IN THE EYE OF A STORM
GOVERNANCE OF EMERGING TECHNOLOGIES IN UK PORTS POST BREXIT

Feja Lesniewska[1]*, Uchenna Ani[2], Madeline Carrr[3], Jeremey Watson[4]

[1]STEaPP, University College London, London, United Kingdom
[2] STEaPP, University College London, London, United Kingdom
[3] STEaPP, University College London, London, United Kingdom
[4] STEaPP, University College London, London, United Kingdom
**f.lesniewska@ucl.ac.uk*

Keywords: PORTS, INTERNET OF THINGS, BREXIT, SECURITY, GOVERNACE

Abstract

As the UK looks towards a future of changing relations with its trading partners, the need to reduce emissions from the maritime sector and the potential economic opportunities from new shipping routes in the Arctic region, it is faced with many decisions. As part of its strategic response the UK is looking to follow other countries, especially in the EU and Asia, in investing in smart ports. Smart ports can bring benefits locally, nationally and globally from reducing greenhouse gas emissions, improving air quality, efficient supply chains and safer working environments. Yet, embedding emerging technologies, like the Internet of Things into critical infrastructure like ports introduces new risks and vulnerabilities that existing governance mechanisms are often unable to address.

This paper firstly examines the growth in digitalisation of port drawing on initiatives in Rotterdam and Singapore. The new risks and vulnerabilities are discussed in the following section using several case studies before turning to review existing cybersecurity governance for ports. The final section focuses on the UK considering the lessons it can draw from the smart port leaders like Rotterdam and Singapore as it looks to implement the innovation and digitalisation element of its new Maritime Strategy.

1. Introduction

As the UK looks towards a future of changing relations with its trading partners, the need to reduce emissions from the maritime sector and the potential economic opportunities from new shipping routes in the Arctic region, it is faced with many decisions about where to invest, in what, and the consequence of those decisions. How to regulate a future sector that is increasingly dependent on a digital ICT infrastructure, is an overarching issue.

Port associations view this moment in the UK's maritime history as an opportunity. The UK Major Ports Group Chair Charles Hammond stated in November 2018 that:

"This is the time for ports. The current focus on Brexit and the UK's trade with the world has shone a light on ports and their importance to the U.K. And it's not just the current context. The ports sector is on the cusp of major technological change to radically transform the business models of major ports and many of our customers and supply chain partners. So, it's never been a more important or exciting time to be in the ports sector." [1]

A key part of the future is the role that innovation and technology will play. Smart ports that incorporate new and emerging technologies into their operational infrastructure are seen to be fundamental to the future of the maritime sector. Smart ports have been shown to reduce costs, improve the environment and increase the competitiveness of a port, region and the state. Leaders in developing smart ports include Rotterdam, Singapore and Antwerp. Vincent Campfens, Director of the Port of Rotterdam, observed that "*a targeted commitment to digital innovation … will allow us to take optimal advantage of new technologies presented by digitalisation: advanced robotics, artificial intelligence, blockchain transactions and hyper-precise data, to name a few.*" [2]. The potential of intelligently designed smart systems tailored to the needs of individual ports is only beginning to be understood.

The UK is already lagging behind in investments to digitise its critical port infrastructure compared to competitors in the EU and Asia, especially China and Singapore. A confluence of political, technical, environmental and economic factors is creating an unprecedented storm that the UK needs to advantageously address. There are many challenges to be faced, but one area that will require significant attention is smart port governance. Increased dependency on digital ICT systems, particularly those that have a significant number of

Internet of Things (IoT) sensors and actuators embedded within them, are at high risk of cybersecurity vulnerabilities.

This paper examines the security and regulatory challenges that the UK faces in transforming its critical port infrastructure. The focus of the paper is the increased inclusion into port operational systems of the Internet of IoT. In section 3, after initial background, the critical infrastructure aspect of ports is explained. Section 4 then considers the benefits available to smart ports, drawing on global two leaders: Rotterdam and Singapore. In section 5 the security risks and vulnerabilities in smart ports are considered using several examples to illustrate the problems port authorities and users have had to address. Section 6 then surveys the governance mechanisms in place for port security, and considers their effectiveness in limiting the risks for smart ports. The UK is the focus of section 7 with lessons from existing initiatives considered for the its smart port strategy and approach to governance post-Brexit, to ensure that risks and vulnerabilities are minimised. The paper concludes that the UK could gain from smart ports but it will need to invest not only in technological transformation but also in ensuring that effective governance mechanisms are in place so that the benefits are not lost.

2. Background

Britain is an island, a maritime nation with a long history of maritime trading. In 2018 Britain's maritime trade was £500 bn and employed around one million people. Ports are vital to this maritime economy. In the UK, the ports industry alone is estimated to have contributed approximately 22.6% to the maritime economy[3]. Ports' significance to the UK economy is set to become even greater and more crucial as the country leaves the European Union (EU).

Within the near future the UK will no longer be part of EU. Nearly 90% of EU external trade and 43% of internal trade occurs via maritime ports [4]. The EU has a maritime infrastructure and trade strategy dedicated to improving the region's internal market, environment and to reducing greenhouse gas (GHG) emissions. The region has prioritised strategic port development to secure trade-flow efficiencies and to improve competitiveness especially as international trade patterns shift with new opportunities in emerging markets.

For the UK to achieve increased competitiveness and efficiency in the maritime trade sector, as well as reduction in GHG emissions after leaving the EU, it will need to invest in its port infrastructure. The UK government's 2050 Maritime Strategy, launched in January 2019, identifies innovation and digitalisation as key to achieving economic, environmental and social goals. The government, maritime sector and other businesses need to mobilise quickly to learn lessons from existing smart port initiatives, especially regarding security, as they collaborate to develop a clear future plan.

3. Ports as critical infrastructure

Ports are part of a critical national infrastructure. They are essential for maintaining 'vital societal functions' as well as contributing to 'health, safety and economic well-being of people'. Ports support national and/or international transport and logistics, and business continuity. They also contribute to national economies by facilitating trade, tourism, job provisions, and the supplement of energy utilisation [5].

Ports are economic facilities, nodes within a global supply chain, and areas for economic and human activities, thus a critical infrastructure that contributes to a nation's success [6].

The European Council's definition of critical infrastructure (CI) as an 'asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a very substantial impact because of the failure to sustain those functions' only applies to ports of a certain size and economic significance for a country. [7] This is because the disruption or damage of critical ports with significant capacities can cause have severe impacts to individuals (injury or death), the environment (pollution and degradation) [8], society, and a nation's economy [9],[10]. The linkages and interdependencies of ports to other critical infrastructures like transport, energy, manufacturing, etc., also means that disruption in a port can directly/indirectly cause ripple effects on those sectors that depend on it.

4. The digital ICT transformation of ports

Digital innovation in ports can create a vital advantage over competitors, as well as contributing to a healthier environment. To achieve the benefits of digitalisation, information and communications technology (ICT) system are being adopted/integrated into ports [11], as they provide the functional and operational opportunities and capacities to facilitate improve planning, control, and management of intra- and inter-port operations [12]. This further enables a better processing and handover of cargo at the interfaces between sea-side, terminal and land-side operations, at the points of inter-linked processes, and the transfer of responsibility amongst designated actors. The high potential for lags and disturbances in port processes emphasises the need for technology innovations that not only expedite operations, but also support better measurement, monitoring and control. Hence ICT components and services, emerging trends such as internet-of-things (IoT) and supporting technologies, are finding their way into ports for the benefits they promise.

The IoT can provide a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communications technologies over the internet [13]. It aims to connect anything with anyone, anytime, and anywhere [14], [15]. The IoT is playing a significant role in the smart infrastructure revolution – from smart homes to smart cities and smart factories. It is not surprising then that the IoT is envisaged to have a key role in

driving the digital transformation of ports, and contribute to the move to what is termed 'hybrid ports' [16] or 'smart ports' [17].

Ports are being re-thought and redesigned concerning infrastructure, organisation, processes and information exchange to take advantage of IoT (sensor and actuators-driven) features. This aims to support the improved management of port infrastructures, to leverage available and new data sources, ensure active communications, and provide an information platform that supports real-time information exchange, coordination, and collaboration amongst actors [18]. Port traffic controllers, logistics network operators, terminal operators, road traffic controllers, and other port stakeholders can greatly benefit from IoT implementations. The possibilities are vast including: fully-automated ports, autonomous cranes for loading/unloading containers, autonomous vehicles for transporting containers, GPS tracking for cargo, assuring the provenance of goods, seamless communication with trucks, trains, and cars along the supply chain, real-time surveillance of ports, and reduced labour and operating costs [19]. IoT devices with embedded sensors can generate and disseminate information through designed communication structures to provide insights into processes that can inform better and intelligent decision-making, increase efficiency and productivity of actors, ensure a safe and sure operational environment, and enhance profitability by identifying new business opportunities [20].

Two ports have pioneered the ICT transformation: Rotterdam and Singapore. Each holds lessons for the UK as it begins to invest in its own digital ICT transformation of the port critical infrastructure.

4.1 Rotterdam

The port of Rotterdam is vigorously pursuing a digital transformation initiative. The port has for a decade, aimed to achieve 'smartness' by building and ensuring the organised and optimised handling of ships via transparent information-sharing. In 2009 Rotterdam led the *Portbase Initiative*, to build a Port Community System – digital linking to smart Dutch ports – combining an application layer, platform and information database to achieve mutual connections and information exchange and to reduce operational costs and handling time [21]. Currently, the port boasts of operating largely unmanned container terminals, autonomous fully electric guided vehicles (AGVs), and unmanned cranes remotely operated from a centralised control. Rotterdam's future plans include implementations of unmanned (autonomous) ships, a remote-controlled jetty, water quality and inspection, and quay inspection vehicles [22].

In early 2018, the port of Rotterdam in collaboration with IBM, announced a multi-year digitalisation initiative aimed at harnessing IoT and cloud management technologies to transform the port's operational environment and create the *'world's smartest port'* [23]. The IoT initiative was to effectively create a digital twin of the port of Rotterdam to replicate all its operations and conditions, including ship movements. The planned system was to leverage on a variety of available data from smart quay walls and sensor-fitted buoys to learn the status of berthing terminals, weather and water conditions. Such information could then be used to improve efficiency via real-time tracking of operations, running test scenarios, and predicting best possible docking times for ships based on the ship characteristics.

Earlier this year (2019), the port of Rotterdam in partnership with IBM, Cisco, Esri and Axians rolled out an IoT-enabled operational platform to support innovations in newer technologies, including edge computing, real-time analytics, artificial intelligence, hyper-precise data and blockchain [24]. The IoT platform involved the first of its kind hydro/meteo system comprising forty-four sensors that obtain port data relating to *"height of tide, tidal stream, salinity, wind speed, wind direction and visibility, many prediction models, data from Rijkswaterstaat and astronomical calculations"*. The IoT-driven innovation enables several capacities, including an ability to more precisely predict the best berthing and departure times for ships based on water conditions, while guaranteeing maximum loads. The platform is reported to be already processing up to 1.2 million data points that are accessible to systems and users, and is proving an essential decision tool for handling incoming ships. It is probably the first recorded instance where a generic IoT platform has been applied to mission-critical objectives to satisfy high safety and reliability shipping standards. Other benefits envisaged from applying the new system include: reduced waiting times, optimised berthing and faster loading times, which in turn can boost the efficiency and profitability of port operations [25].

4.2 Singapore

The port of Singapore is also among the first to embrace digital transformation. It is among global pace-setters in applying smart data to obtain operational insights and improve maritime and port operations. In September 2017 the Maritime and Port Authority of Singapore (MPA) in partnership with IBM commenced the roll out of seven smart data modules under the project *SAFER – 'Sense-making Analytics for maritime Event Recognition'*. The project aimed at automating and enhancing the accuracy of critical maritime tasks. The roll-out of SAFER smart modules commenced after the successful completion of pilot trials on three modules; automated movement detection, infringement analytics, and pilot boarding detection. The release of other modules is expected to follow. SAFER was expected to enable benefits for Singapore's maritime sector in next-generation port operations and monitoring of vessel movements [26]

The port of Singapore has not relented in its aspiration to attain *'smartest port'* status leveraged by technology [37]. A new port infrastructure called Tuas Port is being planned; this will be the largest automated container terminal globally. Work on Tuas Port began in 2016 and the first phase will be completed in December 2020. It will harness 'big data' and feature fully-automated systems for yard and quay cranes, which are already under trial at the Pasir Panjang port [27].

In early 2018, a proof-of-concept (PoC) trial exercise of blockchain-based cargo tracking and tracing was successfully

completed [38]. Built on the IBM blockchain platform, the trial explored real-time track and trace, transparent and reliable execution of multimodal logistics booking, regulatory-compliant execution of multimodal logistics booking processes, and participant permission access control [28]. The blockchain trial reflected Singapore port stakeholder collaboration in efforts to enhance physical and digital connectivity, as well as to improve efficiencies along the global supply chain.

A key port operator, PSA Singapore, has also demonstrated several technological innovations to be implemented in the future Tuas port facilities. Some of these include: robotic arms to simplify twist locks during the loading/unloading of containers, IoT-fitted amphibious and autonomous drone systems that can operate over land and water to inspect wharf side fenders, fulfil ship-shore and shore-ship deliveries, and support security surveillance for terminals. Other innovations include specialist data analytics for equipment (e.g crane maintenance), and motor-driven exo-skeletons that allow humans to handle tough and physically-demanding operations without fatigue. Other examples include Augmented Reality (AR) to facilitate visualisation/detection of defects for effective learning and timely repairs. There are also plans to develop new port systems that can harmonise interoperability among port equipment, and provide centralised automation control and remote diagnostics capacities [29].

Rotterdam and Singapore are the leaders in advancing smart ports systems using a portfolio of emerging technologies including the IoT, Blockchain and AI. Port authorities, governments and others in the maritime and supply chain logistics sectors world-wide, are looking to these two leaders to learn lessons for their own smart port developments. Cybersecurity is a main concern with increased dependency on digital ICTs in smart ports. The next section, drawing on several examples, outlines the nature of cybersecurity risks and vulnerabilities of smart ports.

5. Cybersecurity: new risks and vulnerabilities with smart ports

The benefits of ICT modernisation come with risks[30], [31]. Cybersecurity risks are a function of cyber threats, vulnerabilities and attack likelihoods. ICT with local and internet connectivity typically support the operations of critical infrastructure operations such as ports, and are becoming increasingly attractive to both internal and external malicious cyber actors and criminals that aim to sabotage or gain illegal economic advantage from the port cyber system. A successful mal-intervention, if not prevented or at least mitigated, can make the difference between the making and marring of global maritime trade benefits physically, socially, and economically.

These risk factors have become ever more present in modern ports due to the integration of ICT systems and the rise in connectivity [32]. In the port context, adopting new ICT features also introduces security risks (threats, vulnerabilities, and attack surfaces and likelihoods). The basic characteristics of ports – interdependencies, multiple entry points, handling huge volumes of cargo/passenger data, processing substantial volumes of transactions, high monetary values, involvement of many stakeholders, and non-transparent ownership of goods/equipment [33] – contribute to making ports more vulnerable to cyber-threats and attacks. Security risks are greater with the IoT due to an increased attack surface. Valuable lessons can be learnt about the nature of threats and vulnerabilities from real smart port cyber incidents.

The Port Antwerp incident of 2013 involved hackers using spear-phishing and malware attacks directed at port authority workers and shipping companies. The hackers were able to access the container shipping management system and change the location and delivery times of containers that had drugs. Smugglers then picked up drug-loaded containers before the arrival of the legitimate hauliers [34].

In 2017, the port of Los Angeles' largest terminal also fell victim to the global cyber-attack computers involving the 'Petya' ransomware (virus). The terminal operated by Danish shipping company A.P.Moller-Maersk was shut down for three days and huge volumes of data wiped out, which cost nearly $300 million in economic damage [19], [20]. A similar attack mode – using ransomware – was also used against the ports of London, Barcelona and San Diego in 2018 [21].

These incidents suggest that typical cyber-attack modes that target the maritime industry (especially port systems) include; malware (virus, ransomware), phishing, spear-phishing, application attacks, denial of service (DoS), brute force, network protocol attacks, man-in-the-middle, and credential thefts [22].

Cyber vulnerabilities in ports can emerge in various modes. Typically, vulnerabilities can be technical, organisational or systemic [35], [36], or more typically in line with socio-technical system constituent elements – *technology, people, and processes* [37], [38]. Technical vulnerabilities refer to security exposures in port hardware, software, and network infrastructures that can be exploited to cause disruptions and harm. Ports are characterised by dynamic ensembles of vendors and products, so that it is impracticable to provide an exhaustive list at any point in time. Technical vulnerabilities in port infrastructures can include; errors in technology configurations and implementations, unpatched systems; weak or a lack of user authentication, buffer overflows and uninitialized memory in OT components: weakly implemented encryption, poorly protected external connections (e.g. internet), insecure mobile and remote access, insecure back-end modems, wireless, sensor, and Bluetooth field communications devices, limited use of firewalls, rogue and BYO devices, weak intrusion detection systems (IDSs), firewall filtering deficiencies and insufficient (application-level) firewall support for control system communication protocols [39].

Organisational, process or systemic vulnerabilities can emerge in the form of non-compliance with port cybersecurity policies or the lack of them, poor segregation of duties amongst port personnel, poor or the lack of pre-employment screening,

authentication and authorization policies, violation of least privilege, poor patch and change management, physical access to port facilities (insufficiently controlled areas – cyber-physical issues), insufficient incident response planning and the simulation of emergency situations and responses [40]. Other potential influencers of systemic vulnerabilities in ports as critical infrastructures include: pressures on *'productivity'* (profit maximisation) – causing performance to be prioritised above safety and security, pressure from *'increased computer literacy'* – making it difficult to separate *'knowledge to create'* from *'knowledge to destroy'* in the case of insider threat actors, weak organisational structures characterised by wrong or unwise political and economic decision-making, lack of stakeholder interests, complacency, negligence, corruption, and the lack of cybersecurity awareness, education, and training [41], [42], [43]. These also reflect people-oriented vulnerabilities, especially the lack of basic security management knowledge and skills, which can influence fear, mis-judgements, misperceptions and errors in actions and inactions on the part of port personnel when incidents occur [44]. The location of ports is also a potential influence on security vulnerabilities – malicious cyber actors have been noted to target operators inside ports, where security consciousness and preparedness is often presumed low [45].

Minimising cybersecurity risks and vulnerabilities requires a robust, resilient and adaptable governance approach. Port governance has evolved slowly in light of security threats. The following section outlines the main governance measures and tools that apply to ports and critical infrastructure.

6. Governance and smart port cybersecurity

With digital transformation (especially IoT), cybersecurity is crucial because its absence or compromise in a port can potentially affect the port's operational efficiency, and ability to function safely. Port cybersecurity needs a coherent, resilient and enforceable governance approach. Essential objectives for a governance system include: *confidentiality* and *possession (of control)* for port access controls, *availability, safety* and *resilience* for port operational continuity, *integrity, utility* and *authenticit*y for port information quality and validity. [46].

Port-specific regulation has evolved slowly in comparison to the emergence of new digital ICT. There are broader concerns over the limitations of existing law and regulation to address cybersecurity threats across the entire maritime sector, not only in ports. It is frequently observed that the maritime sector is at least a decade behind similar transport and critical infrastructure sectors such as aviation and international finance. In the 2000s, legislative amendments and new acts have substantially increased the number of safety and security plans and safety management systems that are required by law, from merchant shipping ports, Requirements can be grouped according to themes (preparedness and security, transport, rescue schemes and occupational safety), which can serve as an architecture for structuring plans in the future.

Aviation attacks on the New York Twin Towers in 9/11 prompted an international response by sector specific organisations to improve security of critical infrastructure. The International Maritime Organisation (IMO) developed the International Ship and Port Facility Code (ISPS). The 2002 ISPS Code provides a standard global security framework to enable ports, shipping companies and governments to operate on equal preparedness and response levels. Under the ISPS Code, port facilities are required to have port facility security plans and port facility security officers. Plans related to security measures are drafted for all ports that serve international routes. A security assessment and a security plan form a whole, and the combined information can be used in both assessing and planning existing and remediated facilities. These documents are linked together by law. An emergency plan has been drafted for almost every port, but the practices for drawing up these plans vary between different ports.

The aim of the Code is to provide a standardised, consistent framework for evaluating risk, enabling Governments to counteract changes in threats with changes in vulnerability for ships and port facilities through determination of appropriate security levels and corresponding security measures. An example of current good practice is a security measures exercise organised by ports working closely together. The ISPS code provides that drills and exercises on port safety and security measures be organised every 18 months under the direction of cooperating authorities. The flexible nature of the Code makes it a useful foundation for a dynamic response to deal with emerging ICT threats and vulnerabilities. Key to preventing unnecessary breaches and incidents is the collaboration and knowledge exchange between port authorities and users of data. Singapore is in the process of initiating a maritime CERTs reporting system that could aid the updating of ISPS requirements.

The ISPS Code supplements Amendments to the International Convention for the Safety of Life at Sea (SOLAS) that were adopted in 2002. The SOLAS Convention in its successive forms is the most important of all international treaties concerning the safety of merchant ships. The first version was adopted in 1914, in response to the Titanic disaster, the second in 1929, the third in 1948, and the fourth in 1960. The 1974 Convention has been updated and amended on numerous occasions. Amendments to SOLAS include a new Chapter XI-2 on special measures to enhance maritime security.

In 2003 the IMO adopted a code of practice on security in ports in an effort to drive forward an integrated approach to port-related security, safety and health issues where security fits into existing health and safety guidance documents. This code of practice is intended to promote a common approach to port security amongst member States. This COP is intended to be compatible with the provisions of SOLAS, the ISPS Code and resolutions adopted by the 2002 SOLAS Conference. It extends the consideration of port security beyond the area of the port facility into the whole port.

Increasing concern over cyber-related security issues resulted in the IMO in 2017 producing the Guidelines on Maritime Cyber Risk Management to improve cybersecurity practice in

the sector. However, this applies largely to cybersecurity for on-board vessels systems rather than ports.

Meanwhile, to improve the security of critical infrastructure the European Union (EU) member states have adapted existing policies and regulations as digital technologies have evolved. In the EU member countries, the ISPS code is implemented through the EU regulation on enhancing ship and port facility security (725/2004). The ISPS code has two parts, one mandatory (Part A) and one recommendatory (Part B). The EU regulation makes some of Part B of the ISPS Code mandatory. On exit from the EU the UK will initially continue to follow the mandatory approach to Part B.

There are several main regulatory frameworks that apply to aspects of IoT security. These include the following;

- European Critical Infrastructure (ECI) Protection Directive was adopted in 2008 for energy and transport.

- European Networks and Information Systems (NIS) Directive adopted on the 6 July 2016 specifies legal standards for digital service providers and operators of essential services in critical sectors such as energy, water management, transport, banking and financial market infrastructures.

Currently, there are eighty-nine ECIs designated, primarily in the energy sector, under the 2008 Directive. Reforms are aiming to expand the ECI to include ICT sectors in the list of Europe's critical infrastructure. This should broaden the scope of the Directive to cover IoT related technologies. The 2016 NIS Directive tackles cybersecurity risks by involving Operators of Essential Services (OES) and Digital Service Providers. Ports that handle certain volumes of trade and/or goods of importance to with national security such as energy are classified as OES.

One further development in Europe is the formation of a specialised agency to look into how cyber risks can best be dealt with. The NIS Directive established the European Union Agency for Network and Information Security (ENISA) as the Cybersecurity Agency of the EU. ENISA is behind helping to design a voluntary cybersecurity certification scheme, aimed at harmonising the procedures and instruments for testing and showing conformity with a responsible level of cybersecurity. In 2017, it produced Baseline Security Recommendations for the Internet of Things in the context of critical information infrastructures to inform the governance by both public and private operators in the EU.

Within the European Union further governance measures to improve the security of ports has been developed. However, there are variations between member states in the implementation of Directives related to ports. In some countries, port security is provided by a combination of military and police forces whereas in others it is provided by private enterprises. This ad-hoc deployment of security may hinder industry-wide appreciation, standardisation and handling of port security matters. Without a Pan-European Federal Agency like the US Department of Homeland Security, the European Union has no power to compel member states to work together or to follow prescriptive guidelines.

In an effort to create a unified data standard system the EU has been active through various initiatives, including the Sea Traffic Management (STM) Validation Project to improve the full maritime transport chain by making real-time data available to all. STM links to an IMO initiative on e-Navigation to build the Port Collaborative Decision Making (PortCDM) concept. PortCDM addresses the need to ensure the continuous flow of data about intentions, outcomes, and possible disruptions related to movements and service provision among all those involved in the berth- to-berth maritime transport process so as to gain a high degree of predictability in the planning and execution of all associated operations and activities. The International PortCDM Council has been established, providing guidelines for the global governance of PortCDM, implemented at regional and local levels. It was validated in 13 European ports in early 2018. Convergence around the data management system could, like the ISPS Code, prove to be a foundation for developing a flexible governance infrastructure that can help to deal with the increased cybersecurity threats that smart ports will face**.**

7. UK ports, digitalisation and governance

Although the UK has not been left out in the trend towards port digitalisation initiatives it is behind leaders like Rotterdam and Singapore. This could be about to change. In January 2019 the UK Shipping Minister, Nusrat Ghani in the preface to the UK 2050 Maritime Strategy wrote that 'emerging technology will help the UK's maritime sector evolve to be more efficient, safer and greener' (UK Maritime strategy).

UK ports have started exploring new technologies that build smart characteristics. A new programme that targets the piloting of smart port digital initiatives has been launched in the UK's Northeastern ports. The programme aims to increase trade and to promote economic growth. It is the foremost initiative of the Situational Awareness Information National Technology Service (SAINTS) launched by the North East Satellite Applications Centre of Excellence in collaboration with private industries to explore satellite and Earth-based sensor data to solve key business, government and community problems [40]. Key solution outcomes targeted include; new business opportunities and hinterland collaborations, improving the growth of green energy and low carbon solutions; improving customer experiences, operational excellence and security in and around the port [41].

The UK may have inadvertently entered the smart port game at the right time. The nature of cybersecurity threats, vulnerabilities and impacts that come with adopting new technologies like IoT in ports can be quite uncertain, so it can make sense to learn from the frontrunners, and strategise ways to guarantee safer, more secure and resilient smart port operations. For example, a common security risk associated with the use of satellite-based communications involves high-powered jammers. These can disrupt port-ship

communications and alter navigation and global positioning for ships. Malicious software (viruses) can also be introduced into port control management systems to disrupt or cripple operations. Holding back from investing until better system-wide knowledge has been established can result in more informed and better decision making as to how to design a smart port system that is safe and secure, possibly saving money.

In terms of governance for smart ports in the UK the mechanisms and tools in place to secure port security at the international level will continue to apply to the UK post-Brexit. The UK law based on EU Directives will also remain in place for a period of time. The UK government can draw on other critical infrastructure and cybersecurity regulatory developments, including for the IoT, in the form of standards, codes and laws and incorporate these into requirements for port security plans. As the UK develops its smart port infrastructure it can grasp the opportunity to be a world leader in the governance of smart ports and cybersecurity.

8. Conclusions and recommendations

The UK is at a point of significant political, economic and social change. Whatever the outcome of the Brexit negotiations, maritime trade will remain central to the well-being and security of the country. Ports are a fundamental physical component of the UK trading infrastructure. Smart ports will be essential for the UK to expand its trading capacity efficiently and sustainably so it can remain competitive in a changing world.

With the investment in smart ports the UK will also need to invest into smart governance. It needs to minimise cyber-risks and vulnerabilities to its critical port infrastructure that will result from an increased dependency on digital ICT, especially the IoT. Existing international regulations, codes and guidance for security at ports is currently not sufficiently robust to address the nature and number of risks and vulnerabilities implicit in smart ports. However, the available modelling and design tools means they are flexible and relatively easily adapted to incorporate more stringent and appropriate requirements to be fit for purpose for integrated digital systems including the IoT.

The UK needs to ensure that as smart ports are developed, the relevant supporting agencies are involved from cybersecurity, national infrastructure security, environment and standards bodies. By working collaboratively from the outset, the relevant agencies can ensure that ports meet cybersecurity standards so that national security and the welfare of UK citizens is not compromised. The UK can become a world leader in the smart governance of smart ports. In the eye of this particular storm there is great opportunity, it must be taken if the UK is to prosper in the future.

Acknowledgements

This research was funded by the Engineering and Physical Sciences Research Council (EPSRC) funded PETRAS project.

6 References

[1] H. Sok, “Five-Point Plan Implemented for UK Port Success” November 24th, 2018, Global Trade Magazine [Online]. Available http://www.globaltrademag.com/global-logistics/ocean-ports/five-point-plan-implemented-for-uk-port-success?utm_campaign=shareaholic&utm_medium=twitter&utm_source=socialnetwork [Accessed: 28-Feb-2019].

[2] Rotterdam and Maersk Partner for Port Call Optimization, Port Technology, 25 February 2019 [Online] Available https://www.porttechnology.org/news/rotterdam_and_maersk_partner_for_port_call_optimization [Accessed 28 February 2019]

[3] Cebr, “The economic contribution of the UK Marine industry: A report for Maritime UK,” London, UK, 2017.

[4] A. Chiappetta, “Hybrid ports: the role of IoT and Cyber Security in the next decade,” J. Sustain. Dev. Transp. Logist., vol. 2, no. 2, pp. 47–56, 2017.A. Chiappetta, “Hybrid ports: the role of IoT and Cyber Security in the next decade,” J. Sustain. Dev. Transp. Logist., vol. 2, no. 2, pp. 47–56, 2017.

[5] N. O. Bakir, “A Brief Analysis Of Threats And Vulnerabilities In The Maritime Domain,” 2007.

[6] N. Anand and A. Grainger, “The port as a critical piece of national infrastructure,” Saf. Reliab., vol. 37, no. 2–3, pp. 106–127, 2018.

[7] The Council of the European Union, “Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,” Off. J. Eur. Union, pp. 75–82, 2008.

[8] N. Polemi, Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains. Amsterdam, Netherlands: Elsevier Inc., 2018.

[9] N. O. Bakir, “A Brief Analysis Of Threats And Vulnerabilities In The Maritime Domain,” 2007.

[10] K. Tam, K. D. Jones, and M. Papadaki, “Threats and Impacts in Maritime Cyber Security,” Eng. Technol. Ref., vol. 1, no. 5pp, pp. 1–13, 2016.

[11] L. Heilig and S. Voß, “Information systems in seaports: a categorization and overview,” Inf. Technol. Manag., vol. 18, no. 3, pp. 179–201, 2017.

[12] L. Heilig, E. Lalla-Ruiz, and S. Voß, “Digital transformation in maritime ports: analysis and a game theoretic framework,” NETNOMICS Econ. Res. Electron. Netw., vol. 18, no. 2–3, pp. 227–254, 2017.

[13] C. Zavazava, “ITU Work on Internet of Things,” no. March. International Centre for Theoretical Physics (ICTP), Trieste, Italy, 2015.

[14] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” Elsevier Science Direct, 2018

[15] M. Jardas, Č. Dundović, M. Gulić, and K. Ivanić, “The Role of Internet of Things on the Development of Ports as a Holder in the Supply Chain,” J. Marit. Transp. Sci., vol. 54, no. 1, pp. 61–73, 2019.

[16] A. Chiappetta, “Hybrid ports: the role of IoT and Cyber Security in the next decade,” J. Sustain. Dev. Transp. Logist., vol. 2, no. 2, pp. 47–56, 2017.

[17] L. Heilig, E. Lalla-Ruiz, and S. Voß, “Digital transformation in maritime ports: analysis and a game theoretic framework,” NETNOMICS Econ. Res. Electron. Netw., vol. 18, no. 2–3, pp. 227–254, 2017.

[18] L. Heilig, E. Lalla-Ruiz, and S. Voß, “Digital transformation in maritime ports: analysis and a game theoretic framework,” NETNOMICS Econ. Res. Electron. Netw., vol. 18, no. 2–3, pp. 227–254, 2017.

[19] M. Jardas, Č. Dundović, M. Gulić, and K. Ivanić, “The Role of Internet of Things on the Development of Ports as a Holder in the Supply Chain,” J. Marit. Transp. Sci., vol. 54, no. 1, pp. 61–73, 2019.

[20] M. Jardas, Č. Dundović, M. Gulić, and K. Ivanić, “The Role of Internet of Things on the Development of Ports as a Holder in the Supply Chain,” J. Marit. Transp. Sci., vol. 54, no. 1, pp. 61–73, 2019.

[21] S. Berns, R. Dickson, I. Vonck, and J. Dragt, “Smart Ports Point of View,” Netherlands, 2017.

[22] E. Rademaker, “Change of an Era: Becoming a Smart Port.” Port of Rotterdam, pp. 1–16, 2017.

[23] M. Murison, “Rotterdam and IBM plan to create ‘world’s smartest port’ with IoT,” Internet of Business News Portal, London, UK, 31-Jan-2018.

[24] Port of Rotterdam, “Port of Rotterdam puts Internet of Things platform into operation,” Port of Rotterdam News Portal. Port of Rotterdam Authority, Rotterdam, Netherlands, Jan-2019.

[25] Port of Rotterdam, “Port of Rotterdam puts Internet of Things platform into operation,” Port of Rotterdam News Portal. Port of Rotterdam Authority, Rotterdam, Netherlands, Jan-2019.

[26] T. H. Hwee, “Singapore to roll out smart data to improve maritime, port operations,” The Business Times, Singapore, 22-Aug-2017.

[27] PSA Singapore, “Future Terminals: Tuas Port,” PSA Singapore Website, 2018. [Online]. Available: https://www.singaporepsa.com/our-business/terminals/future-terminals. [Accessed: 19-Feb-2019].

[28] Maritime Information Services Ltd, “Successful Blockchain Trial Concludes in Singapore,” Port Technology Online Newsletter, London, UK, Feb-2018.

IMO, “Guidelines on Maritime Cyber Risk Management,” vol. 44, no. 0. International Maritime Organisation (IMO), London, UK, pp. 1–6, 2017.

[29] Maritime Information Services Ltd, “PSA to Unveil Drones, Robotics and Futuristic Port Tech,” Port Technology Online Newsletter, 2018. [Online]. Available: https://www.porttechnology.org/news/psa_to_unveil_drones_robotics_and_futuristic_port_tech. [Accessed: 19-Feb-2019].

[30] C. Orwat, C. Büscher, and O. Raabe, “Governance of Critical Infrastructures , Systemic Risks , and Dependable Software.” Karlsrube, pp. 1–25, 2010.

[31] H. Carrapico and A. Barrinha, “The EU as a Coherent (Cyber)Security Actor?,” J. Common Mark. Stud., vol. 55, no. 6, pp. 1254–1272, 2017.

[32] S. Lagouvardou, “Maritime Cyber Security: concepts, problems and models,” Kongens Lyngby, Copenhagen, 2018.

[33] L. Jensen, “Challenges in Maritime Cyber-Resilience,” Technol. Innov. Manag. Rev., vol. 5, no. 4, pp. 35–39, 2015.

[34] J. Leyden, “Drug gang hacks into Belgian seaport, cops seize TONNE of smack,” The Register, London, UK, 18-Jun-2013.

[35] T. Hellström, “Critical infrastructure and systemic vulnerability: Towards a planning framework,” Saf. Sci., vol. 45, no. 3, pp. 415–430, 2007.

[36] IMO, “Guidelines on Maritime Cyber Risk Management,” vol. 44, no. 0. International Maritime Organisation (IMO), London, UK, pp. 1–6, 2017.

[37] U. D. Ani, N. Daniel, F. Oladipo, and S. E. Adewumi, “Securing industrial control system environments: the missing piece,” J. Cyber Secur. Technol., Oct. 2018.

[38] U. P. D. Ani, H. (Mary) He, and A. Tiwari, “Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective,” J. Cyber Secur. Technol., Jan. 2017.

[39] U. D. Ani, N. Daniel, F. Oladipo, and S. E. Adewumi, “Securing industrial control system environments: the missing piece,” J. Cyber Secur. Technol., Oct. 2018.

[40] U. D. Ani, N. Daniel, F. Oladipo, and S. E. Adewumi, “Securing industrial control system environments: the missing piece,” J. Cyber Secur. Technol., Oct. 2018