5

LEGAL ISSUES AND REGULATORY DEVELOPMENTS

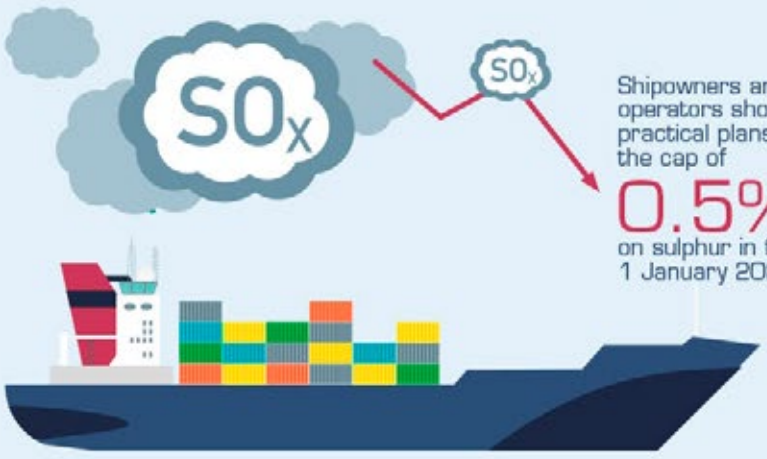
Along with economic benefits and connectivity and efficiency-related benefits from the use of new technologies, maritime shipping faces complex challenges, including cybersecurity threats and risks. Improved understanding and awareness raising is important, and relevant international regulations, including recent IMO guidelines on maritime cybersecurity risk management, as well as industry best practices, guidance and standards aimed at effectively addressing related vulnerabilities and threats, may be noted.

International regulatory developments over the period under review include the entry into force of the International Convention for the Control and Management of Ships' Ballast Water and Sediments, 2004 (known as the Ballast Water Management Convention, 2004), on 8 September 2017, and of the International Labour Organization Work in Fishing Convention, 2007 (No. 188), on 16 November 2017. Significantly for both human health and the environment, the IMO Marine Environment Protection Committee adopted a decision to implement a cap of 0.50 per cent on sulphur in fuel oil used on board ships from 1 January 2020.

CYBERSECURITY IN MARITIME SHIPPING

Raising awareness about and the careful consideration of cybersecurity threats, risks and potential consequences for ships, ports and cargo handling and operations is important, as is the development of and compliance with relevant national and international regulations, best practices, guidance and standards

SHIP-SOURCE POLLUTION



Shipowners and operators should make practical plans to meet the cap of

0.5%

on sulphur in fuel from 1 January 2020

In the light of Goal 14, all countries are encouraged to consider becoming parties to relevant international conventions for marine pollution prevention and control, as a matter of priority

A. TECHNOLOGICAL CHALLENGES AND OPPORTUNITIES IN THE GLOBAL SHIPPING INDUSTRY

1. Cybersecurity[1]

Risks and threats in the maritime sector

Facing commercial pressure and an ever-increasing demand to optimize logistics management systems and operations and improve connectivity, including digital connectivity, maritime shipping has become highly dependent on computerized systems and information and communications technology. Similar to other industry sectors that rely on such technology, computer systems on board vessels or in marine facilities face the same risk of cyberattacks, including through hacking, malware, phishing, Trojan horses, viruses, worms and denials of service, among others, and these can originate from hackers and criminals anywhere in the world. Cyberattacks are most likely to first target vulnerabilities along a supply chain, including negligent users, wireless access points and removable media devices. Unauthorized use of data or systems by authorized persons, such as ship or platform crew, can also have significant negative impacts. Cybersecurity-related incidents may also arise from extreme weather events, including climate-change related events, which pose significant risks to individuals and businesses, including on ships and in ports and marine facilities. In such circumstances, security measures need to be in place to ensure that even in the event of a partial or total destruction of facilities, data is secure and systems can resume operations as soon as possible.

The malicious exploitation and/or failure of information technology systems on board ships may disrupt their safe navigation and propulsion. Similarly, cyberattacks on other systems and technologies used for container terminal operations and cargo handling, including inventory and container tracking systems, can cause significant disruptions to such operations. Offshore platform stability and the positioning of offshore supply vessels can be equally vulnerable to cybersecurity-related impacts, either by modern pirates and smugglers or through non-targeted malware, insider threats and legitimate functions performed at the wrong time or under the wrong conditions (United States Coast Guard, 2016). All such attacks have safety and security repercussions, with potentially serious impacts on human life, the environment and the economy. Other cyberattacks may be aimed at stealing information, such as sensitive company data, which includes production and processing techniques or strategies for negotiating with trading partners. In addition to economic repercussions for companies directly involved, such attacks could have national security, wider financial and other implications. Potential consequences and costs of disruptions from malicious cyberattacks have been compared to those caused by past major incidents involving the maritime transport sector, such as the explosion of the Deepwater Horizon drilling platform in 2010 and the Exxon Valdez oil spill in 1989, although they may have not been caused by a cybersecurity failure (Rouzer, 2015).

In the last decade, concerns have been expressed regarding the low level of cybersecurity awareness and culture in the maritime sector, including in developed countries, such as knowledge of cybersecurity-related incidents that have taken place. Cybersecurity is often considered a theoretical issue, or a technical matter for information technology specialists, which does not directly involve others. In addition, risk assessments and management appear to focus primarily on physical security in ships and ports, with inadequate attention to cybersecurity and the sharing of information on mitigating cybersecurity threats.

For example, an analysis of initiatives and efforts within member States of the European Union with regard to cybersecurity in the maritime sector identified, among others, a generally insufficient focus on cybersecurity, which reduced the capabilities of the sector to consistently assess and deal with related challenges. Insufficient awareness among key stakeholders, including Governments, port authorities, shipping companies and telecommunications providers, of the security challenges, vulnerabilities and threats specific to this sector, was considered one of the main causes of this situation. Other problems identified were the complexity of the maritime information and communications technology environment and the fragmentation of governance at different levels, whether international, regional or national. The study highlighted, among others, the need to define appropriate measures to protect the maritime sector, as a critical infrastructure sector, against increasing cybersecurity threats, and suggested a road map for relevant stakeholders, containing short-term, midterm and long-term priorities for action (European Union Agency for Network and Information Security, 2011).

Threats to ships

With regard to cybersecurity threats affecting ships and their safe navigation, useful findings have been made with regard to automatic identification systems (AIS), global systems that use global positioning system coordinates and exchange up-to-date information about the positions, names, cargoes, speeds and headings of ships with other ships and maritime authorities via radio transmissions. AIS are frequently used by port authorities to warn ships about various hazards at sea. In open seas, they are also used to signal and locate people that may have fallen overboard. AIS are a useful tool for navigation, traffic monitoring, collision avoidance, search-and-rescue operations, accident investigation and piracy prevention, providing additional maritime traffic safety and supplementing

conventional radar installations. In 2000, IMO, through revisions to the International Convention for the Safety of Life at Sea, chapter V, adopted a new requirement for all ships to carry AIS from 31 December 2004. Ships shall therefore maintain AIS in operation at all times, except where international agreements, rules or standards provide for the protection of navigational information. Shipowners and operators can at times manipulate AIS data on their own vessels, most commonly to shut down the systems if "the continual operation of AIS might compromise the safety or security of his/her ship, or where security incidents are imminent" (IMO, 2015), for example when in transit through areas at high risk for piracy, to prevent pirates from locating ships and planning attacks.

A recent evaluation indicated that attackers could penetrate AIS easily, and outlined a range of possible weaknesses and threats, including spoofing, hijacking and availability disruption, each of which was analysed to determine whether the threat was based on software or radio frequency or both. It also reconfirmed the findings of earlier reports on the vulnerability of ship navigation systems (Trend Micro, 2014). Other threats include indiscriminate jamming, which could cause difficulties in determining the correct location of multiple ships (*The Maritime Executive*, 2017).

In 2013, researchers at the University of Texas demonstrated that they could gain navigational control and redirect a ship's course by generating a fake global positioning system signal that overrode the genuine signal. Neither AIS nor global positioning systems for civilian use are encrypted or authenticated and therefore present a potentially easy target. Moreover, the security gaps identified did not require expensive equipment or capabilities; the devices used by Trend Micro and the University of Texas to identify security gaps cost €700 and $2,000 respectively (Marsh, 2014).

In 2009, IMO amended International Convention for the Safety of Life at Sea, chapter V, regulation 19.2, and made it mandatory for ships engaged on international voyages to be fitted with electronic chart display and information systems, in stages depending on vessel type, from July 2012 until July 2018. Such systems are a computer-based alternative to paper-based navigation charts that integrate electronic navigation charts, global positioning system information and data from other navigational sensors, such as radar, fathometer and AIS. Electronic chart display and information systems provide valuable information for navigation, yet are vulnerable to cyberattacks, and their compromise could lead to loss of life, environmental pollution and financial losses (NCC Group, 2014).

A recent study analysed the security risks and weaknesses related to electronic chart display and information systems. Connectivity between such systems and office and communications platforms, combined with access to the Internet, could allow attackers to gain access by various means, such as the introduction of a virus through a portable memory card used by a crew member or the exploitation of an unpatched vulnerability through the Internet. Once such unauthorized access is gained, attackers may interact with shipboard networks and everything connected to them and could, among many possible intentional and unintentional consequences, subvert sensor data and misinterpret it for electronic chart display and information systems. Such actions could influence the decision-making process of navigation personnel and lead to collisions or ships running aground. Several other vulnerabilities in electronic chart display and information systems software could lead to severe disturbances in ship navigation, and related recommendations to remedy the situation include, for example, installing systems properly and isolating them from the rest of a ship's information technology systems with a firewall, to protect them from hacking and the potential diversion of the ship off course (NCC Group, 2014). Managing cybersecurity risks effectively may become more important as the industry is starting to use autonomous ships.

In 2014, the investigation of a collision between a cargo ship and an unstaffed crane barge revealed that a memory card connected to the system had been used to store media files. Although it had not directly contributed to the incident, such abuse of equipment has the potential to corrupt valuable data required to determine the circumstances of an accident. In August 2016, a naval contractor in France was hacked, resulting in the leak of more than 22,000 documents detailing the design of a submarine under construction, and, in October 2016, the computer of an employee of Hewlett Packard Enterprise Services was hacked, resulting in the opening of more than 134,000 personal records of sailors (Marine Link, 2017).

Offshore oil platforms are also at risk, with potential repercussions. For example, hackers may have caused a floating oil platform to tilt, forcing it to be temporarily shut down. It took one week to identify the cause and mitigate the effects. Globally, cyberattacks against oil and gas infrastructure may cost energy companies close to $1.9 billion by 2018, and the Government of the United Kingdom estimates that cyberattacks cost national oil and gas companies around $672 million per year (Reuters, 2014).

Threats to ports

As also highlighted in chapters 4 and 6, seaports are of strategic economic importance. Cyberattacks can have major repercussions for those that rely on computers and related systems, as such systems usually contain information pertaining to a number of different stakeholders. As a result, attackers could, for example, gain access to systems in order to seize a ship, close a port or its terminal or access sensitive information such as pricing documents or time

schedules, manifests, container numbers and others. Even a small cyberattack can cause business losses of millions of dollars (Belmont, 2014; Cyber Keel, 2014; Hazard Project, 2017). For example, in the United States, an attack launched in September 2001 against the Internet systems of the Port of Houston, one of the world's busiest maritime facilities, affected the performance of its entire network and caused data – including on tides, water depths and weather – used to help pilots and ships navigate through the harbour to become inaccessible and, although no injury or damage was caused, could have had major repercussions for those who relied on the computers (*The Register*, 2003). In addition, in 2013, the Port of Long Beach reported several cyberattacks by hackers using distributed denial of service or other methods. In response, the facility undertook a number of cybersecurity measures, including developing a computer network that integrated secure data from federal agencies and private terminal operators; banning commercial Internet traffic from its network; investing nearly $1 million in commercial applications to monitor network activity, intrusions and firewalls; mapping its networked systems and access points; designating controlled access areas for its servers; and backing up and replicating key data offsite (Ship-technology.com, 2013).[2]

Threats to cargo handling and terminal operating systems

Examples of such threats are as follows:

(a) Islamic Republic of Iran, 2011: The State-owned shipping line, which had the largest shipping fleet in the Middle East at the time, was targeted by a cyberattack that damaged data related to shipping rates, loading, cargo numbers, dates and locations, and caused confusion with regard to container location, whether containers had been loaded and which boxes were on board or on shore. In addition, as a result of the attack, the company's internal communications network was lost and, although the data was eventually recovered, operations were significantly disrupted, a considerable amount of cargo was lost and other cargo was sent to the wrong destinations, causing significant financial losses (Cyber Keel, 2014);

(b) Netherlands, 2011: For two years, drug traffickers concealed heroin and at least one ton of cocaine with a street value of £130 million inside legitimate cargo, and recruited hackers to infiltrate a computerized cargo tracking system at the Port of Antwerp, Belgium, to identify the shipping containers in which consignments of drugs had been hidden. The traffickers drove the containers from the port and retrieved the drugs before the legitimate owners arrived. The breach started with phishing attacks, including sending emails with malicious content to employees of transportation companies at the port. After the security breach was discovered and a firewall installed, the perpetrators broke into company offices and concealed sophisticated data interception hardware in cabling devices and computer hard drives, with the aim of stealing credentials in order to obtain the necessary certificates and release codes to retrieve the containers and unload them at the time and location of their choosing (Ship-technology.com, 2013);

(c) 2013: A security company published information about ongoing attacks since 2011, aimed at targets in business sectors in Japan and the Republic of Korea, including shipping and maritime operations. The attackers gained access to the networks of targeted companies, to extract documents, email account credentials and passwords allowing access to further resources in the networks. In contrast to other attacks, these lasted only a few days or weeks, with the attackers withdrawing once the targeted industry knowledge had been obtained (Cyber Keel, 2014);

(d) July 2014: A security company published information about a highly sophisticated malware targeting systems in the shipping and logistics industry worldwide. The malware was embedded at a supplier factory into the operating system of handheld scanners – used to check and inventory items being loaded on and off ships, trucks and airplanes – which were sent to shipping and logistics companies. The malware infiltrated servers and obtained financial and other data (Trap X Security, 2014);

(e) June 2017: A cyberattack affected the worldwide operations of Maersk, delaying shipments due to the closure of terminals in several ports, including the Port of Rotterdam, Netherlands; Jawaharlal Nehru Port, the largest container port in India; and terminals in the United States. Similar to the attacks that affected digital infrastructure worldwide in May 2017, this attack involved ransomware that hijacked control of a computer and demanded payment to an online address in return for regaining access to data and systems (JOC.com, 2017).

International regulatory aspects

To date, international regulations and policies, such as the IMO International Ship and Port Facilities Security Code and other measures, have mainly addressed the physical aspects of maritime security and safety, and the regulation of cybersecurity in maritime operations has mostly been voluntary. Recent developments include the adoption by IMO of guidelines on maritime cybersecurity risk management, which provide high-level recommendations regarding protection against current and emerging cybersecurity threats and vulnerabilities for all participants in international shipping (IMO, 2017a). The guidelines contain five functional elements for effective risk management in the maritime sector, as follows: "1. Identify: Define personnel roles and

responsibilities for cyberrisk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations; 2. Protect: Implement risk control processes and measures, and contingency planning to protect against a cyberevent and ensure continuity of shipping operations; 3. Detect: Develop and implement activities necessary to detect a cyberevent in a timely manner; 4. Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event; 5. Recover: Identify measures to back up and restore cybersystems necessary for shipping operations impacted by a cyberevent" (IMO, 2017b). The guidelines also list best practices, guidance and standards that provide further information for better understanding and addressing cybersecurity vulnerabilities and threats.[3]

As many cybersecurity-related incidents constitute crimes, international standards related to cybercrime are also worth noting. For example, the Convention on Cybercrime, 2001, includes jurisdiction clauses related to ships flying the flag of a party and the nationality of offenders (article 22), and the United Nations Convention against Transnational Organized Crime, 2004, defines transnational crime as, among others, an offence that is committed in one State but has substantial effects in another State, and may be applicable in the context of cybercrime acts that affect maritime operations.

2. Blockchain technology

Overview

Blockchain is a new, distributed ledger technology that has not yet been fully defined or understood. A blockchain is a distributed database (that is, with multiple copies existing on different computer systems) that records information shared by a peer-to-peer network using cryptography and other techniques to create secure and immutable records of transactions (see *Harvard Business Review*, 2017). Such transactions may involve many types of value such as currency (money, stocks or bonds), proof of ownership of tangible assets (goods, property or energy) and intangible assets (votes, identity, ideas or personal data). The use of blockchain technologies is expected to improve the speed and lower the cost of doing business, by simplifying operations and reducing the need for human intervention, automating processes and removing human errors (Knect365, 2016).

The first application of this technology was in finance, with the introduction of the digital currency bitcoin, providing a distributed system of trusted assets and transactions without the need for a central trust authority to act as a third-party guarantor. New blockchain technologies have since evolved, such as ethereum, which allows for the implementation of smart contracts that execute transactions based on the meeting of predefined conditions.

Blockchain technology is still in its early stages, and integrating it with other new technologies and platforms, and adopting relevant business processes, skills and regulations, is a challenge and requires time and investment (Cognizant, 2016). In addition, concerns remain with regard to the cybersecurity implications of blockchain implementation. A recent analysis of the technology identified security benefits, challenges and good practices, and found that some principles of the security of both traditional information technology systems and blockchain technology, such as encryption and key management, were largely the same and faced the same risks (European Union Agency for Network and Information Security, 2016). Blockchain use also faces new challenges related to, among others, consensus hijacking,[4] issues of interoperability between various platforms and smart contract management.

Blockchain technology in maritime shipping

In maritime shipping, the use of blockchain technology has been suggested, for example, for the transfer and sharing of data, including on the status of shipments. This is increasingly done electronically, through electronic data interchange messages, rather than exchanges of paper documents (see United Nations Economic Commission for Europe, 1996). Some major maritime carriers implement shipping portals, such as Cargo Smart, Inttra and GT Nexus, which provide essential digital processes and functionalities for booking, tracking and tracing and documentation, and which allow customers to communicate with carriers. However, in many steps in the shipping process, paper documents are still widely used. Port community systems that play an important role in handling port operations often use the same technology as shipping portals.

Blockchain technology could add important additional functionalities to transport and maritime information and communications technology and electronic data interchange systems, such as data verification and tracking and tracing. At the same time, it is important to develop and apply standards[5] that facilitate the secure exchange of data between such technologies and all relevant stakeholders (*Combined Transport Magazine*, 2016). Early-stage uses and pilot implementations of blockchain in supply chains and the transport and maritime industry include blockchain-enabled verified gross mass data exchanges, under the new International Convention for the Safety of Life at Sea requirements, which could lead to accelerated electronic data interchange standardization (see http://solasvgm.com and http://www.imo.org/en/OurWork/Safety/Cargoes/Containers/Pages/Verification-of-the-gross-mass.aspx); Blockfreight, an open network blockchain system for supply chains; a blockchain logistics consortium project at the Delft University of Technology, Netherlands; a pilot blockchain logistics project at the Port of Antwerp; and Maersk and Walmart pilot projects with International Business Machines

(see https://www.nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html; for the use of blockchains in customs declarations, see https://youtu.be/LeKapqAQimk).

With regard to transport documents, the main challenge in efforts to develop electronic alternatives to traditional paper documents has been the effective replication of each document's functions in a secure electronic environment, while ensuring that the use of electronic records or data messages benefits from the same legal recognition as that afforded to the use of paper documents. For bills of lading, with the exclusive right to the delivery of goods traditionally 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). Following earlier attempts to digitize bills of lading, including Bolero[6] and, more recently and with some success, essDOCS (see http://essdocs.com), some shipping companies have recently been reported to be exploring the use of blockchain technology in this context (JOC.com, 2016).

Blockchain technology has not yet been widely implemented in maritime shipping, however, and it is unclear whether this is likely to change soon. Challenges include ensuring interoperability and a range of legal issues (Takahashi, 2017), as well as the need to devise mechanisms for the effective incorporation of substantive maritime contract clauses and the replication of the processes involved in blockchain-enabled smart contract-based information technology systems. In addition, despite the new possibilities that blockchain may offer for identity generation and management, there are potential concerns regarding its use in applications that involve identity authentication or the protection of privacy or financial data. Developments regarding blockchain technology, as well as related legal issues, costs and infrastructure and other implications should therefore be monitored and further considered.

An international regulatory development relevant to the legal recognition of electronic transferable records is the recent finalization by the United Nations Commission on International Trade Law Working Group IV on Electronic Commerce of a model law on electronic transferable records, adopted in July 2017 (see http://uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf). The model law contains, among others, the definition of an electronic transferable record that must contain data and information identifying it as the functional equivalent of a transferable document or instrument such as, for example, bills of lading, receipts, certificates and other documents used in shipping. The model has four sections, as follows: general provisions (articles 1–7); provisions on functional equivalence (articles 8–11); use of electronic transferable records (articles 12–18); and cross-border recognition of electronic transferable records (article 19). It also sets out requirements to ensure the singularity and integrity of an electronic transferable record, as well as its ability to be controlled from its inception until it ceases to have any effect or validity, in particular in order to allow for its transfer. Since 2015, the United Nations Commission on International Trade Law has been addressing legal issues related to identity management and trust services and to contractual aspects of cloud computing (see http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html).

B. REGULATORY DEVELOPMENTS RELATING TO THE REDUCTION OF GREENHOUSE GAS EMISSIONS FROM INTERNATIONAL SHIPPING, AND OTHER ENVIRONMENTAL ISSUES

1. Reduction of greenhouse gas emissions from international shipping and energy efficiency

Greenhouse gas emissions from international shipping

Maritime transport emits around 1 billion tons of carbon dioxide annually and is responsible for about 2.5 per cent of global greenhouse gas emissions from fuel combustion. By 2050, depending on future economic growth and energy developments, shipping emissions may increase by between 50 and 250 per cent (IMO, 2014a). This is not in keeping with the internationally agreed goal of limiting the global average temperature increase to below 2°C above pre-industrial levels, which would require worldwide emissions to be at least halved from the 1990 level by 2050. The implementation of technical and operational measures for ships could increase efficiency and reduce the emissions rate by up to 75 per cent, and further reductions could be achieved by implementing innovative technologies (IMO, 2009).

The Marine Environment Protection Committee, at its session in July 2017, continued to build on previous work to address greenhouse gas emissions from international shipping, in particular through the adoption of an IMO strategy on the reduction of greenhouse gas emissions from ships in 2018, in accordance with a road map approved at its session in October 2016 (IMO, 2016a, annex 11). The Committee considered various proposals with regard to the strategy from States and industry representatives, and noted the draft outline for its possible structure, which included the following elements: preamble, introduction and context, including emission scenarios; vision; levels of ambition and guiding principles; list of candidate short-term, midterm and long-term measures with possible timelines and their impacts on States; barriers and supportive measures, capacity-building and

technical cooperation and research and development; follow-up actions towards the development of the revised strategy; and a periodic review of the strategy (IMO, 2017c). Delegations expressed concern with regard to the need for proper references in the road map to consideration of the special needs of small island developing States and the least developed countries, in accordance with the Small Island Developing States Accelerated Modalities of Action Pathway, to ensure both progress and inclusiveness, and the need for a high level of ambition with regard to the strategy was highlighted.[7]

Energy efficiency for ships

Energy efficiency measures, legally binding for the entire maritime industry since 2013, include the Energy Efficiency Design Index that sets standards for new ships, and associated operational energy efficiency measures for existing ships. However, no agreement has been reached to date on global market-based measures or other instruments that would reduce emissions from the entire shipping sector.

The Marine Environment Protection Committee, at its session in July 2017, was advised that nearly 2,500 new ships had been certified as complying with energy efficiency standards. Among others, the Committee adopted guidelines for administration verification of ship fuel oil consumption data for ships of 5,000 gross tonnage and above, starting from 2019, and guidelines for the development and management of the IMO ship fuel oil consumption database (IMO, 2017c, annexes 16 and 17). These guidelines make it mandatory for ships of 5,000 gross tonnage and above to collect consumption data for each type of fuel oil they use, as well as additional specified data, including proxies for transport work. The aggregated data will be reported to the flag State after the end of each calendar year, and subsequently transferred to the IMO database.

2. Ship-source pollution and protection of the environment

Air pollution from ships

With regard to NO_x, the Marine Environment Protection Committee adopted amendments designating the North Sea and the Baltic Sea (which are emission control areas for sulphur oxide (SO_x)) as NO_x emission control areas under the International Convention for the Prevention of Pollution from Ships, annex VI, regulation 13. Marine diesel engines operating in these areas will be required to comply with the stricter tier III NO_x emissions limit when installed on ships constructed on or after 1 January 2021. Guidelines on selective catalytic reduction systems were also adopted (IMO, 2017c, annex 13).

With regard to SO_x, the Committee adopted an important decision with regard to human health and the environment, namely to implement a global limit of 0.5 per cent on sulphur in fuel oil used on board ships, as set out in the International Convention for the Prevention of Pollution from Ships, annex VI, regulation 14.1.3, from 1 January 2020 (IMO, 2016a, annex 6). This represents a significant reduction from the 3.5 per cent limit currently in place outside emission control areas.[8] To meet requirements, shipowners and operators continue to adopt various strategies, including installing scrubbers and switching to liquefied natural gas and other low-sulphur fuels. The Committee approved guidelines providing an agreed method for sampling to enable the effective control and enforcement of sulphur content of liquid fuel oil used on board ships under the provisions of the International Convention for the Prevention of Pollution from Ships, annex VI (IMO, 2016b), and amendments to the information to be included in the bunker delivery note related to the supply of fuel oil to ships that have fitted alternative mechanisms to address SO_x emission requirements (IMO, 2017c).

Ballast water management

An important development is the entry into force of the Ballast Water Management Convention, 2004, on 8 September 2017.[9] The Convention aims to prevent the risk of the introduction and proliferation of non-native species following the discharge of untreated ballast water from ships. This is considered one of the four greatest threats to the world's oceans and one of the major threats to biodiversity, which, if not addressed, can have extremely severe public health-related and environmental and economic impacts (see http://globallast.imo.org). From the entry into force date, ships are required to manage their ballast water to meet standards referred to as D-1 and D-2; the former requires ships to exchange and release at least 95 per cent of ballast water by volume far away from a coast and the latter raises the restriction to a specified maximum amount of viable organisms allowed to be discharged, limiting the discharge of specified microbes harmful to human health. Draft amendments to the Convention as approved by the Marine Environment Protection Committee, to be circulated after its entry into force and adopted in April 2018, clarify when ships must comply with the D-2 standard. New ships, constructed on or after 8 September 2017, shall meet the D-2 standard from the date they are entered into service. Existing ships constructed before 8 September 2017 shall comply with the D-2 standard after their first or second five-year renewal survey associated with the International Oil Pollution Prevention Certificate under the International Convention for the Prevention of Pollution from Ships, annex I, conducted after 8 September 2017, and in any event not later than 8 September 2024 (IMO, 2017c).

Hazardous and noxious substances

In April 2017, the Legal Committee of IMO approved a draft resolution calling on States to consider ratifying the

International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea, 1996, as amended by its 2010 Protocol, and to implement it in a timely manner (IMO, 2017d, annex 2). This key instrument has not yet entered into force as, to date, it has been ratified by only one State (Norway). This leaves an important gap in the global liability and compensation framework, while a comprehensive and robust international liability and compensation regime is in place with respect to oil pollution from tankers (International Oil Pollution Compensation Fund regime),[10] as well as with respect to bunker oil pollution from ships other than tankers (International Convention on Civil Liability for Bunker Oil Pollution Damage, 2001).

Pollution from offshore oil exploration and exploitation

The Legal Committee of IMO finalized guidance to be taken into consideration by States when negotiating bilateral and/or regional arrangements or agreements on liability and compensation issues connected with transboundary oil pollution damage resulting from offshore exploration and exploitation activities (IMO, 2017e). The need for a global legal instrument has been considered at IMO since 2011, but no agreement has been reached. While the reluctance of IMO to deal with this issue appears to be related to its mandate, which focuses on ship-source pollution (IMO, 2014b), the continued absence of an international liability regime leaves an important gap in the international legal framework and is a matter of concern, in particular for potentially affected developing countries.

C. OTHER LEGAL AND REGULATORY DEVELOPMENTS AFFECTING TRANSPORTATION

1. Combating maritime piracy and armed robbery

The Maritime Safety Committee, in June 2017, reported a total of 221 piracy and armed robbery incidents worldwide in 2016, a decrease of about 27 per cent compared with 303 incidents in 2015. However, an increase of 77 per cent was observed in West Africa. Piracy off the coast of Somalia remained active, with eight incidents reported between January and April 2017, and around 39 crew members taken hostage. To address the possible underreporting of piracy and armed robbery incidents within the Gulf of Guinea region, the Maritime Safety Committee urged all concerned to report incidents in a timely manner to reporting organizations, to allow for better response and risk management (IMO, 2017a).

2. Legally binding instrument under the United Nations Convention on the Law of the Sea, 1982

Under this Convention, the seabed beyond the limits of national jurisdiction is subject to the principle of the common heritage of humanity, and resources found there are to be used for the benefit of humanity as a whole, and taking into particular consideration the interests and needs of developing countries (article 140). Marine genetic resources are commercially valuable and hold considerable potential for the development of advanced pharmaceuticals; their exploitation may in the near future become a promising activity in areas beyond the limits of national jurisdiction. In the absence of a specific international legal framework regulating related issues, negotiations have been ongoing since 2016 at the United Nations on key elements for an international legally binding instrument under this Convention, on the conservation and sustainable use of marine biological diversity of areas beyond national jurisdiction. The outcome of the fourth meeting of the preparatory committee established in accordance with General Assembly resolution 69/292 of 19 June 2015 (see http://www.un.org/Depts/los/biodiversity/prepcom.htm), held in July 2017, included a number of elements recommended for consideration by the General Assembly in the elaboration of a text. The suggested elements reflected convergence among most delegations during the discussions, and were not exclusive. The outcome also included a list of main issues related to these elements, on which there was divergence of views, as well as a recommendation to the General Assembly to take a decision, as soon as possible, on the convening of an intergovernmental conference. Suggested elements included, among others, the following: general principles and approaches; international cooperation; marine genetic resources, including questions on the sharing of benefits; measures such as area-based management tools, including marine protected areas; environmental impact assessments; and capacity-building and the transfer of marine technology. In this context, it is important for the special requirements of developing countries, in particular the least developed countries, landlocked developing countries, geographically disadvantaged States, small island developing States and coastal African States, to be taken into account when drafting the instrument.

3. Seafarers' issues: International Labour Organization Work in Fishing Convention, 2007 (No. 188)

This Convention, which enters into force on 16 November 2017, aims to provide updated and comprehensive international labour standards for fishing workers.[11] Over 38 million people work in capture fisheries globally, in an industry that is one of the most dangerous professions

(International Labour Organization, 2016). Sustainable Development Goal 14, to conserve and sustainably use the oceans, seas and marine resources for sustainable development, includes several targets dedicated to fisheries, in particular targets 14.4, 14.7 and 14.b. Although the targets do not include direct references to the labour dimension of sustainable fishing, the rights of fishing workers are relevant in this context. Earlier studies have, for example, linked overfishing and illegal fishing to the increasing hazardousness and deterioration of working conditions for fishing workers (Environmental Justice Foundation, 2015; International Labour Organization, 2013a; Pocock et al, 2016). Due to conservation measures aimed at protecting fishing stocks from unsustainable fishing practices, fishing vessels may be forced to travel further out to sea, to hazardous and isolated environments, increasing the possibility for the abuse of fishing workers (International Labour Organization, 2013b). Other problems relate to the practice of flagging fishing vessels to countries that have inadequate labour protection regulations or using open registers that allow for the preservation of anonymity of ownership, which may complicate the issue of vessel labour inspection responsibilities (Food and Agriculture Organization of the United Nations, 2002).

The Work in Fishing Convention, 2007 (No. 188), establishes minimum labour standards for fishing workers on all types of commercial fishing vessels globally. Its objective is to "ensure that fishers have decent conditions of work on board fishing vessels with regard to minimum requirements for work on board; conditions of service; accommodation and food; occupational safety and health protection; medical care and social security" (International Labour Organization, 2007a). The Convention lists commitments undertaken by States Parties in these areas and requires them to implement and enforce national laws, regulations or other measures they have adopted to fulfil the commitments (article 6). The Convention addresses the work agreements of fishing workers, which shall be in writing (articles 16–20); recruitment and placement (article 22); and regular payment and means to transmit payments to their families at no cost (articles 23 and 24). Provisions related to social security protection aim to protect migrant workers' rights, requiring States to "achieve progressively comprehensive social security protection for fishers, taking into account the principle of equality of treatment irrespective of nationality" (article 36 (a)). The Convention also establishes mechanisms for inspection, compliance and enforcement. In its capacity as a flag State, a State Party "which receives a complaint or obtains evidence that a fishing vessel that flies its flag does not conform to the requirements of this Convention shall take the steps necessary to investigate the matter and ensure that action is taken to remedy any deficiencies found" (article 43.1) and, in its capacity as a port State, if a State Party in whose port a fishing vessel calls "receives a complaint or obtains evidence that such vessel does not conform to the requirements of this Convention, it may prepare a report addressed to the Government of the flag State of the vessel [and] may take measures necessary to rectify any conditions on board which are clearly hazardous to safety or health" (article 43.2). In addition, the Convention shall be applied "in such a way as to ensure that the fishing vessels flying the flag of any State that has not ratified this Convention do not receive more favourable treatment than fishing vessels that fly the flag of any member that has ratified it" (article 44). This article, along with port State control, may provide an incentive for a wider implementation of the Convention, to vessels flagged to States that are not Parties to the Convention.

Two sets of International Labour Organization guidelines provide practical guidance for the implementation of flag State and port State inspections (International Labour Organization, 2011 and 2017). In addition, the Work in Fishing Recommendation, 2007 (No. 199), provides guidance on the implementation of the Convention (International Labour Organization, 2007b).

D. POLICY CONSIDERATIONS

The use of new technologies in the maritime industry is associated with increased cybersecurity threats and risks. To ensure that ships navigate safely, important information on board and on shore remains secure and that seafarers and other staff are aware of the dangers and risks involved, Governments, public and private companies and other stakeholders should work together to better understand, assess, manage and implement new technologies. In implementing new technologies, cybersecurity should be carefully considered, along with other important issues, to facilitate risk reduction and mitigation efforts and to increase cybersecurity resilience. Collaborative approaches are important in this context, to raise awareness about possible cybersecurity threats, risks and consequences, and to effectively address these through information exchanges, coordination and dialogue, as well as by upgrading outdated systems, increasing the physical security of information technology facilities and data networks and providing cybersecurity training for employees. Where appropriate, cybersecurity elements should be mainstreamed into regulatory frameworks governing the maritime sector and regulatory compliance should be encouraged and supported. The enforcement of existing cybersecurity regulations is important, as is the development of additional standards and policies. In addition, best practices, guidance and standards adopted to date should be considered, along with the five functional elements in the IMO guidelines on maritime cybersecurity risk management, namely identify, protect, detect, respond and recover.

In the light of the entry into force and widespread adoption of the Paris Agreement under the United Nations Framework Convention on Climate Change,

ongoing efforts to reduce greenhouse gas emissions from international shipping should be pursued as a matter of urgency, including through the implementation of technical and operational measures, as well as innovative technologies for ships. Discussions on a global greenhouse gas reduction strategy should properly reflect and take into account the special needs of small island developing States and the least developed countries, to ensure progress and inclusiveness. With respect to ship-source air pollution, it is important for shipowners and operators to continue to consider and adopt various strategies, including installing scrubbers and switching to liquefied natural gas and other low-sulphur fuels. In addition, practical plans should be in place to implement the cap of 0.5 per cent on sulphur content in fuel oil used on board ships from 1 January 2020.

Given the importance of implementing and effectively enforcing strong international environmental regulations and in the light of the policy objectives inherent in Sustainable Development Goal 14, developed and developing countries are encouraged to consider becoming parties to relevant international conventions for marine pollution prevention and control, as a matter of priority. In this context, the entry into force of the Ballast Water Management Convention, 2004, in September 2017 may be noted. Widespread adoption and implementation of international conventions addressing liability and compensation for ship-source pollution, such as the International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea, 2010, is also desirable, in view of the important gaps that remain in the international legal framework.

Progress is being made in ongoing negotiations at the United Nations on an international legally binding instrument under the United Nations Convention on the Law of the Sea, 1982 on the conservation and sustainable use of the marine biological diversity of areas beyond national jurisdiction. In this context, and in particular with regard to questions on the sharing of benefits from marine genetic resources, capacity-building and the transfer of marine technology, it is important for the special requirements of developing countries, in particular the least developed countries, landlocked developing countries, geographically disadvantaged States, small island developing States and coastal African States, to be taken into account when drafting the instrument.

The entry into force of the Work in Fishing Convention, 2007 (No. 188), will assist the achievement of the Sustainable Development Goals, in particular those related to ocean governance and the sustainable use of the oceans and seas and of marine resources, including fisheries, by adding a labour and social sustainability dimension. All countries, in particular developing countries for which employment in capture fishing is important, may wish to consider becoming parties to this Convention.

REFERENCES

Belmont KB (2014). Blank Rome maritime: Maritime cybersecurity – a growing threat goes unanswered. Available at http://mlaus.org/wp-content/uploads/bp-attachments/3821/K-Belmont-Maritime-Cybersecurity-Articles-0031.pdf (accessed 25 September 2017).

Cognizant (2016). Blockchain's smart contracts: Driving the next wave of innovation across manufacturing value chains. Available at https://www.cognizant.com/whitepapers/blockchains-smart-contracts-driving-the-next-wave-of-innovation-across-manufacturing-value-chains-codex2113.pdf (accessed 25 September 2017).

Combined Transport Magazine (2016). Secure data exchange across supply chains – blockchain and electronic data interchange. 9 November. Available at http://combined-transport.eu/blockchain-edi-for-supply-chains (accessed 3 October 2017).

Cyber Keel (2014). Maritime cyberrisks. Available at https://www2.sfmx.org/bay-area-committees/amsc/cyber-security/ (accessed 25 September 2017).

Environmental Justice Foundation (2015). *Pirates and Slaves: How Overfishing in Thailand Fuels Human Trafficking and the Plundering of our Oceans*. London. Available at https://ejfoundation.org/reports/pirates-and-slaves-how-overfishing-in-thailand-fuels-human-trafficking-and-the-plundering-of-our-oceans (accessed 3 October 2017).

European Union Agency for Network and Information Security (2011). Analysis of cybersecurity aspects in the maritime sector. Available at https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1 (accessed 25 September 2017).

European Union Agency for Network and Information Security (2016). Distributed ledger technology and cybersecurity: Improving information security in the financial sector. Available at https://www.enisa.europa.eu/publications/blockchain-security (accessed 25 September 2017).

Food and Agriculture Organization of the United Nations (2002). Fishing vessels operating under open registers and the exercise of flag State responsibilities. Fisheries Circular No. 980. Available at http://www.fao.org/docrep/005/y3824e/y3824e00.htm (accessed 3 October 2017).

Harvard Business Review (2017). How blockchain is changing finance. 1 March. Available at https://hbr.org/2017/03/how-blockchain-is-changing-finance (accessed 3 October 2017).

Hazard Project (2017). *Cybersecurity in Ports*. Turku, Finland. Available at https://blogit.utu.fi/hazard/materials-for-download/ (accessed 25 September 2017).

International Labour Organization (2007a). Work in Fishing Convention, 2007 (No.188). Available at http://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C188 (accessed 3 October 2017).

International Labour Organization (2007b). Work in Fishing Recommendation, 2007 (No. 199). http://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO:12100:P12100_INSTRUMENT_ID:312536:NO (accessed 25 September 2017).

International Labour Organization (2011). *The Work in Fishing Convention, 2007 (No. 188): Guidelines for Port State Control Officers*. Geneva. Available at http://www.ilo.org/sector/Resources/codes-of-practice-and-guidelines/WCMS_177245/lang--en/index.htm (accessed 3 October 2017).

International Labour Organization (2013a). *Employment Practices and Working Conditions in Thailand's Fishing Sector*. Bangkok. Available at http://www.ilo.org/asia/publications/WCMS_220596/lang--en/index.htm (accessed 3 October 2017).

International Labour Organization (2013b). *Caught at Sea: Forced Labour and Trafficking in Fisheries*. Geneva. Available at http://www.ilo.org/global/topics/forced-labour/publications/WCMS_214472/lang--en/index.htm (accessed 3 October 2017).

International Labour Organization (2016). ILO Work in Fishing Convention, 2007 (No.188), to enter into force. 16 November. Available at http://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_535063/lang--en/index.htm (accessed 3 October 2017).

International Labour Organization (2017). *Guidelines on Flag State Inspection of Working and Living Conditions On Board Fishing Vessels*. Geneva Available at http://www.ilo.org/sector/Resources/codes-of-practice-and-guidelines/WCMS_428592/lang--en/index.htm (accessed 3 October 2017).

IMO (2009). *Second IMO Greenhouse Gas Study 2009*. London.

IMO (2014a). *Third IMO Greenhouse Gas Study 2014*. London.

IMO (2014b). Implications of the United Nations Convention on the Law of the Sea for the International Maritime Organization. Study by the secretariat. LEG/MISC.8. London.

IMO (2015). Revised guidelines for the on board operational use of shipborne automatic identification systems. A.1106(29). London.

IMO (2016a). Report of the Marine Environment Protection Committee on its seventieth session. MEPC 70/18. London.

IMO (2016b). Guidelines for on board sampling for the verification of the sulphur content of the fuel oil used on board ships. MEPC.1/Circ.864. London.

IMO (2017a). Report of the Maritime Safety Committee on its ninety-eighth session. MSC 98/23. London.

IMO (2017b). Guidelines on maritime cyberrisk management. MSC-FAL.1/Circ.3. London.

IMO (2017c). Report of the Marine Environment Protection Committee on its seventy-first session. MEPC 71/17. London.

IMO (2017d). Report of the Legal Committee on the work of its 104th session. LEG 104/15. London.

IMO (2017e). Liability and compensation issues connected with transboundary pollution damage from offshore exploration and exploitation activities. LEG 104/14/2. London.

JOC.com (2016). Blockchain tech could save shippers money, stress. 4 October. Available at http://www.joc.com/international-logistics/logistics-technology/tech-behind-bitcoin-could-enable-digital-bills-lading_20161004.html (accessed 3 October 2017).

JOC.com (2017). Shippers search for answers following Maersk cyberattack. 27 June. Available at http://www.joc.com/maritime-news/container-lines/maersk-line/shippers-search-answers-following-maersk-cyberattack_20170627.html (accessed 3 October 2017).

Knect365 (2016). Could blockchain be the shipping industry's life jacket? 22 December. Available at https://knect365.com/techandcomms/article/6a6fa749-c53f-448d-9036-4f130b062451/could-blockchain-be-the-shipping-industrys-life-jacket (accessed 3 October 2017).

Marine Link (2017). Cybervigilance at sea: The new norm. *Maritime Reporter and Engineering News*. 22 May. Available at https://www.marinelink.com/news/vigilance-cyber-norm425579 (accessed 3 October 2017).

Marsh (2014). The risk of cyberattack to the maritime sector. Available at http://me.marsh.com/NewsInsights/ID/41615/The-Risk-of-Cyber-Attack-to-the-Maritime-Sector.aspx (accessed 25 September 2017).

NCC Group (2014). Preparing for cyberbattleships: Electronic chart display and information system security. Available at https://www.nccgroup.trust/uk/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/ (accessed 25 September 2017).

Pocock NS, Kiss L, Oram S and Zimmerman C (2016). Labour trafficking among men and boys in the Greater Mekong Subregion: Exploitation, violence, occupational health risks and injuries. *Plos One*, 11(12). Available at http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0168500 (accessed 3 October 2017).

Reuters (2014). All at sea: Global shipping fleet exposed to hacking threat. 23 April. Available at http://www.reuters.com/article/tech-cybersecurity-shipping-idUSL3N0N402020140423 (accessed 3 October 2017).

Rouzer B (2015). Cybersecurity and the marine transportation system. Presented at the American Association of Port Authorities cybersecurity seminar. Savannah, United States. 11 March. Available at http://www.aapa-ports.org/unifying/PastDetail.aspx?itemnumber=20333 (accessed 25 September 2017).

Ship-technology.com (2013). Web of intrigue: Protecting ports against cyberterrorism. Available at http://www.ship-technology.com/features/feature-cybersecurity-port-computer-hackers-us-belgium/ (accessed 25 September 2017).

Takahashi K (2017). Implications of the blockchain technology for the United Nations Commission on International Trade Law works. Presented at the Modernizing International Trade Law to Support Innovation and Sustainable Development congress. Vienna. 4–6 July. Available at http://www.uncitral.org/uncitral/en/commission/colloquia/50th-anniversary-papers.html (accessed 25 September 2017).

The Maritime Executive (2017). Mass global positioning system spoofing attack in Black Sea? 11 July. Available at http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea (accessed 3 October 2017).

The Register (2003). United Kingdom teenager accused of electronic sabotage against United States port. 6 October. Available at https://www.theregister.co.uk/2003/10/06/uk_teenager_accused_of_electronic/ (accessed 3 October 2017).

Trap X Security (2014). Trap X discovers zombie zero advanced persistent malware. 10 July. Available at https://trapx.com/trapx-discovers-zombie-zero-advanced-persistent-malware/ (accessed 3 October 2017).

Trend Micro (2014). A security evaluation of automatic identification systems. Available at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais (accessed 25 September 2017).

UNCTAD (2003). The use of transport documents in international trade. Available at http://unctad.org/en/Pages/DTL/TTL/Legal/Carriage-of-Goods.aspx (accessed 25 September 2017).

UNCTAD (2011). The 2004 Ballast Water Management Convention – with international acceptance growing, the Convention may soon enter into force. In: Transport newsletter No. 50. Available at http://unctad.org/en/Pages/DTL/TTL/Transport-Newsletter.aspx (accessed 3 October 2017).

UNCTAD (2012). *Liability and Compensation for Ship-source Oil Pollution: An Overview of the International Legal Framework for Oil Pollution Damage from Tankers*. United Nations publication. New York and Geneva. Available at http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=322 (accessed 3 October 2017).

UNCTAD (2013). *Review of Maritime Transport 2013*. United Nations publication. Sales No. E.13.II.D.9. New York and Geneva. http://unctad.org/en/Pages/Publications/Review-of-Maritime-Transport-(Series).aspx (accessed 3 October 2017).

UNCTAD (2015). The International Ballast Water Management Convention 2004 is set to enter into force in 2016. Transport and Trade Facilitation Newsletter No. 68. Available at http://unctad.org/en/PublicationsLibrary/webdtltlb2015d4_en.pdf (accessed 3 October 2017).

United Nations Economic Commission for Europe (1996). Recommendation 25: Use of the United Nations Electronic Data Interchange for administration, commerce and transport. TRADE/WP.4/R.1079/Rev.1. Geneva. Available at https://www.unece.org/fileadmin/DAM/cefact/recommendations/rec_index.htm (accessed 3 October 2017).

United States Coast Guard (2016). Cyberrisks in the marine transportation system. Available at https://www.uscg.mil/hq/cg5/cg544/docs/USCG_Paper_MTS_CyberRisks.pdf (accessed 25 September 2017).

United States Government Accountability Office (2015). Maritime critical infrastructure protection. Available at http://www.gao.gov/products/GAO-16-116T (accessed 3 October 2017).

ENDNOTES

1. For a definition of the concept, see http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.
2. For further information on enhancing cybersecurity at United States ports and related recommendations, see United States Government Accountability Office, 2015.
3. Including the following: joint industry guidelines on cybersecurity on board ships, second edition, adopted, July 2017 (see https://www.bimco.org/news/press-releases/20170705_cyber-g); ISO and International Electrotechnical Commission standard No. 27001 on information technology: security techniques – information security management systems and requirements; and the United States National Institute of Standards and Technology framework for improving critical infrastructure security. For general information on cybercrime and on addressing cybercrime, see https://www.unodc.org/unodc/en/organized-crime/expert-group-to-conduct-study-cybercrime-feb-2013.html.
4. That is, allowing the creation of changes by hijacking the majority of nodes on a network, which can be an issue on private or permissioned networks with relatively smaller nodes.
5. For example, standardized information technology data dictionaries such as the United Nations Economic Commission for Europe core components library.
6. Bill of lading electronic registry organization; see UNCTAD, 2003, and http://www.bolero.net.
7. Cook Islands, supported by Palau, Papua New Guinea, Solomon Islands, Tuvalu and Vanuatu, as well as interventions by Bahamas and Norway.
8. Within emission control areas in which more stringent controls on SO_x emissions apply, the sulphur content of fuel oil must be no more than 0.1 per cent (1,000 parts per million), from 1 January 2015. The first two SO_x emission control areas were established in Europe, in the Baltic Sea and the North Sea, and took effect in 2006 and 2007, respectively; the third was established in North America and took effect in 2012; and the fourth was established as the United States Caribbean Sea, covering waters adjacent to the coasts of Puerto Rico and the United States Virgin Islands, and took effect in 2014.
9. As at 13 September 2017, there were 65 States Parties to the Convention, representing 73.92 per cent of the gross tonnage of the world's merchant fleet. For more information on related developments see UNCTAD, 2011, and UNCTAD, 2015.
10. International Convention on Civil Liability for Oil Pollution Damage, 1969, and its 1992 Protocol and International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage, 1971, and its 1992 and 2003 Protocols. For an analytical overview of the international legal framework, see UNCTAD, 2012. See also UNCTAD, 2013, pp. 110–111.
11. The Convention revises the following: Minimum Age (Fishermen) Convention, 1959 (No. 112); Medical Examination (Fishermen) Convention, 1959 (No. 113); Fishermen's Articles of Agreement Convention, 1959 (No. 114); and Accommodation of Crews (Fishermen) Convention, 1966 (No. 126).