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).