A. TECHNOLOGICAL DEVELOPMENTS AND EMERGING ISSUES IN THE MARITIME INDUSTRY

1. Cybersecurity

The *Review of Maritime Transport 2017* highlighted examples of cyberattacks and vulnerabilities in navigation and other systems on board ships and in ports, including interference with automatic identification systems and electronic chart display and information systems, the jamming of global positioning systems and the manipulation of cargo and other ship and port systems, including through the introduction of malware, ransomware and viruses (UNCTAD, 2017a). In particular, 2017 was marked by some major global cyberattacks, including the use of ransomware, which demonstrated that such attacks, although not widely targeted at shipping as yet, may have substantial impacts (*The Guardian*, 2017; ZD Net, 2018). Such incidents and other attacks, including some mass global positioning system-spoofing attacks on ships in the Black Sea, emphasize the importance of cybersecurity and cyberrisk management. Further, there have been reports of links between cyberattacks and physical piracy, whereby pirates have reportedly identified ships with valuable cargo and minimal on-board security by infiltrating the systems of shipping companies.

Cybersecurity guidelines for the maritime industry

To date, internationally binding cybersecurity regulations for the maritime industry have not been adopted. However, the IMO guidelines on maritime cybersecurity risk management provide high-level recommendations with regard to safeguarding international shipping from current and emerging cybersecurity threats and helping to reduce related vulnerabilities (IMO, 2017a). The guidelines contain five functional elements for effective risk management in the maritime sector, namely to identify, protect, detect, respond and recover (IMO, 2017b). To be effective, these elements need to be incorporated into all aspects of shipping company operations and personnel management, in the same way that the industry has embraced a safety culture, with the adoption of the International Safety Management Code and the implementation of safety management systems. The main purpose of the Code is to provide an international standard for the safe management and operation of ships and for pollution prevention; it establishes safety management objectives and requires the "company", defined as the shipowner or any person, such as the manager or bareboat charterer, who has assumed responsibility for operating a ship, to establish a safety management system and to establish and implement a policy for achieving these objectives (IMO, 2018a). The Maritime Safety Committee of IMO, in its resolution 428(98) on cyberrisk management in safety management systems, encourages administrations to ensure that cyberrisks are appropriately addressed in existing systems as defined in the Code no later than the first annual verification of the company's document of compliance after 1 January 2021. This is the first compulsory deadline established in the maritime industry for cyberrisks and is an important step in protecting the maritime transportation system and the entire maritime industry from increased cybersecurity threats. In addition, the strategic plan for IMO recognizes the need to integrate new and emerging technologies into the regulatory framework for shipping by balancing the benefits derived from such technologies "against safety and security concerns, the impact on the environment and on international trade facilitation, the potential costs to the industry and finally their impact on personnel, both on board and ashore" (IMO, 2017c).

At the same time, the shipping industry is taking a proactive approach to incorporating cyberrisk management into its safety culture, to prevent the occurrence of any serious incidents. Guidance has been and continues to be developed by classification societies and other industry associations. Shortly after the approval of resolution 428(98), industry bodies released the second version of their guidelines on cybersecurity on board ships, which builds on the first version released in 2016 and is more comprehensive. The second version is aligned with the recommendations in the IMO guidelines, provides practical guidance on maritime cyberrisk management and includes information on insurance-related issues. The industry guidelines suggest that cyberrisk management should do the following (BIMCO et al., 2017):

> "Identify the roles and responsibilities of users, key personnel and management both ashore and on board; identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety; implement technical measures to protect against a cyberincident and ensure continuity of operations. This may include configuration of networks, access control to networks and systems, communication and boundary defence and the use of protection and detection software; implement activities and plans (procedural protection measures) to provide resilience against cyberincidents. This may include training and awareness, software maintenance, remote and local access, access privileges, use of removable media and equipment disposal; [and] implement activities to prepare for and respond to cyberincidents."

A significant new feature of the second version of the industry guidelines is the fact that they address insurance-related issues with regard to losses from a cybersecurity-related incident. The question of whether such losses should be covered by insurance has to date been unclear. In addressing this issue, the guidelines provide that "companies should be able to demonstrate that they are acting with reasonable care in their approach to managing cyberrisk and protecting the ship from any damage that may arise from a cyber incident” (BIMCO et al., 2017). There is currently no regulation in place on cybersecurity in international shipping, yet maritime companies need to be proactive in addressing cyberrisk, as suggested by IMO and various industry bodies, and can no longer claim ignorance with regard to cyberrisk management.

In addition, the guidelines state that in many markets offering marine property insurance, policies may cover loss or damage to a ship and its equipment caused by a shipping incident such as grounding, collision, fire or flooding, even when the underlying cause of the incident is a cybersecurity-related incident. At present, there are exclusion clauses for cyberattacks in some markets and, if the marine policy contains a relevant exclusion clause, the loss or damage is not covered. In such circumstances, the guidelines recommend that companies verify with insurers and/or brokers in advance with regard to whether the policy covers claims for incidents related to cybersecurity and/or cyberattacks (BIMCO et al., 2017).

More generally, limited data on the frequency of attacks, severity of losses and probability of physical damage remain a challenge to underwriters (All About Shipping, 2018).

Finally, with regard to liability for a cybersecurity-related incident, the guidelines state the following (BIMCO et al., 2017):

> "It is recommended to contact the [protection and indemnity insurance] club for detailed information about cover provided to shipowners and charterers in respect of liability to third parties (and related expenses) arising from the operation of ships. An incident caused, for example by malfunction of a ship’s navigation or mechanical systems because of a criminal act or accidental cyberattack, does not in itself give rise to any exclusion of normal [protection and indemnity insurance] cover. It should be noted that many losses which could arise from a cyberincident are not in the nature of third-party liabilities arising from the operation of the ship. For example, financial loss caused by ransomware or costs of rebuilding scrambled data would not be identified in the coverage. Normal cover, in respect of liabilities, is subject to a war risk exclusion and cyberincidents in the context of a war or terror risk, will not normally be covered."

The International Organization for Standardization standard 27001:2013 on information technology – security techniques – information security management systems – requirements, specifies requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization. The standard also includes requirements on the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in the standard are generic and intended to be applicable to all organizations, regardless of type, size or nature.

In addition, some countries have also prepared guidelines on cybersecurity. For example, the National Institute of Standards and Technology in the United States published the *Framework for Improving Critical Infrastructure Cybersecurity* in 2018 and the Institution of Engineering and Technology in the United Kingdom published the *Code of Practice: Cybersecurity for Ports and Port Systems* in 2016 and the *Code of Practice: Cybersecurity for Ships* in 2017. Such codes can help companies develop cybersecurity assessments, plans and mitigation measures and manage security breaches, and should be used along with ship security standards and other relevant IMO regulations.

The maritime industry continues to work on improving the understanding of cybersecurity issues and on increasing risk management. Shipping companies are integrating innovative security technologies with existing systems and software, to prevent internal and external cyberattacks with minimal human intervention, including by providing real-time alerts and blocking malicious files to prevent unauthorized access to critical systems and data (Marine Log, 2018).

In addition to verifying that technology, policies and procedures are in place, and that employees at all levels are aware of cyberrisks and how to react in the event of an attack, companies should consider in particular how data is stored and secured, given growing concerns with regard to data usage and security, for example on social media websites, which illustrate the complexity of potential security risks.

Data storage and security is particularly relevant, given the entry into force on 25 May 2018, of European Union Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which regulates how companies safeguard the processing and movement of the personal data of citizens of the European Union. Some of the key privacy and data protection provisions of the Regulation include requirements related to the consent of subjects for data processing; anonymization of collected data to protect privacy; provision of data breach notifications; safe handling of the transfer of data across borders; and the appointment by certain companies of a data protection officer to oversee compliance with the Regulation. Notably, it is not only companies in the European Union but any company that processes personal data related to offering goods or services or that monitors the behaviour of European Union residents, regardless of its location, that is subject to the Regulation. In the event of non-compliance, the Regulation provides for the administration of fines by supervisory authorities in member States.

2. Internet of things

The Internet of things refers to the network of connected devices with unique identifiers in the form of an Internet protocol address, which have embedded technologies or are equipped with technologies that enable them to sense, gather data and communicate about the environment in which they reside and/or themselves (see www.i-scoop.eu/internet-of-things/).

The shipping sector is increasingly harnessing data generated from satellite information and sensors linking equipment, systems and machinery to support informed decision-making related to route optimization, asset tracking and maintenance. Examples of applications in this domain include software that uses satellite-generated data to determine the most efficient route and estimate in real time the arrival time of vessels; and emerging intelligent containers that use sensors and telematics to track temperature, vibration, humidity and air quality during ocean transport, such as technology used by Maersk and the Mediterranean Shipping Company for reefer monitoring.

The Internet of things is also increasingly used in the industry to improve ship-to-shore connectivity and with regard to intelligent traffic management. A closer interface between ships and ports involves, for example, the use of big data analytics to reduce transit times and time lost when entering ports and other high traffic areas, thereby contributing to alleviating port congestion. For example, the digitalization collaboration initiative between the port of Rotterdam and IBM is helping to prepare this port to host connected ships in future and involves installing sensors across 42 km of land and sea to collect information about traffic management at the port with a view to improving safety and efficiency. A similar initiative between the Maritime and Port Authority of Singapore, academic institutions in Singapore, namely the Institute of High Performance Computing and Singapore Management University, and Fujitsu aims to embed the Internet of things and artificial intelligence technologies to enable long-term traffic forecasts, hotspot calculation and intelligent coordination models.

The Internet of things is also being used to develop systems that support navigation in challenging conditions, such as adverse weather conditions or in congested waterways. For example, in March 2018, Rolls-Royce launched an intelligent awareness system that fuses multiple sensors with intelligent software to create a three-dimensional model of nearby vessels and hazards, to increase safety (Rolls-Royce, 2018). Other applications of the Internet of things currently being tested include the departure of ships without human intervention, the remote controlling of the sailing of ships and the automatic docking of vessels to enable safe berthing (Wärtsilä, 2018).

When shipment events can be recorded in real time, this provides opportunities to optimize operations through blockchain, for example, to track spare capacity, improve connections between different legs of a journey in the global transport network and facilitate capacity-sharing to cope with overcapacity.

3. Use of blockchain

Blockchain is a distributed ledger technology that enables peer-to-peer transactions that are securely recorded, as in a ledger, in multiple locations at once and across multiple organizations and individuals, without the need for a central administration or intermediaries. One of the potential problems identified with regard to digital innovation in the maritime industry is insufficient electronic data interchange standardization and the need for a common data format to exchange information (*Combined Transport Magazine*, 2016). Electronic data interchange involves the electronic transfer from one computer to another of commercial or administrative transactions using an agreed standard to structure the transaction or message data (Economic Commission for Europe, 1996). This lack, along with a general lack of clarity with regard to the potential uses of blockchain, are among the factors that may explain the continued reliance in the shipping industry on paper-based documentation for deliveries of cargo containers.

Overall, blockchain holds potential to improve the security of the Internet of things environment. It addresses several aspects of information security, including confidentiality, integrity, availability and non-repudiation. For example, blockchain can protect the security of documents by blocking identity theft, through the use of public key cryptography; preventing data tampering, compared with document signing and other forms of electronic data interchange, through the creation of a public key and a private key; and stopping denial of service attacks, through the removal of the single target that a hacker may attack to compromise an entire system (Venture Beat, 2017). Allowing data to be managed through blockchain could therefore involve adding an extra layer of security and a gradual decrease in the use of centralized storage and processing for data.

In the maritime industry, blockchain has the potential to be used, among others, to track cargo and provide end-to end supply chain visibility; record information about vessels, including on global risks and exposure; integrate smart contracts and marine insurance policies; and digitalize and automate paper filing and documents. Such applications can help save time and reduce costs related to the clearance and movement of cargo. Several initiatives that focus on the container shipping segment have emerged, although blockchain is not yet fully implemented across the sector. Different varieties of maritime single windows are being developed to handle a quotation encompassing an entire ocean transport transaction, including booking, documentation generation and customs clearance. Maritime single windows imply potential efficiency gains and reduced costs for shipping companies due to standardization, which allows fragmented back-end systems to be superseded, and digitalization, which enables the elimination of intermediaries and inefficiencies related to the processing of documentation. For example, Maersk and IBM intend to establish a joint venture, which remains subject to the receipt of regulatory approvals. The aim of the venture is to develop an open trade-digitalization platform, designed for use by the entire industry, to help companies move and track goods digitally across international borders. The platform will use blockchain and other cloud-based, open-source technologies, including artificial intelligence, the Internet of things and analytics, delivered through IBM, and initially commercialize the following two core capabilities aimed at digitalizing the global supply chain (Maersk, 2018):

> "A shipping information pipeline will provide end-to-end supply chain visibility to enable all actors involved in managing a supply chain to securely and seamlessly exchange information about shipment events in real time; paperless trade will digitize and automate paperwork filings by enabling end users to securely submit, validate and approve documents across organizational boundaries, ultimately helping to reduce the time and cost for clearance and cargo movement. Blockchain-based smart contracts ensure all required approvals are in place, helping speed up approvals and reducing mistakes."

Another example of the use of blockchain in shipping is the completion by Hyundai Merchant Marine and other members of a consortium, in September 2017, of a pilot voyage applying blockchain that used secure paperless processes for shipment booking and cargo delivery. Hyundai Merchant Marine also reviewed the feasibility of introducing the technology into shipping and logistics and tested and reviewed the combination of blockchain with the Internet of things through the real-time monitoring and management of the reefer containers on the vessel (Lloyd's List, 2017).

In addition, in August 2017, Japan formed a consortium of 14 members to develop a platform for sharing trade data using blockchain, and Singapore-based Pacific International Lines signed a memorandum of understanding with PSA International and IBM in Singapore to develop and test supply chain business network solutions based on blockchain (Lloyd's List, 2017). Other initiatives include the cargo-booking portals of INTTRA and GT Nexus; the e-commerce business platform of CMA CGM; and the single window at the port of Cotonou, facilitated by the World Bank, to ease the management of vessel traffic, cargo and intermodal operations.

Potential future applications of blockchain in shipping could include smart contracts, which are contracts in the form of a computer programme run within blockchains that automate the implementation of the terms and conditions of any agreement between parties. Several smart contract prototypes have been launched that involve digitalizing electronic bills of lading and other trade documents, such as CargoDocs under essDOCS and Cargo X. However, the development of financing, payment and insurance aspects related to shipping remain in experimental and pilot stages. Once the use of such contracts reaches maturity, possible scenarios include the negotiation of freight prices directly between asset owners and their counterparts; the automatic processing of payments upon specified conditions being satisfied; and the issuance of insurance policies and settling of marine insurance claims through blockchain.

Blockchain has been deployed for the first time in the marine insurance sector. In May 2018, some industry actors collaborated with Ernst and Young and the software security firm Guardtime to launch the world's first blockchain-based platform for marine hull insurance. The platform, which is ready for commercial use, is expected to help manage risk for more than 1,000 commercial vessels in its first year and is planned to be implemented for other types of insurance for the marine cargo, global logistics, aviation and energy sectors (Splash 247, 2018). The platform "connects clients, brokers, insurers and third parties to distributed common ledgers that capture data about identities, risk and exposures and integrates this information with insurance contracts" and has the ability to "create and maintain asset data from multiple parties; to link data to policy contracts; to receive and act upon information that results in a pricing or a business process change; to connect client assets, transactions and payments; and to capture and validate up-to-date first notification or loss data" (Guardtime, 2017).

In addition, in 2017, two logistics companies, along with a containership operating company, completed a pilot project on blockchain-based paperless bills of lading that involved the use of an application for the issuance, transfer and reception of original electronic documents, and the containers, shipped from China to Canada, were successfully delivered to the consignees (Marine Log, 2017). The potential use of blockchain in this context is worth noting, as commercially viable electronic alternatives to traditional paper-based bills of lading have only recently emerged. Earlier attempts in this regard include the Bill of Lading Electronic Registry Organization (UNCTAD, 2003; www.bolero.net) and, more recently and with some success, essDOCS (www.essdocs.com). The main challenge in efforts to develop electronic alternatives to traditional paper-based transport documents has been the effective replication of a document's functions in a secure electronic environment while ensuring that the use of electronic records or data messages has the same legal recognition as that of paper documents. With regard to bills of lading, as the exclusive right to the delivery of goods has traditionally been linked to the physical possession of original documents, this includes in particular the replication in an electronic environment of the unique document of title function (UNCTAD, 2003).

Blockchain is also being used to improve tuna traceability to help end illegal and unsustainable fishing practices in the tuna industry in Asia and the Pacific. In January 2018, the World Wide Fund for Nature in Australia, Fiji and New Zealand, in partnership with a technology innovator, a technology implementer and a tuna fishing and processing company, launched a pilot project in the tuna industry in the Pacific that will use blockchain to track the journey of tuna "from bait to plate", strengthening transparency and traceability. The aim is to help end illegal, unreported and unregulated fishing and human rights abuses of seafarers and workers in the tuna industry and to address safety issues and broader impacts on the environment (The Conversation, 2018a).

Finally, blockchain is also proliferating in terminal and port development. For example, in April 2015, construction was completed of a fully automated and environmentally sustainable container terminal at the port of Rotterdam, and in September 2017, a field laboratory, Block Lab, was launched, which is aimed at developing applications and solutions based on blockchain.

Given that many blockchain initiatives and partnerships are proliferating, there is a need for the different applications emerging in the shipping industry to be interoperable. As noted by observers, "it would be detrimental for the shipping industry if the different factions and initiatives compete head on trying to make their specific blockchain technology choice the de facto standard for the industry" (JOC.com, 2018). Blockchain promises secure transactions yet, according to some specialists, it may not be as secure as generally anticipated. The use of blockchain may help solve some security issues but may also lead to new, potentially more complex security challenges, as some methods can possibly still be used to hack into a maritime transaction blockchain, including compromising the private keys of users; cracking cryptography, given continuous advances in computing; obtaining control of a majority of the mining nodes used to implement blockchain; and abusing vulnerabilities in smart contracts or coded programmes supported and run within blockchains (Marine Electronics and Communications, 2018a).

There are also concerns that many developing countries, in particular the least developed countries, may be inadequately prepared to capture the opportunities and benefits emerging from digitalization. There is a risk that digitalization may lead to increased polarization and widening income inequalities, as productivity gains might accrue mainly to a few, already wealthy and skilled individuals, given that "winner-takes-all dynamics are typical in platform-based economies, where network effects benefit first movers and standard setters" and that "the overall effects of digitalization remain uncertain; they will be context-specific, differing greatly among countries and sectors [and this] makes it increasingly important for countries to ensure they have an adequate supply of skilled workers with strong non-cognitive, adaptive and creative skills necessary for 'working with the machines'" (UNCTAD, 2017b). Additional concerns have been raised about digitalization, as it could potentially lead to a fragmentation of the global provision and international trade of services. This could open up new avenues for the development strategies of developing countries, yet it is unclear whether digital-based services could provide similar employment, income and productivity gains as manufacturing has traditionally done; "disruptive technologies always bring a mix of benefits and risks [but] whatever the impacts, the final outcomes for employment and inclusiveness are shaped by policies" (UNCTAD, 2017c).