NUS Centre for Maritime Law Working Paper 24/02

NUS Law Working Paper 2024/005

AN EVALUATION OF THE SAFE PORT OBLIGATION IN THE LIGHT OF SMART AND AUTONOMOUS SHIPS

Ntandokazi Shazi

Research Associate, Centre for Maritime Law

[Uploaded May 2024]

An Evaluation of the Safe Port Obligation in the Light of Smart and Autonomous Ships

Ntandokazi Shazi[*]

ABSTRACT

The market for smart and autonomous ships – vessels propelled by highly innovative technologies such as blockchain, the internet of things, robotics, simulation and modelling, big data and business analytics – is estimated to reach US$165.61 billion by 2030. The potential benefits that smart and autonomous ships offer to international trade have captured the attention of major industry players and governments in various parts of the world. However, the widespread adoption of such vessels will necessitate the development of smart ports equipped with complementary advanced technologies, infrastructure, and processes to accommodate them safely. This need is especially critical in the context of the charterer's contractual obligation only to send the vessel under charter to safe ports. This strict obligation will likely compel charterers to avoid sending any smart and/or autonomous ships under charter to ports that cannot safely accommodate them.

This paper will examine the law concerning the 'safe port obligation' of the charterer in the context of smart and autonomous ships. It will highlight that courts will likely allocate liability for any damages to smart and autonomous ships visiting ill-equipped ports to the charterer. Considering the current trends in investment to digitise ports, this paper will also argue that developing regions may struggle to digitise ports, leading charterers to avoid utilising these ports. Finally, this paper will question whether the current cyber security framework is adequate to enable charterers to determine the safety of a particular port in the context of smart and autonomous ships.

Keywords: smart ships, autonomous ships, MASS, safe port obligation, digital ports, smart ports, cyber threats, cyber security.

[*] Research Associate, Centre for Maritime Law, NUS. The author would like to thank Professor Stephen Girvin for his valuable mentorship, revisions and suggestions. The usual disclaimer applies.

1 Introduction

Industry 4.0 describes the current era of connectivity, advanced analytics, automation, and advanced manufacturing technology, which has disrupted global business since the mid-2010s.[1] The shipping industry is experiencing multiple impacts from these technologies, such as the introduction of electronic bills of lading.[2] Notably, Industry 4.0 has also led to the emergence of autonomous ships, known as MASS.[3] Autonomous ships have the potential to restructure the concept of shipping operations completely.[4] However, within the maritime industry, debate continues concerning the feasibility and value of unmanned vessels plying our oceans.[5] Nevertheless, major industry players such as Rolls Royce and Kongsberg Gruppen[6] continue investing significant R&D and resources into autonomous ships, with the market size estimated to reach US$165.61 billion by 2030.[7] With the development of autonomous ships forging ahead, there is a need to consider the entire maritime ecosystem, particularly ports, which serve as the meeting point between land and sea.

Ports and terminals, considered simply loading and unloading facilities in the 1960s,[8] are now rightly recognised as indispensable to the global supply chain. The unique importance of ports and terminals lies in their intrinsic interconnectedness and international nature. With globalisation and the

[1] 'What are the Industry 4.0, the Fourth Industrial Revolution, and 4IR' (McKinsey & Co) <www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir> accessed 19 April 2023.

[2] As to which, see eg, Stephen Girvin and Elson Ong, 'Blockchain and bills of lading' in Stephen Girvin & Vibe Ulfbeck (eds), *Maritime Management, Organization and Liability: A Legal Analysis of New Challenges in the Maritime Industry* (Hart Publishing 2021) ch 10; Ilias Ioannou, 'Is Enabling Legislation Sufficient to Promote the Uptake of Electronic Paperless Trading Systems?' NUS Centre for Maritime Law Working Paper 23/04 (June 2023), downloadable from < https://law.nus.edu.sg/cml/publications/> accessed 7 April 2024.

[3] Maritime Autonomous Surface Ships (MASS) is a term used by the International Maritime Organization (IMO) in its Regulatory Scoping Exercise MSC.1/Circ.1638, International Maritime Organisation, Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS) (Cm 1638, 3 June 2021) [3].

[4] Smart Port, *Smart Ships and the Changing Maritime Ecosystem* (2019) 4.

[5] David Dubay, 'Why We Will Never See Fully Autonomous Commercial Ships' (The Maritime Executive) <https://maritime-executive.com/editorials/why-we-will-never-see-fully-autonomous-commercial-ships> accessed 21 April 2023.

[6] Cichen Shen, 'Samsung Heavy Teams with Kongsberg Maritime to Develop Autonomous LNG Carriers' *Lloyd's list* (London, 20 March 2023).

[7] J Akshay and M Sonia, 'Autonomous Ships Market by Level of Autonomy (Semi-autonomous and Fully-autonomous), Ship Type (Commercial, Passenger, and Defense), Component (Hardware and Software) and Fuel Type (Carbon Neutral Fuels, LNG, Electric, and Heavy Fuel Oil/Marine Engine Fuel): Global Opportunity Analysis and Industry Forecast, 2020-2023' (Allied Market Research 2020) <www.alliedmarketresearch.com/autonomous-ships-market> accessed 21 April 2023.

[8] Ignacio de la Pena Zarzuelo, 'Industry 4.0 in the Port and Maritime Industry: A Literature Review' (2020) 20 Journal of Industrial Information Integration <Industry 4.0 in the port and maritime industry: A literature review - ScienceDirect> accessed 18 May 2023.

corresponding increase in international trade, ports are increasingly vital to the economies of the countries in which they are located.[9] According to the UNCTAD *Review of Maritime Transport 2019*, maritime transport is the backbone of globalised trade and the manufacturing supply chain, as over four-fifths of world merchandise trade by volume is carried by sea.[10] UNCTAD also predicted that international trade would expand at an annual average growth rate of 3.5 per cent from 2019 to 2024.[11] According to the 2023 Review of Maritime Transport 2023, this prediction did not materialise.[12] Antithetically, international trade contracted by 0.4% in 2022; however, this decline is put into context when considering the sharp decline experienced in 2020 due to the Covid-19 pandemic and the subsequent extraordinary market surge that followed in 2021. Several other factors contributing to this decline include the Ukraine war, weaker global economic growth and high inflation.[13] In its 2023 Review, UNCTAD estimated the growth to be at 2.4% in 2023 and to continue moderately from 2024 to 2028. Consequently, ports cannot be left behind when ships are automated and digitalised. Such a discrepancy will likely lead to legal issues concerning the suitability of ports to accommodate smart and autonomous ships. Because charterers, especially time charterers, have an unrestricted right to use a chartered vessel to its maximum commercial potential, they are often obligated to send the vessel only to safe ports, berths and anchorages.[14] This obligation imposed on charterers provides surety for the shipowner that his vessel, master, officers and crew will be protected from risks at the ports to which the vessel is sent despite being under the control or possession of the charterer. Under English law, the safe port undertaking covers various risks, including physical damage to the vessel and non-physical risks, such as delays and administrative risks. These risks will continue to affect smart and autonomous ships, albeit slightly different from how the courts have previously analysed them. Additionally, novel risks may emerge, such as the heightened risk of cyber security caused by increased reliance on technology. It is crucial to consider whether a cyber-attack renders a port unsafe. Moreover, because

[9] *Review of Maritime Transport 2020* (UNCTAD 2020) 121.

[10] *Review of Maritime Transport 2019* (UNCTAD 2019) 4.

[11] Ibid, x.

[12] *Review of Maritime Transport 2023* (UNCTAD 2023) 3.

[13] Ibid.

[14] *Whistler International Ltd v Kawasaki Kisen Kaisha Ltd (The Hill Harmony)* [2001] 1 AC 638 (HL).

unsafety is determined concerning a particular ship,[15] the advent of smart and autonomous ships will necessitate reconsidering what constitutes a safe port and what constitutes an abnormal occurrence.

Safe ports are a core feature of the carriage of goods by sea because this allocates liability between the shipowner and the time charterer. If a time charterer breaches the safe port obligation, it will be held liable for any losses or damages arising from the port's unsafety. This obligation carries significant commercial implications, leaving no room for leniency when assessing the port. As a result, ports, including those in developing regions, have no option but to adapt to accommodate smart and autonomous ships safely or risk classification as 'unsafe'. In such circumstances, time charterers will refrain from nominating such ports or, if nominating them, shipowners will call on the charterer to nominate an alternative.[16] Developing regions that lack the resources or political will to decrease or eliminate risks to smart and autonomous ships will likely be affected. Therefore, this paper argues that governments in developing regions must increase research and investment in developing smart ports.

In order to analyse how the law on safe ports applies to smart and autonomous ships, it is essential to understand how these ships are defined. This will facilitate evaluating the major changes ports must implement to accommodate smart and autonomous ships safely. Additionally, this paper will examine the areas of concern that could lead to 'port unsafety' in the context of smart and autonomous ships and how the law on port safety, as established by case law, would allocate liability for these risks. The paper will recommend standardising infrastructure and facilities, port interoperability and cyber security management.

2 Understanding smart and autonomous ships

The International Maritime Organization (IMO) defines MASS as including ships with varying levels of automation. These range from partially automated systems and decision support, which assist the human crew, to fully autonomous systems operating without human intervention.[17]

[15] *Palm Shipping Inc v Vitol SA (The Universal Monarch)* [1988] 2 Lloyd's Rep 48.

[16] *Kodros Shipping Corporation v Empresa Cubana De Fletes (The Evia) (No 2)* [1983] 1 AC 736 (HL), 764.

[17] See the varying degrees in 'Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS)', MSC.1/Circ.1638, 2.

Smart ships are a result of the increasing digitisation and digitalisation of ships. Traditional ships are being transformed through these processes, giving rise to smart ships.[18] Four core elements make up the smart ship:

1) Navigation: The ship's navigation is conducted by sensors fitted on the ship.[19] These sensors feed data into the navigation subsystem. The data is combined by a software-based sensor fusion block, creating images of the real world.[20] A software-based system called Situation Awareness (SA) then assesses the images and translates the data into actional information.[21]
2) Guidance: The navigational subsystem's created images and other relevant data are utilised by the guidance subsystem to delineate the vessel's route. This includes information on nearby obstacles to avoid collisions, the planned route from origin to destination, other navigational factors, and the status of other ships. [22]
3) Physical ship: Additional hardware may be installed on the physical ship to collect data and support the software-based decision-making system. For example, hardware may replace a master physically viewing the environment from the ship's bridge.[23]
4) Control: The ship is steered in the right direction or controlled by the software-based control system, which processes data from the guidance system and converts it into commands for the various hardware positioning systems on the ship.[24]

These core functional elements or main technologies enable a ship to autonomously traverse the ocean.[25] The most prominent distinction between smart and fully autonomous ships lies in the absence of the crew. Remote control centres may and will likely compensate for this lack of onboard crew.[26]

[18] *Smart Ships and the Changing Maritime Ecosystem* (n 4) 5.

[19] Jesús A Muñoz and Rodrigo Pérez, 'Design of SMART Ships for the IoT' (2017) ICC <https://dl.acm.org/doi/pdf/10.1145/3018896.3018930> accessed 7 April 2024, 4.

[20] Ibid, 6.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Illkyun Im, Dongryeol Shin, Jongpil Jeong, 'Components for smart and autonomous ship architecture based on intelligent information and technology' (2018) 134 Procedia Computer Science <Components for Smart Autonomous Ship Architecture Based on Intelligent Information Technology - ScienceDirect> accessed 18 May 2023.

[26] 'R&D Roadmap for Smart and Autonomous Sea Transport Systems' (SINTEF, TCOMS October 2020) [17] <rd-road-map-smart-autonomous-shipping.pdf (sintef.no)> accessed 18 May 2023.

Smart ships, therefore, serve as the stepping stone toward the eventual realisation of fully autonomous ships. Hence, this paper analyses port safety in the context of smart and autonomous ships. Technology readiness levels indicate that sensor technology is highly advanced and is already being implemented in operational environments, technology that assists ships is at an average readiness level, and fully autonomous ships are at a low technology readiness level.[27] These technology readiness indicators reveal that the issue of port safety is imminent, at least concerning smart ships. Ports that are unable or unwilling to adapt quickly may face detrimental effects. However, technology is developing rapidly, and newer and larger ships are already fitted with highly advanced technological systems.[28] Therefore, investigating port safety in relation to fully autonomous ships is not premature.

3 The problem

The crux of the problem can be summarised as follows: 'A Smart ship will not be able to function in an optimal manner in a conventional port that lacks the corresponding infrastructure systems to support the intelligent systems …'[29] Similarly, it has been argued that 'autonomous ships will rely on highly automated port processes to compensate for the lack of onboard persons to handle, e.g., towage, anchoring, berthing, mooring and cargo handling.'[30]

UNCTAD's Director of the Technology and Logistics Division has commented that:

> Vessels and their cargo are becoming part of the Internet of Things by combining onboard systems and digital platforms. Developing countries will have to ensure that both, their IT and their transport systems, are prepared to connect to global logistics networks.[31]

However, the problem is that 80 per cent of ports still rely heavily on manual, legacy and paper-based transactions, such as whiteboards or spreadsheets, to manage critical services such as towage, pilotage, and boat launches, as well as arranging and executing tasks such as shipboard,

[27] *Smart Ships* (n 4) 7.
[28] Ibid, 8.
[29] R&D Roadmap (n 26) 16.
[30] Ibid, 17.
[31] UNCTAD 'Digitalization Set to Revolutionize Shipping – New United Nations Report' (UNCTAD, 3 October 2018) <Digitalization set to revolutionize shipping – new United Nations report | UNCTAD> accessed 5 November 2023.

ship-port interface and port-hinter-land-based exchanges.[32] According to Innovez One, a provider of port management software, most of the 4,900 ports worldwide do not utilise digital technology for even the most rudimentary processes.[33] While large 'Tier 1' ports are becoming 'smart ports' because of their profile and financial resources, 'Tier 2 and below' ports, the majority of ports, experience various inefficiencies in ordering, execution, and billing.[34] The result is a polarised port system where 20 per cent of ports are efficient, safe and sustainable while 80 per cent are on the opposite end of the spectrum, leading to risks of delays, ship safety concerns, late payments, increased fuel consumption and emissions, reduced revenues, and a lack of traceability.[35]

Approximately six decades ago, containers revolutionised global shipping, and this has gradually led to an increase in the size of ships. This 'container revolution' prompted ports and terminals to invest in new cranes and dredging equipment and required the reinforcement of walls and the extension of berths.[36] In contrast, the development of smart and autonomous ships relies on revolutionary technologies, including i) autonomous robots and systems, ii) the Internet of Things (IoT), iii) blockchain, iv) cybersecurity, v) horizontal and vertical system integration (HVSI), vi) cloud computing, vii) 3D printing and additive manufacturing, viii) big data and business analytics, ix) augmented reality, and x) simulation and modelling.[37] Consequently, ports worldwide need to reconsider and reinvest in their operations, as smart ships require smart ports that utilise the same key enabling technologies such as automation, artificial intelligence, big data, IoT and blockchain.[38] In addition to ensuring compatibility

[32] '80% of ports do not reap the benefits of digitalization' (Safety 4 Sea, 8 February 2021) <80% of ports do not reap the benefits of digitalisation> accessed 09 May 2023. See also Yoss Leclerc and Michael Ircha, 'Canada's Rapidly Evolving Smart Ports' in Tafsir Matin Johansson et al (eds), *Smart Port and Robotic Systems; Navigating the Waves of Techno-Regulation and Governance* (Palgrave Macmillan 2023) 183, who note that MASS vessels (Maritime Autonomous Surface Ships) will have to interact with Smart Port technology to safely enter and berth at a port.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Steve Saxon and Matt Stone, 'Container Shipping: The Next 50 Years' (McKinsey & Company, September 2017) <1543288787953_Steve-Saxon.pdf (hktdc.com)> accessed 18 May 2023, 13.

[37] *Review of Maritime Transport 2018* (UNCTAD 2018) 78; Zarzuelo (n 8) 1.

[38] 'What is a Smart Port' (Port Technology International, 14 April 2021) <What is a Smart Port? - Port Technology International> accessed 12 May 2023.

with smart and autonomous ships, smart ports have the potential to offer enormous benefits to the industry, and it is estimated that the global smart port market will reach 13.9 billion by 2027.[39]

Several questions arise regarding the interaction between smart and autonomous ships and ports. How will unmanned ships berth and manoeuvre within ports? How will smart, fully autonomous, and conventional ships co-exist, especially in heavily trafficked ports? How will compulsory pilotage operate? Will smart and autonomous ships require a change in the skills of port personnel?

Europe and Asia have shown a strong inclination toward preparing their ports to accommodate smart and autonomous ships.[40] In 2021, more than fifty partially automated ports were primarily located on these two continents. However, automation is increasing globally[41] and partially automated terminals have been implemented in countries such as Australia, Mexico, Morocco, Panama, the United Arab Emirates and the United States.[42] North America and Oceania have also started automating operations.[43]

In 2018, the Caofeidian harbour in China aimed to become the world's first fully autonomous port by conducting tests with fully self-driving trucks.[44] The same year, Yangshan Phase 4, the world's largest fully automated container port terminal, opened in Shanghai.[45] The port utilises automated handling equipment for loading and unloading.[46] Instead of workers, operations are conducted by remotely operated bridge cranes, auto-guided vehicles (AGV) and rail-mounted gantry cranes.[47]

[39] Hokey Min, 'Developing a smart port architecture and essential elements in the era of Industry 4.0' (2022) 24 Maritime Economics & Logistics 189, 191.

[40] According to research conducted by the IMO, three-quarters of port operators believe automation will be crucial to maintaining competitiveness by the middle of the decade. Furthermore, two-thirds of port operators consider automation to be essential to attaining operational security and efficiency. See Richard Clayton, 'Ports Await 5G Connectivity to Accelerate Innovation' *Lloyd's List* (London, 18 October 2022).

[41] Andrew Baskin and Mona Swoboda, 'Automated Port Operations: The Future of Port Governance' in Johansson (n 29) 149.

[42] Ibid, 150.

[43] Ibid, 156.

[44] 'Chinese port of Caofeidian tests fully autonomous trucks' (Safety 4 Sea, 18 May 2018) <Chinese port of Caofeidian tests fully autonomous trucks - SAFETY4SEA> accessed 19 May 2023.

[45] 'YSH4 in Shangai: The world's largest automated terminal' (Hapag-Lloyd, 30 September 2019) <YSH4 in Shanghai: The world's largest automated terminal - Hapag-Lloyd> accessed 19 May 2023.

[46] Ibid.

[47] 'World's biggest automated container terminal opens in Shangai' (Safety 4 Sea, 13 April 2023) <World's biggest automated container terminal opens in Shanghai - SAFETY4SEA> accessed 19 May 2023.

The port of Shanghai has reportedly invested substantially in big data, AI, the Internet of Things and automation, even before the COVID pandemic hit.[48]

The Port of Rotterdam, Europe's largest port, aims to be prepared for autonomous ships on a large scale by 2030.[49] The Maritime Port Authority of Singapore (MPA) recognises the importance of readying their ports to welcome autonomous vessels, envisioning 'future ready ports' where autonomous and manned ships co-exist.[50] In 2020, Singapore launched the MASSPorts networks consisting of the flag, coastal and port authorities of China, Denmark, Finland, Japan, the Netherlands, Norway and the Republic of Korea.[51] The network aims to 'facilitate port-to-port MASS trials to validate the proposed guidelines and test the interoperability of port-based systems'.[52]

In 2020, the British Port Association released a report evaluating the implications of autonomous shipping for UK ports.[53] The report identified the challenges and opportunities that autonomous ships will pose to UK ports. It concluded that a Voluntary Industry Code of Practice, providing guidance on the safe operation of small MASS, would be relied on until a more complex regulatory framework was developed.[54] Canadian container ports have also implemented smart technologies in order to transform their intelligent ports[55] into smart ports.

[48] Xin Chen and Cichen Shen, 'Port Digitalization Progressing, but Challenges Remain' *Lloyd's List* (London, 15 July 2022).

[49] Joe Baker, 'How Should Ports Prepare for Autonomous Shipping?' (Ship Technology, 3 December 2018) <How should ports prepare for autonomous shipping? (ship-technology.com)> accessed 9 April 2023. See also A Karas, 'Smart Port as a Key to the Future Development of Modern Ports' (2020) 14 International Journal on Marine Navigation and Safety of Sea Transportation 27, which notes that European seaports such as the Port of Hamburg or Rotterdam are leading the smart port evolution.

[50] Shirley Tay, 'How Singapore is Gearing up for Autonomous Shipping' (Gov Insider, 24 November 2020) <How Singapore is gearing up for autonomous shipping (govinsider.asia)> accessed 10 May 2023.

[51] Ibid.

[52] Ibid.

[53] 'Automation of Ships in Ports and Harbours' (Setfords Solicitors (for the British Port Association), September 2018): <automisation_of_ships_in_ports_and_harbours.pdf (britishports.org.uk)> 5.

[54] Ibid.

[55] See Yoss Leclerc and Michael Ircha, 'Canada's Rapidly Evolving Smart Ports' in Johansson (n 29) 175, which defines the term 'intelligent port'. Intelligent ports use advancing information and communication technologies (ICT) to develop situational awareness of people, processes, procedures, and the flow of information/data via the internet. It also notes that before Ports can be 'smart ports', they must be 'intelligent ports'. 'Intelligent ports' focus on ensuring they have efficient operations within a dynamic environment and that they can react and proactively lessen external and internal impacts.

Ports have not adequately considered the critical role they will play in facilitating autonomous ships.[56] This is particularly true for ports in certain regions, particularly developing regions.[57] The automation of ports requires significant upfront capital investment and commitment to the new technologies.[58] As a result, the adoption of digitalisation is uneven because ports have different capabilities.[59] The international nature of shipping does not permit a divide between ports in the West and in developing and emerging economies. It is argued that this type of 'significant financial obligation and expanded investment horizon requires consideration of new business models and, perhaps, a different approach to collaboration'.[60] Concession-based project finance for smart port development in emerging and developing economies might provide a possible solution.[61] The importance of collaboration is further highlighted by the commitment of the Singapore Maritime and Port Authority, the IMO, the World Bank, and other interested partners to support IMO Member States in digitalising their ports, particularly in capacity building and implementing the Maritime Single Window.[62] In January 2022, UNCTAD also started implementing a project aimed at supporting three 'African countries in assessing the progress of one port on the path to transition into a Sustainable and Smart Port (SSP)'.[63] The project will span three years and also includes accompanying these three ports in creating action plans to promote this shift.[64] Ports in Africa,

[56] Baker (n 49).

[57] The training and upskilling of seafarers is an area of particular concern. As shipping adopts new technologies, it is important to ensure that complementary crew training is provided to deliver the technologies' efficiencies: see Richard Clayton, 'Nigerian Seafarers Need Upskilling as Digital Technologies Evolve' *Lloyd's List* (London, 21 September 2023).

[58] Baskin and Swoboda (n 41) 179.

[59] Martin Wallgren, 'Shipping's Digitalization Requires Trust and Collaboration to Succeed' *Lloyd's List* (London, 13 May 2021).

[60] Baskin and Swoboda (n 41).

[61] Jason Chuah, 'Concession-Based Project Finance for Smart Ports with a Special Focus on Emerging Economies' in Johansson (n 32) 189.

[62] Kitack Lim, 'Future of Shipping: Digitalization' (Future of Shipping Webinars- jointly hosted by IMO and the Maritime and Port Authority, Singapore, 8 October 2020).

[63] Luisa Rodriguez, 'Sustainable Smart Ports to Create Prosperity for All in Times of Disruption and Uncertainty' (UNCTAD, 19 September 2022) <Sustainable smart ports to create prosperity for all in times of disruption and uncertainty | UNCTAD> accessed 18 November 2023. The article defines a 'Sustainable Smart Port' as a 'port that capitalises on (or maximises) the use of technology (or of 'technology-enhanced intelligence' to improve its performance, simultaneously, in the three pillars of sustainability'.

[64] Ibid.

small island developing states (SIDS) and least developed countries (LDCs) have been identified as particularly needing this ‘special attention’ in their digitalisation efforts.[65]

4 Changes in ports

The emergence of smart and autonomous ships undoubtedly necessitates the adaptation of ports. This paper will outline three areas requiring substantial changes: infrastructure, work-process automation, and security.

Firstly, port infrastructure must be capable of accommodating the smart systems utilised by smart and autonomous ships. Ports need to consider the sensor-dependent nature of these ships, which calls for implementing sensors within ports. Sensing technologies play a crucial role in smart ports; these sensors measure the physical characteristics of objects and convert them into numerical values that another device or the user can read.[66] This will create a system for communication between the vessels and ports, facilitating seamless operations.[67] These smart sensors and other key infrastructures, including actuators, wireless devices and data centres, comprise the critical infrastructure of smart ports.[68] Port equipment, such as tugs, will also have to be capable of catering to smart and autonomous ships. Moreover, ports will have to evaluate the suitability of their existing infrastructure, including quays used alongside berthing, navigation channels accommodating different types of vessels, and

[65] ‘IMO and Singapore to give “special attention” to developing ports in data digitalization pilot’ (Port Technology International, 3 May 2021) <IMO and Singapore to give ‘special attention’ to developing ports in data digitalisation pilot - Port Technology International> accessed 6 May 2024.

[66] Min (n 39) 190; Yongsheng Yang et al, ‘Internet of Things for Smart Ports: Technologies and Challenges’ (2018) 10.1109 IEEE Instrumentation Measurement Magazine <Internet of things for smart ports: Technologies and challenges (researchgate.net)> accessed 17 November 2023, 34

[67] R&D Roadmap (n 26) 16.

[68] Yang (n 66) 34

potential obstacles to navigation, such as lifting bridges and locks.[69] Additionally, developing onshore facilities that will enable the remote operation of vessels will be imperative.[70]

Regarding fully autonomous ships, ports must undergo complete automation across three dimensions: the container yard, various interfaces, and the foreland and hinterland.[71] Automating the container yards entails using information systems managed by terminals to handle the flow and stacking of containers.[72] Equipment used within an automated container terminal includes yard cranes, automated guided vehicles (AGV), and quay cranes.[73] For instance, the Yangshan Phase 4 terminal serves as a poignant example. Strikingly devoid of human presence, save for a few truck drivers and isolated workers, it provides an example of the level of automation that can be achieved.[74] Upon entering, truck drivers scan a chip card at this terminal, and the scanner reads the data, informing the driver of the collection point. Subsequently, an AGV brings the designated container.[75] The automation of port interfaces includes several crucial aspects, such as automated mooring systems and gate systems. These gate systems will accurately and swiftly identify a driver's identity, license plate number, and container number. Finally, the automation of foreland and hinterland processes involves the automation of processes beyond the terminal operation, such as self-driving and self-loading trucks and self-driving containers, which will transport containers to the various inland distribution centres or yards.[76]

[69] 'Automation of Ships in Ports and Harbours' (n 50) 5. In May 2023, Kongsburg completed a demonstration voyage of a remote and autonomous ship called the *Eidsvaag Pioner*. The vessel was automatically undocked from the quay, automatically controlled through the navigation and manoeuvres out of the harbour toward the open sea and successfully avoided sea traffic and islands. Upon its return to port it still successfully navigated the congested waterways before automatically docking. This demonstration was indicated to be an opportunity to show the world that remote and autonomous technologies can be successfully deployed on a general cargo voyage. However, it also highlights the important navigational and infrastructural challenges that ports will have to consider when accommodating smart and autonomous ships.

[70] Ibid.

[71] Baskin and Swoboda (n 41) 149.

[72] Ibid, 150.

[73] Yang (n 66) 35.

[74] Hapag-Lloyd 'YSH4 in Shanghai: The World's Largest Automated Terminal' <YSH4 in Shanghai: The world's largest automated terminal - Hapag-Lloyd> accessed 17 May 2023. Another example of an automated container terminal is Xiamen Ocean Gate in China.

[75] Ibid.

[76] An example is the port of Caofeidan's use of self-driving trucks. See also Kok-Lim Alvin Yau et al, 'Towards Smart Port Infrastructures: Enhancing Port Activities Using Information and Communications Technology' (2020) 10.1109 IEEE < Towards Smart Port Infrastructures: Enhancing Port Activities Using Information and Communications Technology | IEEE Journals & Magazine | IEEE Xplore> accessed 18 November 2023, 83400.

Similarly to the standardisation of container specifications and port equipment that facilitated the global adoption of containerisation,[77] the standardisation of port infrastructure, equipment, and facilities will be indispensable to ensure that the full benefits of smart and autonomous ships are realised.

Secondly, port processes must be automated, encompassing towage, anchoring, mooring, and cargo handling. [78] Magnetic berthing will be specifically required for fully autonomous ships.[79] Automating these processes will require new types of cyber-physical systems and new standards for communication and interaction.[80] The standardisation of communication and interaction is particularly vital. Digital Data Streams (DDS), initially introduced in shipping through Automatic Identification Systems (AIS) and which will form the foundation of fully autonomous ships, require the messaging format to be standardised.[81] Standardised DDS will facilitate automated information exchange, allowing communication between ships, between ships and ports, and between ports.[82]

Additionally, port systems and procedures facilitating intelligent coordination and vessel traffic management will play an increasingly crucial role, considering the diverse range of vessel types that ports must manage. This will include the implementation of Just-In-Time protocols and adherence to the Facilitation Convention (FAL) to improve operational efficiency.[83] Adequate training of port personnel will also be necessary.

The third area to consider is the security of ports and port facilities, which potentially hold significant implications for their competitiveness. This paper advocates for the increased digitalisation and automation of ports worldwide to safely accommodate and harness all the potential benefits of smart and autonomous ships. However, it is crucial to emphasise the criticality of investing in cybersecurity alongside these advancements.

[77] Richard Watson, Mikael Lind, Sand Haraldson, ‘Physical and Digital Innovation in Shipping: Seeding, Standardizing, and Sequencing’ (Proceedings of the 50th Hawaii International Conference on Systems Sciences, 2017) 4757.

[78] R&D Roadmap (n 26) 17.

[79] Baker (n 49).

[80] R&D Roadmap (n 26) 17.

[81] Watson (n 77) 4759. DDS will enable the autonomous, unmanned ship to determine its speed and route.

[82] Ibid.

[83] R&D Roadmap (n 26) 20.

Effective cybersecurity management becomes paramount in this context, and ports must develop and implement robust cybersecurity measures to protect their operations.[84] Additionally, ensuring cyber resilience will be necessary, meaning that ports must be capable of recovering quickly in the event of a successful cyber-attack.[85] The highest levels of port management must prioritise this responsibility,[86] as smart ports must be inherently designed to be cyber-resilient. Cyber security cannot be an afterthought.[87]

5 Port safety

The contractual promise of the charterer to nominate a safe port is well-established. It is an important area of law to consider in light of smart and autonomous ships because a large proportion of international shipping operates on charter at any single time.[88] It is based on the exchange of the charterer's right to exploit the commercial value of the ship without granting it the liberty to discount the owner's continuing interest in the vessel and for the personal welfare of the crew and master.[89] The obligation encompasses safeguarding ships from physical and non-physical risks.[90] The oldest case on port safety, *Ogden v Graham,*[91] addressed the political unsafety of a port, a risk unrelated to the physical characteristics of a port. This factor holds significance for this paper because it asserts that non-physical risks, such as the systems and processes implemented at a port, the skills of port personnel, issues of standardisation, and cyber security risks, are likely to be areas of significant concern to smart and autonomous ships. Ports that cannot safeguard smart and autonomous ships because of

[84] Wärtsilä, 'Seeking Cyber Resilience for the Emerging Technology Waves' *Lloyd's List* (London, 19 April 2022).

[85] David Foo 'Future of Shipping: Digitalization. Maritime Perspectives Series – jointly organised by the International Maritime Organization (IMO) and the Maritime and Port Authority of Singapore (MPA)' (Future of Shipping Webinars- jointly hosted by IMO and the Maritime and Port Authority, Singapore, 8 October 2020).

[86] *IAPH Cybersecurity Guidelines for Ports and Port Facilities Version 1.0* (International Association of Ports and Harbors 2021) <https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf> 10. See further Richard Clayton, 'Chief Executives are First in Line in Solid Cyber-security Defence' *Lloyd's List* (London, 28 February 2023).

[87] Foo (n 85).

[87] IAPH (n 86) 10.

[88] Stephen Girvin, 'The Commercial Implications of the ISPS Code' (2005) 330 Marlus 307, 321.

[89] Howard Bennett, 'Safe Port Clauses' in Rhidian Thomas (ed), *Legal Issues Relating to Time Charterparties* (Informa Law from Routledge 2008) 47.

[90] Examples of physical risks to the vessel include inadequate depth of water or the absence of a safe anchorage. Physical risks are the most frequently encountered risks forming the subject of port safety cases.

[91] (1861) 1 B & S 773. See Stephen Girvin, 'The Safe Port in Maritime Law: Decade of Certainty or Muddier Waters?', NUS Centre for Maritime Law Working Paper 17/02 (March 2017) 5.

failures in these areas create the risk that charterers of these vessels will be held contractually liable for sending the vessels to such ports. The safe port obligation imports a strict liability onto the charterer.[92] This strict contractual obligation requires charterers to consider the unique characteristics of the vessel chartered when sending it to a port. It is also said that the charterer's liability is so severe that it carries the risk of the failure of anybody else, such as the quay-owner or harbour authorities, to ascertain the safe condition of the port or berth.[93]

Moreover, the contractual nature of the obligation means that courts will not depart from 'the meaning of the relevant words' when interpreting the clause.[94] The safe port obligation has significant implications for the relationship between the shipowner and the charterer.[95] In the words of Thomas Rhidian, in the result of loss or harm to the ship, the charterer will be 'absolutely liable,' 'no excuses will be entertained.'[96]

However, it also has important implications for the ports because characteristically unsafe ports will be discriminated against by charterers who wish to avoid liability for breaching the safe port obligation. Indeed, the 2022 Tokyo cyber attack is an example of this issue. The Tokyo MOU Port State Control (PSC) authority revealed that in July 2022, its systems were attacked, resulting in its data being impacted for months. The PSC stated that this attack not only impacted the availability of data for ship inspection risk assessment 'but could have also created difficulties for charterers in decision-making'.[97] Since ports of this nature are likely to be situated in developing regions, they will undoubtedly contribute to entrenching inequality with more developed regions.

[92] Howard Bennett (gen ed), *Carver on Charterparties* (2nd edn, Sweet & Maxwell 2021) 205.

[93] Jan Ramberg, *Unsafe Ports and Berths: A Comparative Study of the Charterer's Liability in Anglo-American and Scandinavian Law* (Universitetsforlaget 1967) 605.

[94] *Arnold v Britton* [2015] UKSC 36, [2015] AC 1619, [15].

[95] See Ramberg (n 93) 562, where the contractual nature of this safe port promise is emphasised. The author notes that it is possible to impose a duty on the charterer to direct the vessel only to safe ports and berths. If the charterer thereafter directs the vessel to an unsafe port or berth, it has breached the obligation imposed on it. It must compensate the shipowner in damages, subject to the ordinary rules as to remoteness, causation and mitigation: see David Foxton et al (eds), *Scrutton on Charterparties and Bills of Lading* (25th edn, Sweet and Maxwell 2024) [9-023].

[96] Rhidian Thomas, 'The Safe Port Promise of Charterers from the Perspective of The English Common Law' (2006) 18 SAcLJ 602. See also Choi Wai Bridget Yim, 'Safe Port Promise by Charterers: Rethinking Outstanding Complications' (2016) 30 Australian and New Zealand Maritime Law Journal 1 [2.4].

[97] Adam Corbett, 'Tokyo MOU Reveals Cyber-Attack Compromised Data' (Tradewinds, 9 May 2023) <Tokyo MOU reveals cyber-attack compromised data | TradeWinds (tradewindsnews.com)> accessed 18 April 2024.

High levels of investment are going into smart and autonomous ships because of the refutable benefits they will offer to increase the safety and efficiency of transport and trade. As their usage increases, this strict safe port obligation on charterers will demand that the ports they nominate for the smart and autonomous ships have duly adapted in the abovementioned ways.

The concept of port safety was defined in *The Eastern City*:[98]

> If it were said that a port will not be safe unless, in the relevant period of time, the particular ship can reach it, use it, and return from it without, in the absence of some abnormal occurrence, being exposed to danger which cannot be avoided by good navigation and seamanship …[99]

This definition includes several exceptions or defences against a finding of unsafety for the charterer. One such defence applies when the shipowner or master could have avoided the danger through good navigation and seamanship. This is because most, if not all, ports will have some dangerous aspects to them; however, provided there are countermeasures put in place to minimise the dangers[100] and such dangers can be overcome by good navigation and seamanship, the port will be safe.[101] In *The Polyglory*[102] case, Parker J established the test for 'good navigation and seamanship,' stating that 'the port will be safe if an ordinarily prudent and skilful master can find a way of reaching it safely'.[103] If more than this is required of the master, the port could arguably be deemed unsafe.

Moreover, considering non-physical risks are more likely to pose problems for smart ports, 'prudent conduct' can replace 'good navigation' when assessing whether the danger could be avoided.[104] Therefore, if the envisaged danger is the risk of a cyber attack at the nominated port and such a risk cannot be 'avoided by the response that a reasonable master might reasonably be expected to adopt', the port could be deemed unsafe. A shipowner could decline the order to such a port.[105] In this context,

[98] *Leeds Shipping Co Ltd v Societe Francaise Bunge (The Eastern City)* [1958] 2 Lloyd's Rep 127 (CA).

[99] Ibid, 131.

[100] Choi (n 96) [2.5].

[101] See *The Eastern City* (n 98) 131.

[102] *Kristiandsands Tankrederi A/S v Standards Tankers (Bahamas) Ltd (The Polyglory)* [1977] 2 Lloyd's Rep 353 (quoting Devlin J in *GW Grace & Co Ltd v General Steam Navigation Co Ltd (The Sussex Oak)* [1950] 2 KB 383, 391).

[103] Ibid*,* 362.

[104] Bennett (n 89) 57.

[105] Ibid.

an example of imprudent conduct by the master or shipowner would be negligence concerning their cyber security on board the ship.

The safe port definition encompasses ports, wharves, berths, and other places within the port.[106] The safe port obligation is invariably included in standard form time and some voyage charterparty contracts.[107] The NYPE 2015 form is an example of a time charterparty standard term, which guarantees loading and discharge at 'any safe anchorage or at any safe berth or safe place'.[108] In cases where the charterparty does not explicitly provide such a warranty, one may be implied under the general rules of implication and business efficacy.[109] This includes ascertaining the intention of the parties to the contract.[110] An example of a voyage charterparty standard term is the Shellvoy 6, which states that 'Charterers shall exercise due diligence to order the vessel only to ports and berths which are safe for the vessel …'.[111]

While it is said that this definition does not represent the ultimate solution in determining what a safe port is in a particular case, it has proven to withstand the test of time.[112] Therefore, this paper will analyse how some of the various elements of this definition might apply to smart and autonomous ships and smart ports.

5.1 'The Particular Ship'

As previously mentioned, the safety of a port is contingent upon the specific type of ship that is under charter. Consequently, the ship's particular features become crucial in assessing the port's suitability for accommodating the vessel.[113] This principle finds support in judicial decisions, starting with the

[106] Where the contract only provides for a safe berth and not a safe port, only the safety of the port is warranted unless the unsafety of the entire port affects the nominated berth: see *Atkins International HA v Islamic Republic of Iran Shipping Lines (The APJ Priti)* [1987] 2 Lloyd's Rep 37 (CA), 42.

[107] See, eg, Asbatankvoy, cl 9. See also *The Eastern City* (n 98), where the charterparty included an obligation to 'proceed to one or two safe ports in Morocco'. There is no printed clause in the Gencon form other than in the context of the 'near clause'.

[108] See Baltime (2001 rev), cl 14; Gentime, cl 2(a).

[109] See Stephen Girvin, *Carriage of Goods by Sea* (3rd edn, OUP 2022) 441; *The APJ Priti* (n 106) 42; *Scrutton on Charterparties and Bills of Lading* (n 95) [9-012].

[110] Ramberg (n 93) 589.

[111] See cl 4. It should also be noted that this clause is qualified by 'due diligence', and therefore, the charterer is only required to exercise 'reasonable care', determined objectively, in nominating a safe port: see *K/S Penta Shipping A/S v Ethiopian Shipping Lines Corp (The Saga Cob)* [1992] 2 Lloyd's Rep 545 (CA), 551.

[112] *Transoceanic Petroleum Carriers v Cook Industries Inc (The Mary Lou)* [1981] 2 Lloyd's Rep 272, 276; *Gard Marine & Energy Ltd v China National Chartering Co Ltd (The Ocean Victory)* [2017] UKSC 35, [2017] 1 WLR 1793, [11].

[113] *Scrutton on Charterparties and Bills of Lading* (n 95) [9-019].

landmark case, *The Eastern City.* In this case, the court considered the vessel's classification as a large ship. It held that the master had not acted inappropriately by attempting to depart from the port, as it aligned with the customary practice of larger vessels utilising the port.[114] Indeed, the courts have indicated such a concern by looking at the specifics of the particular ship in question, such as whether the ship was laden or in ballast.[115]

Moreover, including the closely related 'safely aground' clause in certain charter parties, such as the NYPE 2015, underscores the significance of the nature and characteristics specific to each vessel. The clause stipulates that;

> The vessel during loading and/or discharging may lie safely aground at any safe berth or safe place where it is customary for vessels of a similar size, construction, and type to lie at the following areas, ports…, if so requested by the charterers, provided it can do so without suffering damage.[116]

It is, therefore apparent that smart and autonomous ships, characterised by their unique features propelled by highly advanced technologies, necessitate equivalent technological adaptations by the ports accommodating them.

5.2 'The Relevant Period of Time'

The charterer's obligation is one of prospective safety rather than a continuing warranty. This entails an assessment of the breach of the safe port promise based on the date of port nomination.[117] However, the warranty pertains to the characteristics of the port when the ship arrives in the future.[118] Any characteristics deviating from the ordinary characteristics of the port are classified as an 'abnormal occurrence,' and liability for such occurrences does not rest with the charterer but with the shipowner's insurer.[119] Two questions arise: firstly, what knowledge is required of the charterer, and secondly, what

[114] *The Eastern City* (n 98) 133.

[115] See *Brostrom & Son v Dreyfus & Co* (1932) 44 Ll L Rep 136, 137; *Limerick Steamship Co Ltd v WH Stott & Co Ltd* [1921] 1 KB 568.

[116] Clause 1(d). This is an optional clause in NYPE 2015.

[117] *The Ocean Victory* (n 112) [21].

[118] *The Evia (No 2)* (n 16) 764.

[119] *The Ocean Victory* (n 112) [25]-[26].

information would such a charterer rely on to determine the safety of a specific port for a smart or autonomous ship under charter?

5.3 The knowledge requirement

In *The Evia (No 2)*,[120] Lord Roskill states that any obstacles, such as collisions in the approaches or any conditions like ice-bound ports, which 'would in all human probability be out of the way' before the ship was required to enter the port, would not render the port unsafe. This means that although such obstacles and unsafe conditions may exist before the ship arrives, the port is still considered safe if the charterer expects them to be resolved by the vessel's arrival. Consequently, when determining the safety of a port, the court would need to retrospectively evaluate the facts relating to the port at the time of nomination. It has been argued that these facts enable the charterer to form an expectation or prediction regarding the prospective safety of the port.[121] How the courts assess the charterer's knowledge of the nominated port's facts is crucial, especially considering the emergence of smart and autonomous ships, as it sheds light on the nature of this warranty and how liability is likely to be determined between the charterer and shipowner.

The UK Supreme Court's ruling in *The Ocean Victory* has definitively settled that a foreseeability test is inadequate for determining the safety of a nominated port.[122] This case arose out of the grounding of the bulk carrier *Ocean Victory* at the port of Kashima in Japan. The vessel was on demise charter under the Barecon 89 form, as amended, which required trading between safe ports. The court had to consider whether the concurrent occurrence of long waves and northerly gales, a normal characteristic of the port separately, constituted an abnormal characteristic of the port.[123]

In the High Court,[124] Teare J concluded that the combination of these weather events did not qualify as abnormal and ruled that the port was unsafe. However, the Court of Appeal held that the judge was in error. This error stemmed from Teare J's application of the foreseeability test, referring to the occurrence of the two weather events, where he stated that 'nobody at the port could, I consider, be

[120] See (n 16) 757.

[121] David Chong Gek Sian, 'Revisiting the Safe Port' [1992] SJLS 79, 89.

[122] *The Ocean Victory* (n 112) [37]-[39], affirming *Gard Marine & Energy Ltd v China National Chartering Company Ltd (The Ocean Victory)* [2015] EWCA Civ 16, [2015] 1 Lloyd's Rep 581, [58]-[59].

[123] *The Ocean Victory* (n 112) [15].

[124] [2013] EWHC 2199 (Comm), [2014] 1 Lloyd's Rep 59.

surprised if they did [occur]' and described the occurrences as 'at least foreseeable'.[125] The Court of Appeal held that the judge derived this test from Mustill J's ruling in *The Mary Lou*,[126] but that case neither employed nor suggested using the foreseeability test as a stand-alone test.[127] Instead, foreseeability was considered along with the frequency of historical occurrences of the event as part of the relevant factors to be assessed when determining whether a particular event was a normal characteristic of the port.[128]

Previously, in *The Saga Cob*,[129] Parker LJ emphasised that the employment of a foreseeability test alone was insufficient for determining what constitutes a natural characteristic of a port, stating:

> [T]hat the guerillas had two boats and that they had made one seaborne attack 65 miles away, it was foreseeable that there could be a seaborne attack either en route from Assab to Massawa or in the anchorage at Massawa. If this were enough it would seem to follow that, if there were a seaborne guerilla or terrorist attack in two small boats in the coastal waters of a country in which there had been sporadic guerilla or terrorist activity on land and which had many ports, it would become a normal characteristic of every port in that country that such an attack in the port or whilst proceeding to it or departing from it was sufficiently likely to render the port unsafe.[130]

This statement clarifies that the mere theoretical foreseeability of an event does not automatically classify it as a 'normal characteristic' of a port. Applying a foreseeability test to the principle of strict liability would imply that any risks foreseeable as the probable result of a particular activity might, under certain circumstances, warrant strict liability on the charterer performing such activity.[131] This would certainly create disadvantageous results for the charterer. The court's rejection of this approach as impractical and unrealistic is welcome, particularly in light of the development of smart and autonomous ships and the advancement of smart ports. Implementing new and advanced technologies

[125] Ibid, [127].

[126] Above (n 112).

[127] *The Ocean Victory* (n 122) [58]. See also Charles Baker 'The Safe Port/Berth Obligation and Employment and Indemnity Clauses' [1988] LMCLQ 45, which argued that there was no indication in the speeches of Lord Roskill or Lord Diplock in *The Evia (No 2)* (n 16) that a charterer only needed to exercise reasonable foreseeability when nominating a port.

[128] See *The Mary Lou* (n 112) 278.

[129] *The Saga Cob)* (n 111), 550-551.

[130] Ibid.

[131] Ramberg (n 93) 58.

and infrastructure, port processes, and procedures discussed in this paper will introduce novel elements to the port environment, which may entail a new capacity for failure. It would be unreasonable to argue that it was foreseeable for a nominated port to be targeted by a cyber-attack due to the heightened vulnerability faced by digital or smart ports compared to traditional ports. Similarly, the occurrences of failures or malfunctions in any of the innovative technical systems or advanced equipment used in a smart port should not be deemed foreseeable. Adopting such an approach would pose an unrealistic risk of rendering numerous smart ports unsafe in the event of vessel damage or delays.

Applying a foreseeability test or any other knowledge requirement would not even be necessary when assessing the administrative safety of a port. In other words, when evaluating whether a port is deficient in its setup or management.[132] Port authorities must take 'reasonable precautions' by implementing specific systems to mitigate hazards at a port.[133] The effectiveness of these precautions lies in their ability to prevent the occurrence of danger; it is not sufficient for the port authorities to merely make an effort.[134] The port will only be safe if the implemented systems operate correctly. Therefore, a failure in port policies, systems, or procedures – for instance, the absence of a proper system or procedure to safely and without delay accommodate both autonomous ships and traditional ships within a single port[135] or incompetent pilotage and towage specifically for smart and autonomous ships or tugs that are unsuitable for smart and autonomous ships[136] – would render the port unsafe without requiring the court to assess what the charterer may have known or foreseen. It is arguable that a failure to implement appropriate systems would not qualify as an 'abnormal occurrence' either, and an isolated failure within a system that has historically worked well is also unlikely to constitute an abnormal occurrence.[137]

[132] *The Evia (No 2)* (n 16), 33.

[133] Ibid.

[134] *The Mary Lou* (n 112) 277.

[135] *Maintop Shipping Co Ltd v Bulkindo Lines Pte Ltd (The Marinicki* [2003] 2 Lloyd's Rep 655, [74], is an example of a case where the court found that the lack of proper systems at the port created a 'very unsatisfactory regime prevailing in the port administration in relation to the safety of vessels' (Belinda Bucknall QC).

[136] *Schiffahrt Nordhafen Ltd v Pacific & Gulf Carriers Corp of Liberia (The Aristagelos)* SMA 1423 (NY Arb 1980) is an example of a case where an arbitral panel found the port to be administratively unsafe because of incompetent pilotage and inadequate towage.

[137] Alexander McKinnon, 'Administrative Shortcomings and Their Legal Implications in the Context of Safe Ports' (2009) 23 Austl & NZ Mar LJ 186, 195.

Parker LJ in *The Saga Cob* appeared to endorse an analysis that looks to the charterer's actual knowledge.[138] In this case, the shipowners argued that if the port of Massawa was unsafe, it followed that the charterers, who knew all the relevant facts, had failed to exercise due diligence. However, the court disagreed with this notion. It held that in its view, 'if a charterer knows all the facts and orders the vessel to a port which is regarded generally by owners of the vessels to be safe, he might well be protected'.[139] Furthermore, the court emphasised that it decided the case based on what a 'reasonably careful charterer' would have known.[140] This approach is more forgiving towards the charterer as it analyses the question of port safety from their perspective, allowing it to argue that it acted reasonably in acquiring and evaluating the information upon which it based its conclusion regarding the port's safety. However, *The Saga Cob* dealt with the charterer's duty to exercise due diligence in nominating a safe port rather than imposing an absolute warranty. Therefore, this less stringent approach, which looks at the charterer's actual knowledge, might still hold validity and would be contingent on the charterer of a MASS vessel having more bargaining power than the shipowner. However, subsequent cases have held that an 'absolute knowledge approach' is preferred.[141] The 'absolute knowledge' approach completely disregards the charterer's actual or subjective knowledge and instead attributes all the relevant facts about the port's safety to it.[142] It has been argued that *The Evia (No 2)* adopted the absolute knowledge approach in its well-known definition of a safe port.[143] In this definition, the charterer's promise is unqualified by any knowledge or lack thereof.[144] The safety of the port is examined based on the facts existing at the time of nomination, which pertain to the time of the vessel's arrival.[145] *The Ocean Victory* confirmed this approach by stating that 'one has to look at the reality of the particular situation in the context of all the evidence, to ascertain whether the particular event was sufficiently likely to occur to have become an attribute of the port'.[146] This statement strongly suggests that the charterer's actual or subjective knowledge is irrelevant, and the court will only consider the

[138] Ibid, 192.
[139] *The Saga Cob* (n 111), 551.
[140] Ibid.
[141] This term is used by Chong (n 121).
[142] Ibid, 87
[143] Ibid, 89.
[144] Ibid.
[145] *The Ocean Victory* (n 112) [21].
[146] Ibid, [59].

facts as they existed at the time of nomination to determine whether the charterer was justified in assuming that those facts indicated the port would be safe for the vessel upon its arrival.

The preferred approach outlined above places a heavier burden and risk on the charterer concerning allocating the risk of liability for an unsafe port. Therefore, when applied to smart and autonomous ships, charterers are likely to assume the risks of sending such vessels to ports that have not adapted to accommodate them safely. This risk is further compounded by the fact that the defence of *volenti non fit injuria,* available to the charterer against an allegation of breaching the safe port warranty, has been determined subjectively.[147]

In *The Eastern City*, after the court found that the port was, in fact, unsafe, it had to consider whether the shipowner should have been debarred from recovering damages because it had voluntarily taken the risk of sailing to an unsafe port.[148] The reason for this is that the cause of the loss or liability is no longer the unsafety of the port; instead, the master's acceptance of orders to proceed to an obviously unsafe port would constitute a *novus actus interveniens*. In that case, the court clarified that it looked to the master's actual knowledge to determine whether he had voluntarily taken on that risk. In deciding the matter, Sellers LJ reasoned, 'it was not suggested, as we understand it, that the master had received any special warning of unusual danger and had deliberately ignored it,' indicating that the master needed to have actual knowledge of the unsafe conditions and carefully considered and performed his action with full awareness or consciousness.[149]

In *The Stork,*[150] Morris LJ explained that even if a safe port promise were breached, 'this would not justify the deliberate act of allowing the ship to suffer damage '.[151] The master or shipowner have to possess 'knowledge that the ship has been wrongly directed to run into danger'[152] and deliberately ignore that knowledge for the court to find that they voluntarily ran the risk. He further stated that the

[147] McKinnon (n 137) 190. See, generally, Andrew Tettenborn (gen ed), *Clerk and Lindsell on Torts* (24th edn, Sweet & Maxwell 2023) 3-47.

[148] *The Eastern City* (n 98).

[149] Ibid, 136. The *Oxford English Dictionary* defines 'deliberate' as meaning: 'carefully considered; done with full awareness or consciousness. In later use also (chiefly in negative sense, of an action regarded as undesirable or reprehensible): intentional; done on purpose rather than by accident'. See <https://www.oed.com/dictionary/deliberate_adj?tab=meaning_and_use#7249221> accessed 19 March 2024.

[150] *Compania Naviera Maropan S/A v Bowaters Lloyd Pulp & Paper Mills Ltd (The Stork)* [1955] 2 QB 68 (CA).

[151] Ibid, 104.

[152] Ibid.

shipowners or master were not always obligated to doubt the order's validity and had no duty to go beyond what was reasonably available to a prudent shipowner or master to obtain information.[153] Furthermore, Mustill J in *The Mary Lou* indicated that if the master acts reasonably, even though mistakenly, it is still unlikely that his actions will be a *novus actus interveniens*.[154]

The contrast between the use of an objective approach in ascertaining what the charterer knew about the nominated port and the subjective approach used to determine what the master knew about the port illustrates that the responsibility for the unsafety of a port accommodating smart and autonomous ships is likely to fall on the charterer.

In summary, the significance of analysing the nature of this safe port obligation in charterparty contracts, including what the charterer knew and the test utilised by the courts, lies in the allocation of risk. Since this is a commercial agreement, it must be evident when making the charterparty who will bear the risk of damage or delay of a smart or autonomous ship due to a port being unsuitable for such a vessel.[155]

As a result, the charterer that charters a smart or autonomous ship will risk assuming substantial liabilities if it sends the vessel to ports incapable of safely accommodating such ships, potentially leading to damage or delays to the vessel. Any facts indicating unsafety, such as inadequate cybersecurity management, unsuitable tugs, or deficient port processes and procedures, may contribute to a finding of unsafety. Since current indications of investment show that ports in developing regions are most likely incapable of safely accommodating smart and autonomous ships, charterers will be justified in their reluctance to send their vessels to those ports, thereby affecting their competitiveness,[156] otherwise termed as inter-port competition.[157]

[153] Ibid.

[154] *The Mary Lou* (n 112) 281-283.

[155] *EL Oldendorff & Co GmbH v Tradax Export SA (The Johanna Oldendorff)* [1974] AC 479 (HL), 553-554.

[156] See Karas (n 49) 28, who states that 'modern ports without intelligent solutions can not survive the intensity of competition'.

[157] See *Review of Maritime Transport 2019* (n 10) 50, which explains that inter-port competition is affected by conditions such as economic and regulatory issues.

5.4 What information?

The charterer is presumed to possess knowledge of all the relevant facts or information related to a port they have nominated.[158] Consequently, this information is of significant importance to charterers. There is a crucial need for readily available information concerning the state of ports worldwide, enabling charterers to make informed assessments, and this information is widely available.[159]

Charterers would require access to information regarding the infrastructure and equipment, cyber security management, and administrative processes and procedures of smart ports to effectively evaluate the safety of a port intended to accommodate smart and autonomous ships.

This paper contends that developing smart ports is essential for accommodating smart and autonomous ships. However, the heightened risk of cyber security issues requires specific attention to the information available to charterers concerning the cyber security state of a particular port. One crucial question in this regard is the extent to which cyber security risks render a port unsafe.

According to existing precedent, a single instance of a cyber-attack at a port would not automatically render a port unsafe, as '[t]he mere happening of a casualty does not necessarily imply a breach [of the safe port obligation]'.[160] Such an event would be considered an abnormal occurrence for which the charterer cannot be held responsible. Determining what qualifies as an abnormal occurrence depends on various factors, including the port's history, the frequency of the event, and the degree of foreseeability of the event occurring.[161] Therefore, evidence indicating repeated cyber-attacks or evidence showing that a port has not taken appropriate action to protect against cyber-attacks could lead to a finding of unsafety.

Cybersecurity represents one of the top three port risks, alongside piracy and terrorism,[162] and cyber incidents were rated second among the top five risks for the shipping and maritime sector.[163] In 2023, Australia's biggest port operator, DP World Australia, was the target of a cyber attack that led to the

[158] *The Ocean Victory* (n 112) [39].

[159] This can be obtained through various port databases such as Speed guide.net <SG TCP/IP Ports Database (speedguide.net)>.

[160] *The Mary Lou* (n 112) 278.

[161] *The Ocean Victory* (n 112) [38].

[162] Ignacio de la Pena Zarzuelo, 'Cybersecurity in Ports and Maritime Industry: Reasons for Raising Awareness on this Issue' (2021) 100 Transport Policy 1.

[163] *Review of Maritime Transport 2020* (n 9) 119.

suspension of operations at the major ports of Sydney, Melbourne, Brisbane and Fremantle.[164] The attack targeted systems enabling trucks to share data with the terminal operator. Consequently, although vessel operations could proceed, trucks could not enter or exit the facilities, resulting in over 30,000 containers stranded on the docks.[165] Furthermore, research conducted by the classification society DNV indicates that more than three-quarters of maritime professionals believe a strategic waterway or major port will be shut down due to a cyber attack in the next two years.[166] DNV also highlighted that the increased interconnection between ships and onshore technologies meant that attacks were 'likely to have a greater impact in the future'.[167]

Various organisations have published standards to address this challenge, such as the US National Institute of Standards and Technology (NIST)[168], the International Organization for Standardization (ISO/IEC 27001),[169] and the British Standards Institution (BSI). These standards apply universally to all industries and are valuable as they promote best practices and risk management and ensure efficient and sustainable operations.[170] The importance of these standards is evident in the fact that the IMO and the Baltic and International Maritime Council (BIMCO)[171] incorporate them when developing guidelines such as the *Guidelines on Cyber Security Onboard Ships* and Resolution MSC 428 (98) on Maritime Cyber Risk Management in Safety Management Systems.

[164] 'DP World Hack: Port Operator Gradually Restarting Operations Around Australia After Cyber Attack' *The Guardian* (London, 13 November 2023) <DP World hack: port operator gradually restarting operations around Australia after cyber-attack | Cybercrime | The Guardian> accessed 20 November 2023. Cf also the cyber attack against Transnet in South Africa in July 2021: *Building Capacity to Manage Risks and Enhance Resilience: A Guidebook for Ports* (UNCTAD 2022) 76-77.

[165] Marcus Hand, 'DP World Resumes Australia Port Operations After Crippling Cyberattack' (Seatrade Maritime, 20 November 2023) <DP World resumes Australia port operations crippled by cyberattack (seatrade-maritime.com)> accessed 20 November 2023.

[166] Paul Peachy, 'Cyber Attack Likely to Shut Down Major Waterway Within Two Years, DNV Warns' (Tradewinds, 6 June 2023) <Cyber-attack likely to shut down major waterway within two years, DNV warns | TradeWinds (tradewindsnews.com)> accessed 20 April 2024.

[167] Ibid.

[168] National Institute of Standards and Technology 'Framework for Improving Critical Infrastructure Cybersecurity' 2018 <Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (baltimorecityschools.org)> accessed 21 June 2023.

[169] International Organization of Standardization, 'ISO/IEC 27001 Information Security Management Systems' <ISO/IEC 27001 Standard – Information Security Management Systems> accessed 21 June 2023.

[170] British Standards Organization, 'Cybersecurity Standards: Protecting Networks, computers and data' accessed at <Cybersecurity Standards - Protecting networks, computers and data | BSI (bsigroup.com)> accessed 21 June 2023.

[171] Zarzuelo (n 162). See *The Guidelines on Cyber Security Onboard Ships* version 4 (2021) <https://www.ics-shipping.org/resource/guidelines-on-cyber-security-onboard-ships-version-four/> accessed 19 March 2024. See also *Review of Maritime Transport 2021* (UNCTAD 2021) 127.

Another example of published guidelines by the IMO is the *Guidelines on Maritime Cyber Risk Management*.[172] Unlike the Guidelines on Cyber Security Onboard Ships, these guidelines, along with MSC 428(98), apply to all stakeholders in the shipping industry, including ports and harbours. The *Guidelines on Maritime Cyber Risk Management* 'provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities'.[173] Additionally, they include functional elements aimed at supporting effective cyber risk management.[174]

The International Association of Ports and Harbor's (IAPH)[175] *Cybersecurity Guidelines for Ports and Port Facilities* is another example of industry-specific guidelines.[176] The *Guidelines* recognise that the rapid digitalisation in port communities heightens the urgency for executives to prioritise organisational cyber resilience.[177] The Guidelines support the global port community in line with the IMO's MSC-FAL 1/Circ 3. However, despite both sets of guidelines sharing similar elements in their approach to cyber security management, including protection, detection, and mitigation measures,[178] the IAPH provides more comprehensive guidance than the IMO's MSC-FAL 1/Circ 3. Specifically, the IAPH provides guidance to port executive committees in determining a reasonable level of investment in cyber risk management, a dimension lacking in the IMO's MSC-FAL 1\Circ 3.[179] While port managers have questioned the concept of a proposed level of investment and whether the return on investment would justify the spending,[180] it is submitted that establishing a reasonable level of investment for cyber risk management is essential for any guidance addressing cybersecurity risks in smart ports. Any doubt

[172] (MSC-FAL 1/Circ 3).

[173] Annex, para 1.1.

[174] The *Guidelines* define *cyber risk management* as 'the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions to be taken to stakeholders' (para 3.1).

[175] The IAPH is a non-governmental organisation comprising 168 ports and 143 port-related businesses globally: see *IAPH Guidelines* (n 86) 7.

[176] Ibid.

[177] Ibid, 8.

[178] Ibid, part 7. The MSC-FAL 1/Circ 3 identifies similar elements as the IAPH which include 'identify, protect, detect, respond and recover'. However, more detail is provided in relation to each element in the IAPH.

[179] See Executive Summary, 8.

[180] Clayton (n 86).

about this necessity indicates the incorrect perception that cyber security is not an integral part of port operations.[181]

While the *IAPH Guidelines* address this concern, they are not mandatory. Nevertheless, the IAPH has presented these *Guidelines* to the IMO Committee to garner support for their promotion and dissemination.[182] Furthermore, the IAPH has requested that the IMO include the Guidelines in the next version of the circular *Guidelines on Maritime Cyber Risk Management* as additional detailed guidance and industry standards.[183] Although this proposition could create minimum standards for cybersecurity in ports internationally, it does not create mandatory international standards.

Other relevant and essential instruments of the IMO are the International Ship and Port Facility Security (ISPS) Code[184] and the International Safety Management (ISM) Code.[185]

5.5 The ISPS Code

The ISPS Code is a maritime security instrument brought into force by Chapter XI-2 of the SOLAS Convention. The Code mandates various stakeholders, including contracting governments, government agencies, local administrations, and the shipping and port industries, to implement measures and procedures that enhance maritime security.[186] The ISPS Code exclusively addresses maritime security concerning both ships and ports. Part A of the Code sets out mandatory requirements, while Part B consists of recommendatory provisions for implementing the Part A provisions.

Important provisions of the ISPS Code related to ports include s 14, which obliges contracting governments to establish security levels, provide guidance for protecting against security incidents, and require port facilities to act accordingly. The security levels range from security level 1 to 3 and are defined as follows:

[181] Ibid.

[182] 'Measures to Enhance Maritime Security: IAPH Cybersecurity Guidelines for Ports and Port Facilities Submitted by IAPH' (IMO, 2 July 2021) <IAPH Cybersecurity Guidelines for Ports and Port Facilities (iala-aism.org)> accessed 7 July 2023.

[183] MSC-FAL.1/circ.3/Rev.1.

[184] 'International Ship & Port Facility Security Code and SOLAS Amendments 2002' (IMO, 12 December 2002).

[185] IMO, International Safety Management Code Resolution A741(18) as amended by MSC 104(73), MSC 179(79), MSC 195(80) and MSC 273(85) (IMO, 2010).

[186] See s 1.2.

- security level 1: ‘means the level for which minimum appropriate protective security measures shall be maintained at all times.’[187]
- security level 2: ‘means the level for which appropriate additional protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.’[188]
- security level 3: ‘means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.’[189]

According to the Code, the higher the security level, the greater the likelihood of a security incident occurring. The duty to set a security level cannot be delegated.[190] Ports operating at security level 1 must ensure that various activities outlined in s 14.2.1-7 are carried out, considering the guidance in Part B. These activities include ‘ensuring the performance of all port facility security duties,’[191] ‘controlling access to the port facility,’[192] ‘monitoring the port facility, including anchoring and berthing areas,’[193] ‘monitoring restricted areas to ensure only authorised persons have access,’[194] ‘supervising the handling of cargo,’[195] ‘supervising the handling of ship’s stores’[196] and ‘ensuring that security communication is readily available’.[197] If the security level increases, additional protective measures specified in the port facility security plan must be implemented for each of these activities.[198] When a port facility security officer is advised that a ship’s security level is higher than that of the port facility or the ship cannot comply with the Code’s requirement or its ship security plan, the port facility security

[187] s 2.1.9.
[188] s 2.1.10.
[189] s 2.1.11.
[190] s 4.3.1.
[191] s 14.2.1.
[192] s 14.2.2.
[193] s 14.2.3.
[194] s 14.2.4.
[195] s 14.2.5.
[196] s 14.2.6.
[197] s 14.2.7.
[198] s 14.3, s 14.4.

‘shall liaise with the ship security officer and coordinate appropriate actions, if necessary,’[199] and where appropriate ‘report the matter to the competent authority.’[200]

Section 15 of the ISPS Code mandates a port facility security assessment to evaluate the port’s security and identify the parts most vulnerable to an attack.[201] The assessments must be periodically reviewed and updated, considering the changing threats and other modifications in the port facility.[202]

Section 16 requires developing and maintaining a Port Facility Security Plan appropriate for the ship port/interface based on the security assessment. The security plan encompasses implementing measures to prevent the introduction of weapons, dangerous substances, or devices intended to harm persons, ships, or ports into the port.[203] It also includes measures to prevent unauthorised access to the port facility,[204] procedures for responding to security threats or breaches of security, provisions for maintaining critical operations of the port facility or ship/port interface,[205] procedures for periodic plan review and updating,[206] and procedures for reporting security incidences.[207]

Section 17 requires the designation of a Port Facility Security Officer for each port, responsible for fulfilling specific duties and responsibilities to ensure adherence to the Code.

Section 18 addresses drills, training, and other exercises related to port facility security.

Another noteworthy provision is reg 9 of SOLAS Chapter XI-2. This allows contracting governments to require ships intending to enter their ports to submit certain information. This information includes details about the ship’s certificate and its issuing authority, the security level at which the ship is operating, the security level at which the ship operated at any previous port where it conducted a ship/port interface and specification of any special or additional security measures taken by the ship in

[199] s 14.5.
[200] s 14.6.
[201] Barış Soyer and Richard Williams ‘Potential Legal Ramifications of the International Ship and Port Facility Security (ISPS) Code on Maritime Law’ [2005] LMCLQ 515, 517.
[202] s 15.4.
[203] s 16.3.1.
[204] s 16.3.2.
[205] s 16.3.3.
[206] s 16.3.8.
[207] s 16.3.9.

any previous port where it conducted a ship/port interface.[208] Regulation 9.2.3 stipulates that the ship must maintain records of this information for the last ten port facilities it entered.

If a ship's master fails to provide the requested information, the port may deny entry to the vessel.[209] The port may also deny entry if it has reasonable grounds to believe that the ship is non-compliant with the requirements of Part A of the ISPS Code.[210] This regulation could be necessary for managing cybersecurity in smart ports due to the increased risk associated with technological interfaces used for communication between smart and autonomous ships and ports. Smart and autonomous ships will likely regularly interface with ports through computer and network systems, for example, during compulsory pilotage.[211] Consequently, there is a significant risk of these ships potentially exposing subsequent ports to cybersecurity threats if they have previously visited a port with inadequate cybersecurity management. Therefore, the right of a subsequent port to deny entry to a vessel that has previously visited a port with poor cyber security measures becomes vital in the context of smart ports.

Part B, the non-mandatory part of the ISPS Code, offers guidance on implementing the security provisions of Chapter XI-2 of SOLAS and Part A of the Code. Concerning the Port Facility Security Assessment required under s 15 of Part A, this section emphasises that the assessment should specifically address 'radio and telecommunication systems, including computer systems and networks.[212] This also recommends that expert assistance be engaged in conducting this assessment.[213] Notably, s 15.7 identifies 'electrical distribution systems, radio and telecommunication systems and computer systems and networks' as crucial assets or infrastructure that should be prioritised based on their importance to the functioning of the port.

Moreover, s 15.11 stipulates that the assessment should consider potential threats resulting from security incidents, such as damage or destruction to the port facility or ship by explosive devices, arson, sabotage, vandalism, hijacking, seizure of the ship, tampering with cargo, essential equipment or

[208] Reg 9.2.1.

[209] See reg 9.2.5.4.

[210] Reg 9.2.1 (2.1-2.5).

[211] Most ports have implemented compulsory pilotage regimes in one form or another. In Singapore, this is imposed by the Maritime and Port Authority of Singapore Act 1996 (2020 rev ed), s 60. For the UK, see, eg, Richard Douglas, Peter Lane and Monica Peto, *Douglas & Geen on The Law of Harbours, Coasts and Pilotage* (5th edn, LLP 1997) para 20.58.

[212] Part B s 15.3.5.

[213] Part B, s 15.4.11.

systems of the ship or its stores, and the use of the ship as a weapon or a means to cause damage or destruction. These threats are highly relevant to the potential consequences of cyber-attacks against autonomous ships within the smart port's vicinity and smart ports themselves.

Furthermore, s 15.16 emphasises that identifying vulnerabilities in the physical structures of the port should include considering 'measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks'.[214]

The Port Facility Security Plan outlined in s 16.8.4 must account for 'the communication systems provided to allow effective and continuous communication between port facility security personnel and ships in port…'. The procedures and safeguards necessary to maintain such communication must always be upheld.[215] The security plan must also establish procedures and practices to protect security-sensitive information held in paper or electronic format.[216] Additionally, s 16.25.8 identifies essential electrical, radio, and telecommunication areas as potential restricted areas, allowing access to only authorised individuals for security reasons.

All the provisions mentioned above in Part B of the Code can be interpreted as including port cybersecurity matters. Furthermore, as analysed above, the requirements in Part A of the Code can be considered sufficient for managing the cybersecurity threat in smart ports. These requirements are sufficiently rigorous as they provide for assessments, plans, security officers, identification of essential assets and infrastructures, periodic reviews, and updates. UNCTAD confirms this analysis in its *Review of Maritime Transport 2020*, which states cybersecurity is covered under the ISPS Code.[217] It refers to Part B, s 8.3 of the Code, which provides that the security assessment should address '5. Radio and telecommunications systems, including computer systems and networks, and 6. Other areas that may, if damaged or used for illicit observation, pose a risk to persons, property or operations on board a ship or within a port facility'.[218] However, the report does not recognise that despite the scope of the mandatory requirements in Part A, their application to a port's computer and network systems remains merely recommendatory. Therefore, because of the split between Part A and Part B, ports could elect

[214] Part B, s 15.15.5.

[215] Part B, s 16.8.5.

[216] Part B, s 16.8.6.

[217] *Review of Maritime Transport 2020* (n 9) 119.

[218] Ibid, 119-120.

to fulfil the requirements of Part A of the Code concerning other areas of the port and port facilities, but not necessarily regarding the cybersecurity of their computers and network systems.

Another way to approach this issue is by assessing the extent and attitudes of contracting governments in implementing the ISPS Code. The first IMO progress report on implementing the ISPS Code acknowledged progress in certain areas, such as the number of training programs provided in developing regions.[219] However, it notably emphasised that the levels of implementation of the ISPS Code internationally varied. Specifically, the approval of Port Facility Security Plans was slower than the global average in Africa, Eastern Europe, and the Commonwealth of Independent States, highlighting the lack of uniformity resulting from the approach of the ISPS Code.[220]

The approach of the ISPS Code is to manage the security risks of ships and ports, mandating the assessment of these risks concerning each port to determine the appropriate security measures.[221] It does this in preference to setting detailed mandatory rules.[222] While this approach may suffice for traditional ports, more is needed for smart ports, for which this paper has advocated. Cyber security management should be enforced in a mandatory, standardised manner in smart ports, establishing a reasonable level of investment that smart ports must attain.

The ISPS Code addresses maritime security. Therefore, it is the most appropriate instrument to handle the increasing risk of cybersecurity incidents in digitalised ports. Although the Code only specifically mentions computer and network risks in Part B, it is arguable that the Code adopts a general approach to activities that threaten maritime security and which it is intended to detect and deter.[223]

The term 'security incident' is defined as 'any suspicious act or circumstance threatening a ship's security, including a mobile offshore drilling unit or a high-speed craft, or of a port facility or of any

[219] IMO Progress Report on the Implementation of the Special Measures to Enhance Maritime Security Details in SOLAS Chapter XI-2 and the ISPS Code: Note by the Secretariate IMO MSC 79th Session, Agenda Item 5, IMO Doc MSC 79/5/1 Secretariat (24 September 2004) Annexure 2 (Status of Implementation by Geographical Regions).

[220] Robin Bowley, *Preventing Terrorist Attacks at Sea: Maritime Terrorism Risk and International Law* (Routledge 2023) 59; IMO Progress Report on the Implementation of the Special Measures to Enhance Maritime Security Details in SOLAS Chapter XI-2 and the ISPS Code: Note by the Secretariate IMO MSC 79th Session, Agenda Item 5, IMO Doc MSC 79/5/1 Secretariat (24 September 2004) Annexure 2 (Status of Implementation by Geographical Regions)

[221] Soyer and Williams (n 201) 517.

[222] Bowley (n 220) 71.

[223] Proshanto Mukherjee, 'The ISM Code and the ISPS Code: A Critical Legal Analysis of Two SOLAS Regimes' (2007) 6 WMU J of Maritime Affairs 147, 158.

ship/port interface or any ship to ship activity'.[224] This definition can encompass the threat of cybersecurity incidents or cyber-attacks at smart ports. Coupled with the fact that the Code does not exclusively refer to any specific activities or crimes it deals with but suggests certain areas covered in Part B, there is ample reason to include the management of cybersecurity in smart ports as one of the 'security incidents' that the ISPS package is intended to prevent and combat.

On the other hand, the ISPS package, as a maritime security instrument, was created to address the dominant criminal offences in the maritime security domain, namely piracy and 'unlawful offences' under the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (the SUA Convention). However, because it was developed before the completion of the SUA offences and before resolving the dilemma of non-high sea piracy, it could not expressly articulate these criminal activities in its provisions.[225] Additionally, consideration of the *travaux préparatoires* of the ISPS Code leads to the conclusion that the SUA Convention serves as the Code's corresponding substantive criminal law instrument.[226]

Therefore, two potential approaches can be taken to determine whether cyber security management in smart ports could be included in the mandatory provisions of Part A. The first approach involves construing the definition of 'security incident', which represents the incidents the package aims to prevent and combat, as a 'catch-all imprecise justification for the application of the ISPS regime'.[227] The second approach interprets it more narrowly, applying only to the dominant maritime criminal offences of the SUA Convention.

Further essential aspects to consider regarding the suitability of the ISPS Code to address cyber security issues in ports, particularly smart ports, are highlighted in the Preamble of the Code. The Preamble expressly states that while the extension of the SOLAS Convention to cover port facilities was agreed upon due to its quick response to security threats, the provisions for port facilities would be limited to the ship/port interface. It was decided that the International Maritime Organization (IMO) and the International Labour Organization (ILO) would address the broader security issue within port areas. Additionally, it was agreed that the provisions should not extend to dealing with the actual response to

[224] *SOLAS Consolidated Edition 2020* (IMO 2020) reg 1.13.
[225] Mukherjee (n 223) 158.
[226] Ibid, 159.
[227] Ibid.

attacks or the necessary clear-up activities following an attack. As previously discussed, cyber security management in smart ports must incorporate security measures to prevent attacks and resilience measures to enable a quick recovery in case of an attack. This highlights that even if the ISPS Code is interpreted in the broader sense of including cybersecurity management in the definition of 'security incident', thereby incorporating it as part of the incidences to which the mandatory Part A applies, it would not be sufficient to address the entire spectrum of cybersecurity management required in smart ports.

Significantly, it should be noted that the ISPS Code does not clearly define the practical weight of the various threat security levels. The fact that a port is subject to the highest level of threat to security under the ISPS Code should not automatically render that port unsafe, and the converse would also be true.[228] A factual enquiry into whether the port had implemented sufficient measures to combat the danger would be necessary.[229] Moreover, if a port moves its security level to Security level 2 or 3, it could arguably be labelled as prospectively unsafe.[230] The level of reliance that can be placed on the designated security level of a port in determining whether there was a breach of the safe port obligation by the charterer is arguably opaque.

Moreover, whether a port is compliant or non-compliant with the ISPS Code is not determinative of the question of a breach of the safe port promise.[231] A fully compliant port could be unsafe where the threat was so potent and imminent that it could not be considered safe under the charterparty.[232] Again, the converse would be true because a non-compliant port would not constitute a breach in the abstract; rather, it would do so only if the aspect in which the port is non-compliant exposes the chartered vessel to an unacceptable level of risk from a security threat.[233]

Even if a shipowner obtained the information that a nominated port was not ISPS compliant, no case law indicates that a shipowner would be entitled to refuse to proceed to such a port. Suppose a port is generally considered unsafe because it puts the physical safety of the vessel in danger. In that case,

[228] Bennett (n 89) 53.

[229] Ibid.

[230] Stephen Girvin, 'The Commercial Implications of the ISPS Code' (2005) Marlus 307.

[231] Bennett (n 89).

[232] Ibid.

[233] Ibid, 54. Cf also Simon Kverndal QC, 'The ISM and ISPS Codes: Influence on the Evolution of Liabilities' in D Rhidian Thomas (ed), *Liability Regimes in Contemporary Maritime Law* (Informa Law from Routledge 2007) 151, 166.

mere non-compliance of the port is unlikely to constitute sufficient danger to justify the port being 'unsafe' under the definition in *The Eastern City*[234] and for the master to be entitled to refuse such an order.[235]

In *The Sussex Oak*,[236] Devlin J found that a shipowner is not obliged to comply with an illegitimate order, as the charterer would legally have no power to make such an order.[237] This case also recognised that an order to proceed to an unsafe port would be illegitimate, even if there were no express safe port clause in the charterparty.[238] However, the operation of this principle would depend on establishing the port's 'unsafety' due to its non-compliance. A potential solution to circumvent this issue is to specify explicitly in the charterparty that non-compliant ports are excluded. Any orders to such excluded ports would undoubtedly constitute an illegitimate order, falling outside the defined trading limits.[239]

This shows that the ISPS Code has failed to establish an international standard for port cyber security. To determine the facts of the cyber security management of a specific port, charterers, shipowners or courts would need to obtain information from the port authorities themselves. The problem with this is that port authorities may be reluctant to give out information relating to their security. Implementing a mandatory international standard would, of course, circumvent this issue.

5.6 The ISM Code

The ISM Code establishes international standards for the safe management and operation of ships and for pollution control.[240] It achieves this by outlining functional requirements for a Safety Management System (SMS) that every shipowner[241] must develop, implement and maintain.[242] The shipowning company must also appoint a 'designated person' to monitor compliance with the Code and ensure the availability of sufficient resources and shore-based support.[243] All the contracting states to SOLAS are

[234] See above (n 98).

[235] Soyer and Williams (n 201) 531.

[236] Above (n 102).

[237] Ibid, 396.

[238] Soyer and Williams (n 201) 530.

[239] *Halcyon Steamship Co Ltd v Continental Grain Co* [1943] KB 355 (CA).

[240] Preamble, s 1. See *Splitt Chartering APS v Saga Shipholding Norway AS (The Stema Barge II)* [2020] EWHC 1294 (Admlty), [2021] 2 Lloyd's Rep 307, [70].

[241] See the definition of 'Company' in Part A, s 1.1.2. For detailed consideration, see Phil Anderson, *ISM Code: A Practical Guide to the Legal and Insurance Implications* (3rd edn, Informa Law from Routledge 2015); Kverndal (n 227).

[242] s 1.4.1-6

[243] s 4.

obliged to comply with the ISM Code, irrespective of its incorporation into national law.[244] An additional noteworthy aspect in this context is that any domestic law in a contracting country conflicting with and prevailing over the ISM Code would constitute a violation of the SOLAS Convention.[245]

Furthermore, despite its nature as a Code, which is typically non-binding, it was made mandatory by the 1994 amendments to the SOLAS Convention, introducing Chapter IX into the Convention.[246] At its initial adoption, the Code was merely recommendatory; however, its potential to enhance maritime safety and pollution prevention, coupled with the evident shortcomings of its voluntary predecessors, led to its transformation into a mandatory requirement.[247]

Chapter IX, reg 3 makes it mandatory for companies and ships to comply with the Code; companies 'shall comply'.[248] Additionally, this regulation explicitly states that the Code's requirements are to be treated as mandatory, and compliance with these requirements is to be evidenced by a document of compliance.[249] The Convention also stipulates that the SMS must be maintained according to its requirements and verified periodically to ensure proper functioning.[250]

The SMS serves as a framework that shipowners can use to achieve the objectives of the Code.[251] Sharing a similar feature to the ISPS Code, the ISM Code is flexible. It is described as enforcing self-regulation on the shipowner. In other words, instead of imposing measures on the shipowner, it allows the shipowner to develop and maintain its own SMS that takes into account the specific circumstances of the shipowner's company.[252] This is said to result in a more relevant and legitimate SMS, thus promoting a higher level of compliance.[253]

[244] Liang Chen, 'Legal and Practical Consequences of not Complying with the ISM Code' (2000) 27 Maritime Policy & Management 219, 220.

[245] Ibid, 221.

[246] See Foreword to the ISM Code.

[247] Antonio J Rodriguez and Mary Campbell Hubbard, 'International Safety Management (ISM) Code: A New Level of Uniformity' (1999) 73 Tul L Rev 1585, 1595.

[248] See reg 3.1.

[249] Reg 3.2 and reg 4.

[250] See regs 5 and 6.

[251] Rodriguez and Hubbard (n 247) 1593.

[252] See *Sea Glory Maritime Co v Al Sagr National Insurance Co (The M/V Nancy)* [2013] EWHC 2116 (Comm), [2014] 1 Lloyd's Rep 14, [192].

[253] Bjørn-Morten Batalden and Are Kristoffer Sydnes 'Maritime Safety and the ISM Code: A Study of Investigated Casualties and Incidents' (2014) 13 WMU J of Maritime Affairs 3, 5.

Shipowners found by their flag state's administrative organs to have complied with the requirements set out in the ISM Code are issued a Document of Compliance (DOC).[254] Ships belonging to such certified shipowners will, however, still undergo a separate onboard audit to confirm compliance with the ISM Code, and such ships will be issued a Safety Management Certificate.[255] The issuing administrative organ is required to verify both documents under Regulation reg 6 periodically.

Although the ISM Code solely applies to ships and their shipowners[256] and thus does not require ports to develop an SMS for addressing cybersecurity risks, Resolution MSC 428(98)[257] applies to ports and port facilities. This Resolution calls for an approved SMS that incorporates cyber risk management in line with the objectives and functional requirements of the ISM Code.[258] However, it is doubtful that this Resolution imports the mandatory nature of the Code. The Resolution itself is not binding, and it only refers to the objectives and functional requirements outlined in sections 1.2 and 1.4 of the ISM Code. It does not incorporate other vital provisions of the Code, such as the appointment of a designated person or the requirement to keep a document of compliance that certifies compliance with the Code.[259] These aspects of the Code contribute to its high effectiveness in managing safety, as it upholds a rigorous standard of ongoing compliance with the Code. It is submitted that this high standard of continued compliance in managing cybersecurity is essential for smart ports accommodating smart and autonomous ships.

6 Recommendations

An analysis of the requirements of both the ISPS Code and the ISM Code reveals that both instruments have the potential to provide an adequate framework for managing the grave cybersecurity risks anticipated in smart ports accommodating smart and autonomous ships. However, the issue with both instruments and the available guidelines addressing cybersecurity in ports is that they do not establish mandatory standards for ensuring the security and resilience of smart ports against cyber threats. The

[254] See reg 4.1.

[255] See reg 4.3.

[256] See reg 1.2, which defines 'Company' to include the shipowner or any organization or person such as the manager, or bareboat charterer. See also reg 2.

[257] On Maritime Cyber Risk Management in Safety Management Systems: above, text to n 174.

[258] See s 1.

[259] Reg 4.

current framework for dealing with cybersecurity risks within ports and port facilities fails to address the matter with the seriousness it deserves.

The severity of cybersecurity risks in ports arises from the interconnectedness of ports and ships. A cyber-attack at one port could affect numerous ships and subsequent ports, leading to delays and substantial financial loss.[260] Furthermore, the insurance market's scepticism towards cyber risks and the lack of adequate insurance products to cover these risks add to the issue's complexity.[261] This paper argues that there should be mandatory cybersecurity management in ports to address these challenges effectively.

The best approach to addressing the cybersecurity challenge in smart ports would be to create IMO standards that include the details of the various cybersecurity guidelines mentioned above and possessing the same qualities as the ISM Code. The choice of the ISM Code as a model for the proposed mandatory smart port cybersecurity standards is based on its interpretation and implementation. The first reason for this choice is the mandatory nature of the ISM Code. Secondly, the object and purpose of the ISM Code are to compel the responsible stakeholders to ensure adequate safety management of their operations. The third reason is that the Code's primary aim is to create an international standard for safety management, thereby fostering cohesion. Lastly, the court's interpretation and implementation of the ISM Code provide essential insights into fulfilling its object and purpose, as demonstrated in the case of *The Eurasian Dream.*[262]

In this case, a fire broke out on the deck of a pure car carrier. As a result of the fire, the vessel's cargo of new and second-hand vehicles was damaged or destroyed, and the vessel itself was rendered a constructive total loss.[263] The cargo interests claimed against the carriers, alleging unseaworthiness regarding its equipment, competency of master and crew, and adequacy of documentation supplied to

[260] G Weaver et al, 'Estimating Economic Losses from Cyber-Attacks on Shipping Ports: An Optimization-based Approach' (2022) 137 Transportation Research Part C 103423 <Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach - ScienceDirect> accessed 20 November 2023, 2.

[261] Ibid, 1; 6. See also Jonathon Saul and Carolyn Cohn, 'Insurance Gaps Leave Shipping Exposed to Growing Cyber Threats' (Reuters, 12 January 2017) <Insurance gaps leave shipping exposed to growing cyber threats | Reuters> accessed 18 November 2023.

[262] *Papera Traders Co Ltd v Hyundai Merchant Marine Co Ltd (The Eurasian Dream)* [2002] EWHC 118 (Comm), [2002] 1 Lloyd's Rep 719.

[263] Ibid, [1].

the vessel.[264] Although the defendants admitted to some aspects of the alleged unseaworthiness, they argued that it was common ground that the vessel was not required to comply with the ISM Code at the relevant time. Therefore, judging the vessel or its owners for failing to adhere to ISM standards regarding the vessel and its equipment was erroneous.[265]

The court found the vessel unseaworthy in various aspects related to the competency and efficiency of the master and the crew. The court made several findings, including:

- The master's lack of experience with the vessel, the type of vessel (a car carrier), and the company (Univan);
- The ignorance of the master and crew regarding the specific hazards of car carriers and the characteristics and equipment of the *Eurasian Dream*;
- The lack of knowledge about the particular fire risks of the vessel when in port, the need to supervise stevedores on car decks, and the fire hazards created by simultaneous and proximate refuelling and jump-starting operations on a car deck;
- Insufficient instruction to the crew to prevent simultaneous refuelling and jump-starting on the same vehicle or in the same area, and the master had not received such an instruction himself from his employers (Univan);
- Ignorance of the specific firefighting systems and inadequate training in firefighting for the master and crew;
- Inadequate fire drills and failure to fight the fire properly according to its source and size;
- The crew's failure to inform the master of the cause of the fire when taking steps to fight it and, the master himself making no effort to make enquiries; and
- Insufficient training on an advanced firefighting course for the master, the chief engineer, and the chief officer before the incident occurred.

The court's findings align with the requirements outlined in the ISM Code. Specifically, these requirements relate to the 'Master's responsibility' in s 5, 'Resources and Personnel' in s 6, and 'Emergency Preparedness' in s 8 of the ISM Code. Indeed, the judge applied or used the 'ISM test' when

[264] Ibid, [100]; [101]; [102]; [103].

[265] Ibid, [110].

determining whether the vessel was unseaworthy,[266] although acknowledging the vessel's lack of SMS certification at the relevant time and that it was not obligated to have this.[267] However, the court still used the standards of the ISM Code, thus giving it recognition as a generally accepted international standard. More significantly, this finding was made even before the Code became mandatory.[268]

The ISM Code has indeed impacted day-to-day legal practice because, unlike the ISPS Code, compliance with its procedures is often used as evidence in litigation.[269] Many certificates and documents required under the Code, as well as proof of communication with the designated person and between the designated person and the highest level of management in the company, are standard items for disclosure.[270]

Given the specific requirements of the ISM Code and its current implications in court matters, this paper concurs with the comment that its mission is to identify substandard ships, shipowners and managers. Furthermore, it suggests that 'one of the effects of enforcing the code is to prevent those sub-standard shipping companies or ships from having an unfavourable competitive edge in the market'.[271] This implies that the Code has the effect of subjecting all ships to a similar safety standard, which is what this paper argues for concerning cybersecurity in smart ports.

A mandatory Code, similar to the ISM Code specifically addressing cybersecurity in ports, could offer similar assistance to courts when determining whether a port was unsafe owing to poor cybersecurity management. This proposed Code would serve as an internationally accepted standard, irrespective of whether a particular port is located in a state that is not an IMO member and, therefore, not obliged to adhere to such a Code. Courts could utilise these international standards in assessing the facts surrounding the safety of the port and make determinations based on them. Implementing such a mandatory Code would create a uniform approach to evaluate the cybersecurity safety of smart ports accommodating smart and autonomous ships, regardless of location. Uniformity, specifically regarding

[266] 'An insight into the interpretation and implementation of the ISM Code' (Gard, Insight, 01 February 2003) <gard.no/web/updates/content/51603/an-insight-into-the-interpretation-and-implementation-of-the-ism-code> accessed 28 July 2023.

[267] *The Eurasian Dream* (n 262) [141].

[268] Filippo Lorenzon, 'Safety and Compliance' in Yvonne Baatz (ed), *Maritime Law* 5th edn (Informa Law, 2021) 377.

[269] Ibid, 378.

[270] Ibid.

[271] Chen (n 244) 222.

cybersecurity management in smart ports, is required. Absent it, the result is ‘a maze of differing and often conflicting laws’ from various nations, some of which may impose high standards while others are more relaxed.[272] It has already been argued that this method adopted by the ISPS Code is inefficient.

Support for this view can be observed in an opinion piece in *Lloyd’s List*, acknowledging the IMO’s work in publishing the various cyber security guidelines mentioned previously whilst simultaneously commenting on their insufficiency. It is argued that it is necessary for governments and regulatory bodies to formulate ‘a robust legal framework for cybersecurity and to ensure universal compliance with international standards’.[273]

In conclusion, while it is widely acknowledged that the automation of ships poses numerous challenges and risks, the significant investments made in research and development by private companies and governments indicate that the potential rewards of an automated voyage outweigh them. Smart ships and, eventually, fully autonomous ones will become commonplace in our oceans. Therefore, ports, as the intended safe havens for these ships, must be adequately equipped to accommodate them. The digitisation of ports is inevitable in this context due to its direct connection to crucial commercial considerations. Charterers are often contractually obligated to send their vessels only to safe ports, and courts have correctly interpreted this obligation strictly. Considering the changes and novel threats that may arise with using smart and autonomous ships, any failure in ports to accommodate them may result in the charterer bearing the risk of any damage to the vessel. Most importantly, the interconnectedness of maritime trade requires that all ports embark on digitising their ports and making the changes required to accommodate smart and autonomous ships safely.

The information necessary for charterers to make this crucial decision is widely available, except for cyber security risks, which are anticipated to increase with the widespread adoption of smart and autonomous ships and smart ports. The existing guidelines for cybersecurity within ports are deficient in that they do not establish mandatory minimum standards commensurate with the heightened risk connected with increased digitisation in ports. Therefore, this paper advocates developing a mandatory port cybersecurity code that establishes international standards that the courts can enforce.

[272] Rodriguez and Hubbard (n 247) 1586.

[273] ‘Cyber attacks: Downside of the Digital Revolution’ *Lloyd’s List* (London, 12 May 2023).