5

LEGAL ISSUES AND REGULATORY DEVELOPMENTS

This chapter provides a summary of important international legal and regulatory issues, as well as some related technological developments during the period under review, and presents some policy considerations.

Among the issues worth highlighting is the need to implement IMO resolution MSC.428(98) of 16 June 2017 on maritime cyberrisk management in safety management systems, which encourages Administrations to ensure that cyberrisks for shipping are appropriately addressed in safety management systems, effective 1 January 2021. Thus, in preparation for its implementation – ahead of the first inspection by the international safety management auditors after 1 January 2021 and particularly during 2020 – shipping companies need to assess their risk exposure and develop information technology policies to include in their safety management systems, in order to mitigate increasing cyberthreats. Owners who fail to do so may risk having their ships detained by port State control authorities. Strengthening cybersecurity is likely to increase in importance, given that cyberrisks have grown, with greater reliance on virtual interaction as a result of the ongoing COVID-19 crisis.

In addition, work is progressing with respect to the development, testing and operation of maritime autonomous surface ships, and their market value is growing. Industry collaboration on the use of autonomous drones is also continuing, including with regard to inspections and commercial drone delivery to vessels anchored in port. The use of electronic trade documentation has increased in importance, particularly in the context of the COVID-19 pandemic, and international organizations and industry bodies have issued calls for Governments to remove restrictions on the use and processing of electronic trade documents, and where possible, ease requirements for any documentation to be presented in hard copy.

Other important regulatory developments relate to the reduction of greenhouse gas emissions from international shipping and other ship-source pollution control and environmental protection measures. Issues covered include shipping and climate change mitigation and adaptation; air pollution, in particular sulphur emissions; ballast water management; biofouling; pollution from plastics and microplastics; safety considerations of new fuel blends and alternative marine fuels; and the conservation and sustainable use of marine biodiversity of areas beyond national jurisdiction. In addition, an important development covered in this chapter includes a decision by the European Commission to extend the liner shipping Consortia Block Exemption Regulation[25] until 25 April 2024.

[25] Commission Regulation (EC) No 906/2009 of 28 September 2009 on the application of article 81(3) of the Treaty to certain categories of agreements, decisions and concerted practices between liner shipping companies (consortia).

LEGAL ISSUES AND REGULATORY DEVELOPMENTS

Legal issues

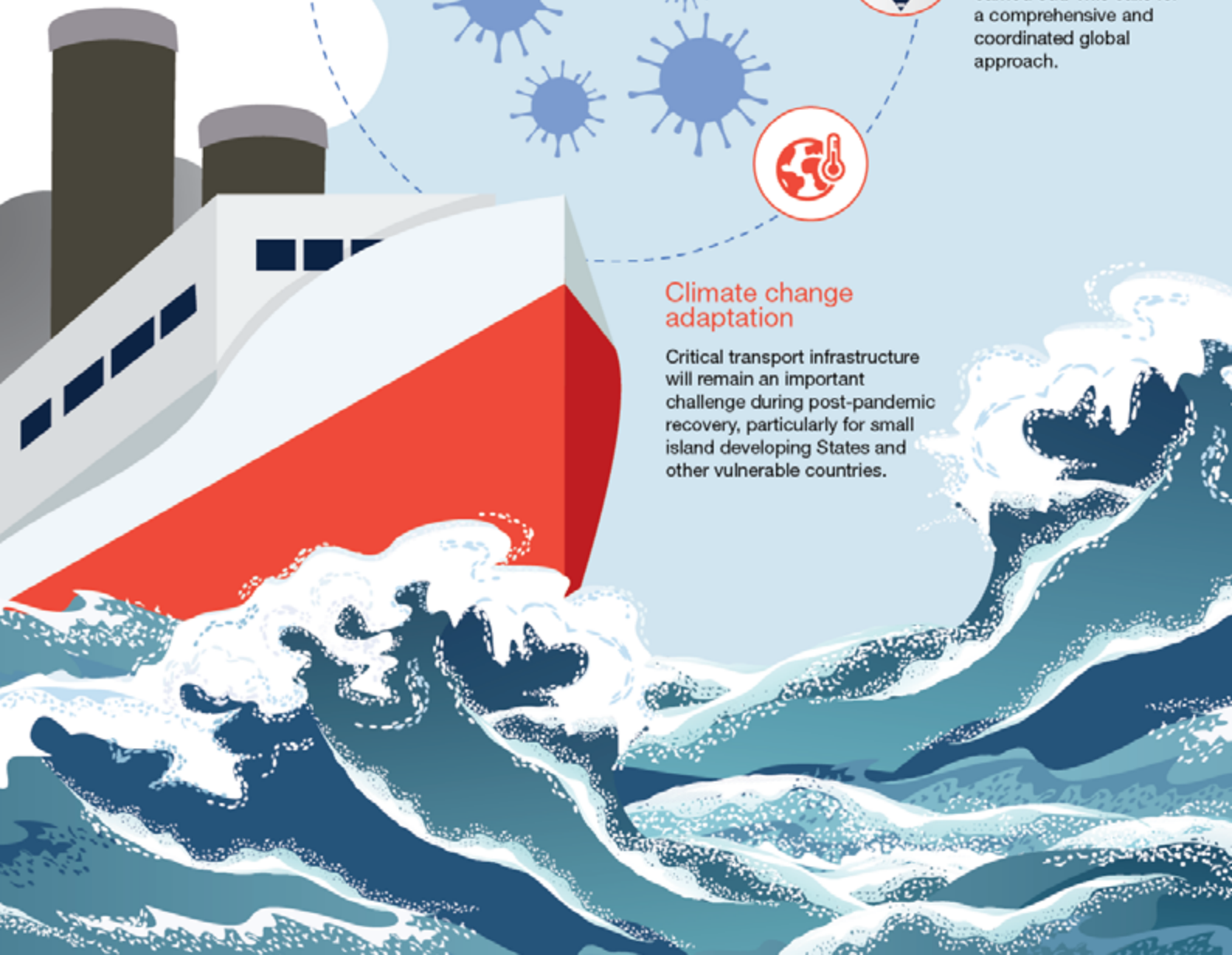
Coordinated government and collaborative industry action, as well as commercial risk-allocation through standard form contractual clauses, will be required to address wide-ranging commercial law implications of the COVID-19 crisis and ensure that legal and administrative systems do not become overwhelmed.

Cybersecurity

With increasing reliance on virtual interactions as a result of the ongoing COVID-19 crisis, and the related rise in cyberthreats and vulnerabilities, coordinated efforts to develop appropriate cybersecurity mechanisms should be pursued as a matter of urgency.

Sulphur limit

Despite some COVID-19-related disruptions in the implementation on **1 January 2020** of the mandatory IMO sulphur limit and the ban on the carriage on non-compliant fuel oil as of **1 March 2020**, steps should be taken to ensure that delays will not unduly impact full implementation.



Seafarers' travel restrictions

Designating seafarers and other marine personnel "key workers" will ensure that crew changes can be carried out. This calls for a comprehensive and coordinated global approach.

Climate change adaptation

Critical transport infrastructure will remain an important challenge during post-pandemic recovery, particularly for small island developing States and other vulnerable countries.

A. TECHNOLOGICAL DEVELOPMENTS AND EMERGING ISSUES IN THE MARITIME INDUSTRY

1. Ensuring maritime cybersecurity

Ship cybersecurity

Ships have become better integrated into information technology networks. Moreover, communication and operational processes have been further digitalized, and smart navigation and advanced analytics are being used to optimize ship operations and reduce fuel consumption and greenhouse gas emissions. In line with these recent trends, implementing and strengthening cybersecurity measures has become a priority for shipowners and managers. In 2019, cyberincidents were rated second among the top five risks for the maritime and shipping sector, according to a major industry survey (Allianz, 2019). While cyberrisks had already become a major concern, the COVID-19 crisis has compounded existing problems and provided a new impetus for action. The importance of cybersecurity is expected to grow further, given the increasing reliance on virtual interactions as a result of the pandemic, and the related rise in cyberthreats and vulnerabilities.

The Digital Container Shipping Association – a consortium of nine container lines[26] – recently published a cybersecurity implementation guide to ensure vessel preparedness for relevant IMO regulations, outlining best practices that would provide all shipping companies with a common language and a manageable, task-based approach for meeting the IMO implementation deadline of January 2021 (Digital Container Shipping Association, 2020a). The guide is in line with BIMCO and National Institute of Standards and Technology cyberrisk management framework guidelines, enabling shipowners to effectively incorporate cyberrisk management into their existing safety management systems. The guide aims to provide a management framework that can be used to reduce the risk of cyberincidents that could affect the safety or security of vessels, crews or cargo. It breaks down the BIMCO framework into themes and maps them to the controls that underpin the functional elements of the Institute: identify, protect, detect, respond, recover (Digital Container Shipping Association, 2020b). In January 2020, the first cybersecurity management system – that of the Nippon Yusen Kabushiki Kaisha Group – had already been certified by industry classification society Nippon Kaiji Kyokai, commonly known as ClassNK, as being compliant with the latest IMO guidelines (Nippon Yusen Kabushiki Kaisha Line, 2019).

[26] Maersk Line, CMA CGM, Hapag-Lloyd, Mediterranean Shipping Company, Ocean Network Express, Evergreen Line, HMM, Marine Transport Corporation and Zim Integrated Shipping Services, covering 70 per cent of world trade. The consortium was first launched in November 2018.

Among the relevant IMO instruments, the above-mentioned IMO resolution on maritime cyberrisk management in safety management systems affirms that an approved safety management system should take into account cyberrisk management in accordance with the objectives and functional requirements of the International Safety Management Code[27] and encourages Administrations to ensure that cyberrisks are appropriately addressed in safety management systems no later than the first annual verification of the company's document of compliance after 1 January 2021 (IMO, 2017a).

The International Safety Management Code, in force since 1 July 1998, is now more important than ever to ensure that vessels become cyberresilient and report any identified cyberrisk, given that the underreporting of cybersecurity incidents is considered a problem in the maritime industry (Safety4Sea, 2019a). Many issues may be identified on board ships that make them more vulnerable to cyberattacks, including unsecure networks and software, lack of seafarer training and insufficient protection of data. Shipping companies will need to consider these issues and include cyberrisk into their safety management systems, so they know how to deal with and approach a cyberincident. As this will require some time, all work should be completed ahead of the first inspection by International Safety Management auditors after 1 January 2021. Owners who fail to comply may risk having their ships detained by port-State control authorities that will aim to enforce the requirement in a uniform and equitable manner. At the same time, implementing cybersecurity is important to protect shipping assets and technology from mounting cyberthreats, in particular given that cyberrisks are expected to grow, with greater reliance on virtual interaction as a result of the ongoing COVID-19 crisis.

Cybersecurity is covered under the International Ship and Port Facility Security Code, in force since 1 July 2004 (see BIMCO et al., 2018 for related guidance). Thus, as set out in part A, section 8.4 of the Code, ship security assessment shall include, inter alia, "2. the identification and evaluation of key ship board operations that it is important to protect; 3. identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and 4. the identification of any weakness, including human factors in the infrastructure, policies and procedures".

[27] The main purpose of the International Safety Management 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 a safety management system to be established by "the Company", which is defined as the shipowner or any person, such as the manager or bareboat charterer, who has assumed responsibility for operating a ship. The company is then required to establish and implement a policy for achieving these objectives (www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx).

Part B, section 8.3 of the Code states that a ship security assessment should address, among others, the following elements on board or within the ship: "5. radio and telecommunications systems, including computer systems and networks, and 6. other areas that may, if damaged or used for illicit observation, pose a risk to persons, property or operations on board a ship or within a port facility".

With regard to cyberrisks, the IMO Assembly had as early as 2017 adopted a strategic plan that recognized the need to integrate new and advancing technologies into the regulatory framework for shipping (IMO, 2017b). In addition, to support effective cyberrisk management, two IMO committees, the Maritime Safety Committee and the Facilitation Committee, had adopted guidelines that provide high-level recommendations to safeguard shipping from current and emerging cyberthreats and vulnerabilities. These recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO (that is to say, the International Safety Management Code and the International Ship and Port Facility Security Code) (IMO, 2017c). These guidelines present five functional elements: to identify, protect, detect, respond and recover.[28]

Other useful guidance, standards and regulations, adopted at the international, regional and national levels, are described below.

European Union Network and Information Security Directive (EU) 2016/1148 requires all Member States to protect their critical national infrastructure by implementing cybersecurity legislation by May 2018 (European Union, 2016). Inter alia, the Directive in chapter 2 lays down obligations for all Member States to adopt a national strategy on the security of network and information systems; creates a cooperation group to support and facilitate strategic cooperation and the exchange of information among Member States; establishes a computer security incident response teams network; sets security and notification requirements for operators of essential services and digital service providers; and spells out obligations for Member States to designate national competent authorities, single points of contact and computer security incident response teams. The Directive covers organizations in vital sectors that rely heavily on information networks and are referred to as "operators of essential services", including those in energy, transport, utilities, banking and finance, digital services and health care. As noted in preambular paragraph 10, in the water transport sector, security requirements for companies, ships, port facilities, ports and vessel traffic services under European Union legal acts cover all operations, including radio and telecommunication systems, computer systems and networks.

International standard 27001:2013 of the International Organization for Standardization and International Electrotechnical Commission, commonly known as ISO/IEC 27001:2013, specifies the requirements for setting up, implementing, maintaining and continually improving an information security management system within the context of an organization (International Organization for Standardization, 2013). It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

The Framework for Improving Critical Infrastructure Cybersecurity of the United States National Institute of Standards and Technology was prepared to assist companies with their risk assessments by helping them understand, manage and express potential cyberrisks internally and externally (National Institute of Standards and Technology, 2018).

The Code of Practice on Cybersecurity for Ships of the United Kingdom was drawn up to help companies develop cybersecurity assessments and plans, and mitigation measures, and to manage security breaches; it should be used along with ship security standards and other relevant IMO regulations (Institution of Engineering and Technology, 2017).

Guidelines on Cybersecurity on Board Ships offer guidance to shipowners and operators on procedures and actions to maintain the security of cybersystems in the company and on board ships (BIMCO et al., 2018).[29] Both the IMO guidelines and the United States National Institute of Standards and Technology framework have been taken into account. The guidance specifies, among others, that company plans and procedures for cyberrisk management should be incorporated into existing security and safety risk management requirements contained in the International Safety Management Code and the International Ship and Port Facility Security Code.

In the Asia-Pacific region, for instance, many countries have developed cybersecurity legislation and policy, elements of which are applicable across all industry areas; they have also set up relevant implementing bodies and entities both at the national and regional levels. However, sector-specific guidance and initiatives tailored to business needs, or the provision of methods to address unique risks or specific operations in certain sectors, including in the maritime sector, appear to be limited in the region (BSA/The Software Alliance, 2015; North Atlantic Treaty Organization Cooperative Cyberdefence Centre of Excellence, 2019).

At the national level, for instance, the China Classification Society in July 2017 issued guidelines on requirements and security assessments of ship cybersystems, offering

[28] For information on a platform aimed at helping shipowners and operators to better understand their vulnerabilities and improve their cybersecurity processes and systems ahead of the IMO deadline, see Safety4Sea, 2020a.

[29] For additional industry guidelines, see also Safety4Sea, 2018.

solutions for the increasingly serious threat to ship cybersecurity (China Classification Society, 2017). In February 2020, the Republic of Korea released guidelines based on international standards for type approval of maritime cybersecurity to help inspect the cybersecurity level and functioning of cybersystems, including remote access equipment, integrated control and monitoring systems on board ships (Safety4Sea 2020a).

Port cybersecurity

Ports are important to keep supply chains moving and economies across the world functioning. While they are becoming "smart", relying more on technologies and digitalization to become more competitive and optimize operations, ports are also facing increased cybersecurity challenges and threats. A recent report on port cybersecurity identifies the following good practices for terminal operators and officials responsible for cybersecurity implementation at port authorities (European Union Agency for Cybersecurity, 2019):

- Define clear governance concerning cybersecurity at port level, involving all stakeholders involved in port operations.
- Raise awareness of cybersecurity matters at port level and foster a cybersecurity culture.
- Enforce the technical cybersecurity basics such as network segregation, updates management, password hardening and segregation of rights.
- Consider security by design in applications, especially since ports use many systems, some of which are opened to third parties for data exchange. Any vulnerability in those systems can be a gateway to compromising port systems.
- Enforce detection and response capabilities at port level to react as quickly as possible to any cyberattack before it affects port operation, safety or security (see www.sauronproject.eu/).

Prompted by the Ryuk ransomware attack on enterprise environments in December 2019[30] (National Cybersecurity Centre, 2019; United States Coast Guard, 2019a) and by concerns that the maritime network is vulnerable to cybercrime (Riviera, 2019; United States Coast Guard, 2019b), the United States Coast Guard issued new guidelines for dealing with cyberrisks at Maritime Transportation Security Act regulated facilities (United States Coast Guard, 2020). According to the guidelines, regulated facilities must assess and document risks associated with their computer systems and networks in a facility security assessment and address them in a facility security plan or alternative security programme. Following this, owners and operators must demonstrate compliance. To allow time for owners or operators of such facilities to tackle cybersecurity vulnerabilities, the initial implementation period is 1.5 years with no further need to update a facility security assessment or an alternative security programme until 30 September 2021.

Similarly, the Department for Transport of the United Kingdom updated its 2016 cybersecurity guidance for ports and the wider maritime industry against cyberthreats. The guidance aims to help ports develop cybersecurity assessments and identify gaps in their security, while providing advice on handling security breaches and incidents and defining clear roles and responsibilities to deal with cyberattacks (Institution of Engineering and Technology, 2020).

COVID and maritime cybersecurity

Maritime digitalization has been an ongoing trend for some time both on board ships and ashore. The COVID-19 outbreak has heightened the need for digitalization and has brought maritime industry stakeholders closer through the collaborative use of digital technologies. These include video conferencing and other online platforms, as well as the sharing and remote monitoring of data to ensure that supply chains continue to function (Riviera, 2020a; Riviera, 2020b). At the same time, reports indicate an increase in shipping cyberattacks of 400 per cent between February and June 2020 (Splash, 2020a). According to cybersecurity systems provider Naval Dome, the ability of companies to sufficiently protect themselves has been reduced by travel restrictions, social distancing measures and economic recession. However, the primary reason behind this spike has been an increase in malware, ransomware and phishing emails exploiting the COVID-19 crisis (Marine Link, 2020).

With regard to ports, for instance, the COVID-19 crisis demonstrated that while some port communities had already digitalized their business processes and developed into smart ports, many others were lagging behind, relying heavily on personal interaction and paper-based transactions as the norm, for shipboard-, ship–port interface- and port–hinterland-based exchanges. As highlighted in a recent port industry policy statement, only 49 of the 174 IMO Member States have functioning port community systems (International Association of Ports and Harbours et al., 2020a). In these circumstances, the main shipping and port industry organizations have launched a call to action to accelerate the digitalization of maritime trade and logistics.[31] They have set the following priorities:

- Assess the state of implementation and find ways to enforce the already mandatory requirements defined

[30] Encryption was used to block access to systems, devices or files until a ransom was paid.

[31] BIMCO, Federation of National Associations of Ship Brokers and Agents, International Association of Ports and Harbours, International Cargo Handling Coordination Association, International Chamber of Shipping, International Harbour Masters Association, International Marine Purchasing Association, International Port Community Systems Association, International Ship Suppliers and Services Association, and the Protect Group.

in the IMO Convention on Facilitation of International Maritime Traffic, 1965 to support the transmission, receipt and response of information required for the arrival, stay and departure of ships, persons and cargo, including notifications and declarations for customs, immigration, and port and security authorities, through electronic data exchange.

- Ensure the harmonization of data standards beyond the aforementioned Convention to facilitate the sharing of port and berth-related master data for just-in-time operation of ships and optimum resource deployment by vessel services and suppliers, logistics providers, cargo handling and clearance, thereby saving energy, improving safety and cutting costs and emissions. This can be achieved by using the supply-chain standards of the International Organization for Standardization, the standards of the International Hydrographic Organization and the *IMO Compendium on Facilitation and Electronic Business*.
- Strive for the introduction of port community systems (www.ipcsa.international/) and secure data exchange platforms in the main ports of all Member States represented in IMO.
- Review existing IMO guidance on maritime cyberrisk management with regard to its ability to address cyberrisks in ports, developing additional guidance where needed.
- Raise awareness, avoid misconceptions and promote best practices and standardization on how port communities can apply emerging Internet technologies and automation; facilitate the implementation of such emerging technologies and other innovative tools to increase health security in port environments; and develop a framework and road map to facilitate the implementation and operationalization of digital port platforms that can connect with hinterland supply chains as well, and where data can be securely shared.
- Establish a coalition of stakeholders willing to improve transparency of the supply chain through collaboration and standardization, starting with the overdue introduction of the electronic bill of lading.
- Set up a capacity-building framework to support smaller, less developed and understaffed port communities, not only by providing technical facilities but also by training personnel (International Association of Ports and Harbours et al., 2020a).[32]

[32] For more information and a list of maritime technology initiatives that have been made available to help the industry deal with the disruption caused by the pandemic, see https://thetius.com/maritime-technology-initiatives-supporting-the-industry-covid-19-response. Also see International Association of Ports and Harbours et al., 2020b.

Given that digitalization and cyberrisks and vulnerabilities are growing during the ongoing COVID-19 crisis and its aftermath, related capacity-building will be required for many developing countries. On a more general note, in the developing world at large, the lack of reliable and affordable Internet services and a widespread digital divide continue to be a major concern, which needs to be effectively addressed (see Economic Commission for Asia and the Pacific, 2019).

2. Technological developments in shipping

Autonomous ships, navigation systems and drones

Work is advancing on the development of maritime autonomous surface ships, drones and navigation systems (see also UNCTAD, 2018; UNCTAD, 2019a). In 2019, it was announced that the Mayflower autonomous ship[33] would be attempting the world's first unmanned transatlantic crossing from Plymouth, United Kingdom, to Plymouth, Massachusetts, United States in the second half of 2020. This was described as a symbolic voyage, whereby a new Mayflower would set sail 400 years after the historic voyage, this time using artificial intelligence and other advanced technologies, providing for safer navigation and hazard avoidance (Safety4Sea, 2019b). The full-size, fully autonomous research ship was launched on 16 September 2020 and during its journey would spend six months gathering data about the state of the ocean (BBC News, 2020).

According to a report by technology and innovation consultancy Thetius, the market for maritime autonomous surface ships is worth $1.1 billion annually and will grow by 7 per cent each year to $1.5 billion by 2025. In addition, 96 per cent of almost 3,000 patents relating to autonomous shipping technology worldwide were registered in China. According to the report, this will lead other nations to develop and implement autonomous shipping within five years (Thetius, 2020). The report does not appear to include COVID-19-related considerations, however.

Global navigation satellite systems, used for the safe navigation of ships, and automatic identification system signals via satellites, tracking ships around the world, are considered critical to improve the safety of ship navigation and the reliability of data for vessel tracking and analytics, including for insurance purposes (also see chapter 3A). However, the safety of such systems can be compromised by jamming, spoofing or hacking, as evidenced by various incidents, which can be dangerous and may lead to grounding and collisions.

[33] Partners in this project are International Business Machines, Promare and the University of Plymouth, United Kingdom.

Automatic identification system tracking of ships may be occasionally disrupted, as some vessels switch off their devices when they enter zones in which they are legally prohibited from performing fishing or other illegal activities. Therefore, it is important to strengthen both global navigation satellite systems and automatic identification system communications, which both use satellites. For instance, the European Space Agency has started developing a solution to mitigate risks for its services in this area (Digital Ship, 2020).

Industry collaboration is continuing with respect to drones as well, including for instance, the launching in Singapore of a ship-to-shore pilot project by Wilhelmsen and Airbus, which worked to deploy drone technology in real-time port conditions, delivering a variety of small, time-critical items to vessels anchored in port (Splash, 2019), as well as the first commercial drone delivery to such vessels. Drone deliveries can help save costs, time and carbon-dioxide emissions compared with traditional shipping and have reduced unnecessary human contact during the pandemic. The drones that were used in the project could only deliver a maximum of 5 kg loads over 5 km, but the company was planning to complete the development of a drone that could carry 100 kg loads over 100 km, by the second half of 2021 (Splash, 2020b). In addition, in June 2020, the industry-first inspection by an autonomous drone, of an oil tank on a floating production, storage and offloading vessel, was completed. The drone uses light detection and ranging to navigate inside the tank, where reception of satellite signals for accurate positioning is unavailable in this enclosed space, and a three-dimensional map of the tank is created. As the technology matures, drones are expected to navigate more autonomously (Riviera, 2020c).

With regard to regulatory issues and intergovernmental meetings related to technology in shipping, the IMO Subcommittee on Navigation, Communications and Search and Rescue met in January 2020. It discussed advances in modernizing the Global Maritime Distress and Safety System – under the regulations in chapter IV of the International Convention for the Safety of Life at Sea, 1974, that is to say, performance standards for navigational and communication equipment. Interested parties were invited to give a progress report on updates to the document entitled "E-navigation strategy implementation plan: Update 1" (MSC.1/Circ.1595). The Subcommittee also reviewed issues related to the long-range identification and tracking system and testing and operating of maritime autonomous surface ships. The Subcommittee's recommendations will be reviewed by the Maritime Safety Committee at its next meeting. The Committee was scheduled to meet in May 2020, but the meeting was postponed because of the COVID-19 crisis (IMO, 2020a).

Regulatory and other issues related to maritime autonomous surface ships were on the agendas of the IMO Legal Committee (scheduled for March 2020) and the IMO Facilitation Committee (scheduled for April 2020); both meetings also had to be postponed.[34]

Paperless bills of lading

Negotiable bills of lading are used for the carriage of goods by sea, particularly in containerized transport, which carries the world's manufactured cargo. They are also used in the commodities trade in cost, insurance and freight terms (commonly known as CIF). Bills of lading must be physically presented to the carrier to obtain delivery, due to their documentary security function and their key role as a document of title in international trade (see Gaskell et al., 2000; UNCTAD, 2003). For various reasons, despite numerous attempts over the past decades, commercially viable electronic equivalents have only recently begun to emerge (UNCTAD 2003). The International Group of Protection and Indemnity Clubs provides indemnity insurance to about 90 per cent of the world's ocean-going tonnage (International Group of Protection and Indemnity Clubs, 2020). The Group has recognized six electronic bill-of-lading systems or providers to date (United Kingdom Protection and Indemnity Club, 2017; United Kingdom Protection and Indemnity Club, 2020a; United Kingdom Protection and Indemnity Club, 2020b). Against this background, and in the light of the increased need for virtual interactions resulting from the ongoing COVID-19 crisis, recent developments and efforts to enable and promote paperless bill of lading solutions, including the following, are particularly worth noting.

The Digital Container Shipping Association announced plans to promote an initiative to enable the open collaboration necessary for achieving full electronic bill of lading adoption, based on the belief that an electronic bill of lading would be beneficial for all parties in container shipping (JOC, 2019). As part of this initiative, the Association aims to develop open-source standards for necessary legal terms and conditions, as well as definitions and terminology to facilitate communication among customers, container carriers, regulators, financial institutions and other industry stakeholders. In its view, carriers could reduce costs and inefficiencies associated with the manual creation of paper documents. If successful, ports and regulatory agencies would benefit from having access to the digital data within the electronic bills of lading, and irregular shipping patterns would be easier to identify.

According to research by the Association, paper bill processing costs three times as much as electronic

[34] IMO set a remote meeting plan for September–December 2020 (https://imo-newsroom.prgloo.com/news/imo-sets-remote-meeting-plan-for-september-december-2020).

bill of lading processing, which was determined to be an extra $4 billion annually in collective processing costs, at a 50 per cent adoption rate for the container shipping industry. With regard to the success of electronic air waybills for airfreight introduced by the International Air Transport Association in 2010, the Association suggests that a 50 per cent adoption rate may be feasible by 2030 if steps are taken now to begin standardizing electronic bills of lading (Digital Container Shipping Association, 2020c). This is an ambitious and worthwhile goal; however, air waybills, unlike negotiable bills of lading, do not serve as documents of title providing their holder with independent documentary security (UNCTAD, 2003). Therefore, there are fewer legal and regulatory problems associated with the use of electronic air waybills.

Progress is being made regarding acceptance of this technology by government authorities, banks and insurers, and this is likely to be accelerated as a result of the COVID-19 crisis. For instance, a number of Digital Container Shipping Association members had reported a sharp increase in electronic bill of lading adoption, in an effort to keep trade moving. As noted previously, the International Group of Protection and Indemnity Clubs has so far approved six electronic bill-of-lading systems or providers. As noted by the Association, in the case of negotiable bills of lading, the standard electronic bill of lading would likely have to be used in conjunction with new technologies, such as distributed ledger technology, peer-to-peer technology and blockchain technology, which offer potential solutions for eliminating the risk of a single catastrophic failure or attack that would compromise the integrity and uniqueness of an electronic bill of lading (Digital Container Shipping Association, 2020c; JOC, 2020).

Recently, Ocean Network Express, the world's sixth largest container line (see also chapter 2) became the latest shipping line to offer fully electronic bills of lading to their customers. The liner company recently announced that it had handled its first electronic negotiable bill of lading, using essDOCS's paperless document solution, CargoDocs, which is among the systems approved by the International Group of Protection and Indemnity Clubs (https://essdocs.com/). Ocean Network Express used this electronic bill of lading for a shipment of containerized synthetic rubber from the Russian Federation to China and is planning to allow customers to use electronic bills of lading on a regional and subsequently global basis commencing in the second quarter of 2020 as part of initiatives aimed at delivering an improved, digital customer experience (Ocean Network Express, 2020). Further, India is to integrate electronic bills of lading and digital documentation into the country's electronic port community system, incorporating the CargoX platform for blockchain document transfer into its infrastructure, to manage the secure exchange of data (Smart Maritime Network, 2020).

Given the number of earlier attempts to create commercially viable electronic alternatives to traditional paper-based bills of lading across the shipping industry, including, Bolero[35] and some other recent systems, such as essDOCS, the success of ongoing initiatives will remain to be seen. However, the COVID-19 crisis provides an added impetus for resolving long-standing legal and regulatory problems. The main challenge in efforts to develop electronic alternatives to the traditional paper bill of lading has been the effective replication of the document's functions in a secure electronic environment, while ensuring that the use of electronic records or data messages enjoys the same legal recognition as that of paper documents. For negotiable bills of lading, with the exclusive right to the delivery of goods traditionally linked to the physical possession of original document, this includes in particular, the replication, in an electronic environment, of the unique document of title function (UNCTAD, 2003). There are also concerns over legal enforceability, as not all Governments have legislative provisions to this effect in place.

Establishing the widespread use of a fully electronic equivalent to the traditional bill of lading will require much international cooperation and coordination to ensure that commercial parties across the world are readily accepting and using relevant electronic records, and that legal systems are adequately prepared. In addition, capacity-building may be required, particularly for small and medium-sized enterprises in developing countries that may lack access to the necessary technology or means of implementation. In this context, too, increasing cybersecurity and related capacity-building will be a matter of critical and strategic importance for the further development of international trade in an electronic environment.

The use of electronic trade documentation, including electronic bills of lading equivalents, has increased significantly in importance since the COVID-19 pandemic, and related physical distancing, teleworking and disrupted or suspended postal services have affected large parts of the world population. This matters, particularly since trade finance transactions typically require significant levels of in-person review and processing of hard-copy paper documentation. In these circumstances, international organizations and industry bodies have issued calls for Governments to remove restrictions on the use and processing of electronic trade documents and the need for any documentation to be presented in hard copy. For instance, the International Chamber of Commerce has called on all Governments to take two key actions without delay: as a temporary measure, void any legal requirements for trade documentation to be in hard copy and adopt the United Nations Commission on International Trade Law Model Law on Electronic Transferable Records (International Chamber of Commerce, 2020a; United

[35] See www.bolero.net and UNCTAD, 2003.

Nations Commission on International Trade Law, 2018; UNCTAD, 2017a).[36]