularly serious concern, and now branching out to include cyber-security.

What follows are the main regulations incorporating cyber-security in the industry.
Stormy seas ahead Cyber-security guidance for the maritime industry

To improve cross-border collaboration and cyber-security risk management, the Network and Information Systems Directive (NISD) sets standards of security for the maritime industry. Introduced in 2017, it requires affected parties to:

- implement measures to continuously and adequately assess risks and then prevent them;
- seek systems security assurance, including those outsourced to third parties, to support appropriate risk management; and
- establish incident response strategies to minimise effects, including defining when to contact a member state’s Computer Security Incident Response Team.

The NISD applies to entities that depend on information systems to provide ‘essential services’ to customers of the European Union. In terms of how this applies to the maritime industry, Annex 2 of the regulations says the directive applies to:

- freight and passenger water transport, including inland, sea, and coastal;
- managing bodies of ports;
- port facilities (e.g. anchorages, berths, etc.);
- entities operating works and equipment contained within the port; and
- operators of vessel traffic services, including any service to improve safety/efficiency of traffic, as well as interact with or track it.[1]

This regulation is already in force, meaning any organisations not already compliant should have a plan to address its requirements.

**NISD**

**SOLAS and ISPS**

The Safety of Life at Sea (SOLAS) and its amendment, the International Ship and Port Facility Security (ISPS) Code, have formed the basis for international shipping security. They outline the requirements to which contracting governments, port authorities and shipping companies must adhere, to in order to maintain secure operations at sea.

The framework requires such entities to cooperate in assessing security, detecting threats, and implementing security controls for ships and ports used in global trade.[1] Each entity needs to have identified security governance roles and responsibilities at multiple levels, from strategic to operational, to ensure they can assess and implement security plans. Although cyber-security is not explicitly mentioned, these roles are increasingly expected to address such risks in line with the recommendations of the MSC-FAL.1/Circ.3.[2]

**Safety Management System**

Most ships’ safety management systems (SMSs) do not currently contain cyber-security–relevant elements, but this is set to change. The 98th session of the IMO Maritime Safety Committee accepted the MSC-FAL.1/Circ.3 ‘Guidelines on maritime cyber risk management’ as a recommendation, meaning Ship Security Officers (SSOs) and chief security officers (CSOs) should be looking to incorporate cyber-security elements into their SMSs. Further to this, by 2021 it is recommended that all SMSs should contain some aspects of cyber-security, including strategies for risk remediation, and core cyber-security processes and practices, such as account management. The precise details of what to include are not entirely clear; CSOs will need to consider whether they have identified and addressed all risks being faced by their ships, and document their controls appropriately.

**Potential future developments**

Future safety-focused regulations will likely encompass cyber-security and resilience principles. Many maritime industry entities already have commercial reasons to reduce risk and protect their businesses, but an agreed and enforceable minimum standard of cyber-security for companies and vessels will ensure all participants are on a level playing field.

Approaches such as the NISD, with its business-level criteria for risk management and assurance of security, create this protection for shipping businesses in support of the European economy. However, wider guidance through the IMO is needed to extend the reach of such regulations to vessels themselves, and to all flag carriers.

...by 2021 it is recommended that all SMSs should contain some aspects of cyber-security, including strategies for risk remediation, and core cyber-security processes and practices, such as account management.
Shipping will only work if responsibility is shared: industry and organisations must invest in cyber security.

Although not insurmountable, the issues faced by the maritime industry require careful consideration. Work is needed at the industry level, as well as within individual organisations.

Industry action points

**LEARN FROM CORPORATE LESSONS**

At an industry level, cyber-security tooling and processes need to be aligned with new standards across organisations, ideally by using existing work from the corporate realm. As has occurred in many corporate sectors, a common set of security principles can be developed and applied to the vessel and port contexts.

Standards for security will, no doubt, increase costs in the maritime supply chain – and will likely require regulation for enforcement – but these standards are essential to securing it.

**ALIGN SAFETY AND SECURITY**

Safety is a well-understood concept within the maritime community, and regulation has helped reduce the likelihood of large-scale disasters, even if safety lapses still occur on a smaller scale.

A potential next move to consider is identifying specific cyber-security failure risks as safety hazards; other industries, such as energy, have begun analysing their systems to understand which are critical to certain operational outcomes. This allows cyber-security to be improved for the systems most likely to cause high-impact failures.

Adding any cyber-security requirements that stem from such analysis to the current SOLAS audit process, as well as modifying the regulations for future vessel construction, may help drive a culture of security onboard a vessel. It could also establish a minimum baseline of planning and technical controls.
Individual action points

Individual organisations must take steps to ensure readiness for potential cyber-security incidents. We recommend a three-step approach:

1. Assess
   Build a view of your risks and the issues others are seeing;

2. Protect
   Implement the tools, processes, and culture to protect your organisation; and

3. Respond
   Put plans in place to handle a cyber-security incident.

Assess
- Understand your risks:
  Each shipping company, port facility, and vessel should identify and understand the criticality of their assets. This criticality should be based on the potential financial, operational, regulatory, and reputational impacts that would occur if they were disrupted or destroyed. Additionally, there should be close monitoring of the threat landscape, to fully identify risks to the operations of the maritime industry; those who have been delegated security responsibilities should be tracking who may want to target either them specifically, or the industry as a whole, what their motives could be and how they could approach an attack.

- Share information:
  Often the improvement of cyber-security is hampered by a lack of information, which makes building a business case difficult. Without knowing what is happening to other, similar organisations and the cost it is creating, many organisations assume they are not at risk or have over- or under-spent on cyber-security. Sharing information among industry participants helps deliver a true picture of the risks to each business. It also has the benefit of helping protect the industry as a whole, in turn protecting each of its participants.

Protect
- Invest in security culture:
  As part of the move to implement cyber-security, SSOs and CSOs will need to work together to disseminate an understanding of cyber-security across the business. Cyber-security plays a role in the security of IT and operational technology (OT) systems; as such, it is important that all staff are aware of the risks, and how a cyber attack might manifest in their area.

- Prevent and detect:
  As part of ongoing governance, security should be continuously assessed to identify control gaps mapped back to risks identified. It is no longer good enough to simply tick these off a list; controls should be tested to check they are operating effectively, to ensure risk is reduced to an acceptable level. Following this, Cyber Security Officers (CySOs) (or the equivalent) should consider various factors when designing their security improvement plans, including cost, resources, scalability, longevity, additional security risks and business benefits.

- Prevent fraud:
  Firms need to consider the way they handle invoices and payments to external organisations. Fraudsters have been finding increasingly sophisticated ways to subvert standard payment management processes. This is occurring through the interception or hijacking of insecure communications, particularly where email is concerned. To address this, firms will need to reconsider how some basic activities are undertaken. More rigorous processes are needed to exchange information, particularly if payment details and other financial information is being exchanged.

Respond
- Implement an incident management plan:
  Having identified the risks a firm faces, a crisis management plan needs to be put in place for that time when a risk becomes an incident. This plan should tie together the shipside activities spelled out in each vessel’s SMS and the portside actions the back-office IT team needs to manage, ensuring a coherent and complete response to any incidents that arise.

- Build relationships:
  A successful response to incidents is rarely undertaken solo. Ensure that you have built the relationships with partner organisations, specialist suppliers, and law enforcement agencies that will allow you to react quickly and without resource constraints in the event of an incident.
Thanks/Acknowledgements

Maritime Cyber Threats research group - University of Plymouth.

Page 17

Page 20

Page 22
