2018-09-02

Effective maritime cybersecurity regulation the case for a cyber code

Hopcraft, R

10.1080/19480881.2018.1519056
Journal of the Indian Ocean Region
Informa UK Limited

Routledge
Taylor & Francis Group

Journal of the Indian Ocean Region

ISSN: 1948-0881 (Print) 1948-108X (Online) Journal homepage: https://www.tandfonline.com/loi/rior20

Effective maritime cybersecurity regulation – the case for a cyber code

Rory Hopcraft & Keith M. Martin

To cite this article: Rory Hopcraft & Keith M. Martin (2018) Effective maritime cybersecurity regulation – the case for a cyber code, Journal of the Indian Ocean Region, 14:3, 354-366, DOI: 10.1080/19480881.2018.1519056

To link to this article: https://doi.org/10.1080/19480881.2018.1519056

JOURNAL OF THE INDIAN OCEAN REGION
2018, VOL. 14, NO. 3, 354–366
https://doi.org/10.1080/19480881.2018.1519056

Routledge
Taylor & Francis Group

RESEARCH NOTE

Effective maritime cybersecurity regulation – the case for a cyber code

Rory Hopcraft and Keith M. Martin

Information Security Group, Royal Holloway, University of London, Egham, UK

ABSTRACT

Ships and ports are increasingly connected to each other through cyberspace. This connectivity streamlines many aspects of maritime business, but also exposes maritime operators and administrations to new types of risk including hacking and outage. The maritime industry has been slow to realize the implications of this new environment within which it operates, and now lags behind other industries (like aviation) when it comes to cyber risk mitigation and regulation. We argue that the International Maritime Organisation (IMO), alongside its members, urgently needs to create robust and resilient cybersecurity regulations. We suggest that the IMO should consider creating a standalone Cyber Code, based on a framework created by previous IMO Codes such as the Polar Code. Since the IMO uses Codes as a legally binding instrument, this would help to ensure the continued safety and efficiency of the maritime industry in the face of threats from cyberspace.

KEYWORDS

Maritime cybersecurity; International Maritime Organisation; cybersecurity regulation; maritime industry; port security; risk management

Background

Over the last decade, the world maritime industry has amplified its reliance on cyber-enabled technology (IMO, 2017a). This technology has been used to increase both the safety and productivity of maritime activities, including the remote monitoring of vessels. However, this technology has simultaneously opened up the maritime industry to new risks from cyberspace in its efforts to safeguard vessels and cargoes. These risks range from unintentional human errors to ensuring software and data integrity to planned state-level attacks. This situation is exacerbated by integrated information technology and the intensification in communication between ships and land-based entities, which opens up many more methods in which a ship at sea could be exposed to a threat from the cyber-realm.

Within the maritime sector, the adoption of cyber-enabled technology has occurred incrementally over time, so the industry has been relatively slow to implement effective risk mitigation and appreciate the extent to which ships and ports need to be kept up-to-date in dealing with cyberspace (Latarche, 2018). The International Maritime Organization (IMO), the specialized United Nations (UN) body charged with facilitating cooperation to achieve the practicable standards of maritime security and regulate

CONTACT Rory Hopcraft Rory.Hopcraft.2014@live.rhul.ac.uk Royal Holloway, University of London, Egham, UK

shipping, has also been late and somewhat inactive in considering regulation when it comes to a number of cybersecurity standards.

While full digitalization of ships and related systems is a global risk-management issue, it is of high significance to the Indo-Pacific region, which incorporates the third largest of the world's oceans and acts as the gateway to many of the major shipping lanes, straits and canals, including the Suez Canal. At the same time, the Indo-Pacific region experienced the rise of a number of non-traditional security threats including piracy between 2008 and 2013 (IMO, 2017b). This spike was attributed to an increase in the financial value of cargoes transiting the area, being led by strong demands for imports of crude oil to both India and China, and the export of petroleum products (UNCTAD, 2017). So while maritime security does remain a high priority in a variety of ways, the expanded nature of security threats no longer entails only physical attacks by pirates and other criminal groups on the water itself. Security decisions must also deal with the digitization in the maritime industry that involves attacks on cyber-enabled ships by cybercriminals and a growing myriad of hostile state and non-state actors.

A cumulative body of literature has documented how maritime systems are vulnerable to an ever-growing range of cyber threats that can cause considerable damage (BIMCO, 2017; IET, 2016; TRANSAS, 2016). Malicious attacks on maritime systems have come about through many points of vulnerability due to not taking necessary steps for cyber security mitigation and preparedness, including poor access control to communications systems and manipulation of employees (social engineering). The consequences of these types of issues have been varied, including extortion, the loss or compromise of business sensitive information and the opportunistic criminal disruption of chart navigation systems (Kelion, 2018). Yet with both ports and vessels moving towards systems of automation and connectivity, the security of a modern-day vessels will need to ensure significant security improvements to address ongoing issues like ransomware attacks and cyber-sabotage. Such security concerns need to be assessed within the reality of globally accessible navigation systems and the fact that the operation of modern technology-dependent vessels are configured in ways that can invite these types of cyber-incidents.

In short, multiple systems may be connected together. It is therefore imperative that the maritime industry, through the IMO, creates actionable, robust and resilient cybersecurity regulations that reflect this technological revolution. New regulations and guidelines are vital to progress towards a less vulnerable infrastructure as well as allowing the maritime industry space to improve efficiency and decrease costs, without heedlessly comprising the safety and security of the seafarer. At the very least, navigation and associated digital communication will continue to indispensably buttress the maritime sector, improving the technology that supports activities such as international shipping, cruising, leisure boating and marine scientific exploration

This research paper will outline some of the central challenges in the development of robust maritime cybersecurity regulations. It will argue that there is a need to embed an appropriate risk management regime via capacity-building and the advance and championing of global cyber-security standards. We will also address how a collaborative approach by the maritime industry can help to bring about a sense of renewed urgency to ensure more formal process in establishing a self-reinforcing Cyber Code with respect to maritime cyber-security.

The maritime cybersecurity challenge

Discussing and implementing a broad-based cybersecurity strategy is a demanding task in any fast-moving, multi-cultural and multi-lingual environment. There are several core issues that make cybersecurity issues for the maritime industry especially complicated.

First is the linkage between on-board and terrestrial systems. The IMO is a 'competent international organization' according to the United Nations Convention on the Law of the Sea (UNCLOS) (UN, 1982), meaning they are charged with the adoption of international shipping rules and standards in matters concerning maritime safety and efficiency (IMO, 2014a). UNCLOS is explicitly targeted at the world's oceans and seas, which places obligations on and gives responsibilities to coastal and non-coastal states. However, much of the infrastructure that enable communication is land-based, outside of the IMO's direct jurisdiction. This land-sea infrastructure interdependence is only set to strengthen over the coming decade, either through the building of remotely monitored or fully autonomous unmanned ships without human intervention on-board.

Second, there are many different classes of vessel, all of which operate in dissimilar environments. These vessels tend to have different computer systems built into them. These systems will vary greatly depending on their class, use, and working environment. And each vessel class, as defined by the Classification Societies, has specific requirements for on-board systems. Notably, vessels are frequently designed with an operational life expectancy of over 25 years (IMO, 2005, p. 57) and a vessel may be re-purposed several times during its lifetime. So it is not uncommon for vessels to contain shipboard computer networks and systems that are badly out-dated and that are predisposed to cyber-attacks (Jones, Tam, & Papadaki, 2016).

A third complexity is that many ships habitually carry specialist equipment which was not designed with cybersecurity in mind. Some of the aging operational technology found on vessels have been demonstrated to be inherently unreliable and insecure, such as the maritime navigational aids GPS and ECDIS, (Kelion, 2018; University of Texas at Austin, 2013). This is despite being mandated by the IMO and designed in accordance with international standards. To complicate matters, there are many different equipment providers, meaning each vendor can implement security protections in their own particular way, making the harmonizing of equipment requirements with existing cybersecurity standards adopted by other sectors problematic. Moreover, some systems need to be publicly accessible, for example, if they are required for identifying and locating a vessel in distress and that is threatened by serious and/or imminent danger.

Finally, a wide range of third-party service providers are employed by maritime operators in order to maintain and update a vessel's operational systems. Contractor visits occur when a vessel is in port, which limits the time for conducting the necessary work required to take appropriate action to protect key assets. It is perfectly possible that a ship's crew have little understanding of how on-board systems interact with each other. This might comprise of back-up and restore systems that are necessary for shipping operations or services if impaired. Frequently changing crew patterns also increase the chance that installed systems are operated by individuals who are unfamiliar with them, increasing the risk of user error and poor real-time management of security breaches and incidents. These risk operation problems will be exacerbated when the vessel is at high sea

and the only immediate support available is via limited and low-speed bandwidth connections (ESC Global Security, 2015).

A community based approach to regulation building

Given both the increasing sophistication of global cyber-attacks and the enhanced digitization in shipping, the issue of maritime cybersecurity regulation requires urgent attention. One part of this process involves the establishment of appropriate conventions and workable principles. As such, it is vital that the process of establishing robust and resilient maritime cybersecurity regulations is done through international collaboration, and in a manner that respects both regional needs and mutual economic dependencies. These regulations must also address interdependencies and relationships between systems at a data or information level

The impact of a threat to security to act as a catalyst to the creation and implementation of a regulatory security architecture is not a new concept within the maritime space. Glück (2015) suggests that threats like piracy have acted as a vehicle for the accelerated production of transnational collectives to improve maritime security relations and subsequently have led to the creation of security communities (Bueger, 2015). Based on an assessment of the risk, these communities share knowledge and develop a common understanding of problems and opportunities through socialization. These convergent communities can then support shared practices and habits that aim to promote positive-sum and profitable elements, such as reducing logistics costs and 'frictionless' shipping that removes the need for a customs border (while still suppressing undesirable, often counter-productive or illegal, activity).

Both the EU and UN are examples of international security communities that have come to share common norms of behavior and acted to and institutionalize new platforms for mutual engagement, based on, for instance, law-bound standards of police and government conduct. So too is NATO, for instance, whose Operation Ocean Shield in 2009 was mandated – in full accordance with the relevant UN Security Council Resolutions – to contribute to international efforts to counter maritime piracy and to support efforts like joint surveillance with regional governments (NATO, 2016). Such capacity building missions included the building of training centers as well as developing relationships between the defence and commercial sector. Overall, collaborating through supranational organizations does allow for drafting of shared strategy documents that, over time, can support specific mandates to strengthen international and regional security initiatives.

Furthermore, security concerns on land can act as a precondition for a more systematic approach incorporating wider maritime security issues (Remuss, 2010). International support can be given to help coastal states think about how to best support safe and secure shipping and set up their navies and coastguards that are tailored to specific maritime needs.

While not a stand-alone solution to the maritime security threats, the IMO can act as a platform for the international maritime community to monitor compliance and mitigate cyber risks. All IMO regulatory discussions are conducted through its membership which has a vast range of expertise and proficiencies. The Djibouti Code of Conduct is one example of how the IMO, through collaborative work has helped in the fight against piracy in the Indian Ocean. It was signed in 2009 and then later revised in 2017. Involving

more than 20 states, alongside with regional stakeholders, the Code provides an example of how the IMO used its expertise and power to initiate the establishment of multi-agency, multidisciplinary maritime security partnerships. This institutional framework, where possible, coordinates military and civilian resources to avoid duplication and strengthens trans-regional coordination such as facilitating the operational coordination of regional navies.

Cyber-security however, cannot be approached through a limited regional oceanic network of like-minded actors. Due to the unique nature and scope of maritime systems and digital infrastructure, the impacts and detrimental flow-on effects of an attack are not limited to just one region or domain. The far-reaching impacts of the cyber-attack on A.P. Moller-Maersk in 2017, highlights the importance of international collaborative approaches to addressing cybersecurity threats. This attack started on an office terminal in Ukraine, spread through the company's global network, and eventually impacted international port terminals including those in India (Saul, 2017).

Nonetheless, regional stakeholders are still important to regulatory discussions, as they are more acutely aware of the immediate geopolitical, environmental, resource and related issues for a particular region. The Indian Ocean is one of the major conduits for Middle Eastern oil transport, and therefore its shipping lanes are predominantly used by tankers, which carry their own specific risks. Also, as was seen by the worldwide implications of a 2017 ransomware attack – WannaCry through the Windows XP operating system – there are some states who lack the capability to easily implement updated technical mitigation processes (AFP, 2017). Problematically, this lack of capacity will inhibit their ability to co-ordinate with non-government stakeholders and met stringent regulatory compliance.

So maritime cybersecurity is an inter-dependent global challenge, tackled by a comprehensive strategic framework of international collaboration, feedback, coordination and communication in order to achieve common or complementary risk analysis. The creation of a stronger shared understanding of both the risks and impacts of a cyber-attack will allow the formation of a cross-sectoral security community, focused on cybersecurity and associated threats to operation-critical, technology platforms such as navigation systems. It is through standardization and certification that all relevant regional and international stakeholders will be able to better assist with incident management as well as acting to ensure the development of adaptable regulation, which is then monitored and evaluated by all within the sector.

The role of codes in the IMO

The IMO uses a mixture of conventions and codes to enforce regulation and best practices to ensure safe and efficient shipping. The IMO's main legal basis is given by the Safety of Life at Sea Convention (SOLAS) (IMO, 2014c), which is legally binding to any vessel within certain parameters. By appending regulations to SOLAS, the IMO can adapt and modernize its requirements as technology develops. Any amendments to these conventions continue to be legally binding under Article 26 of the Vienna Convention on the Law of Treaties (1969) (UN, 1980).

Codes within the IMO are normally viewed as guidelines unless they are mandated under a precise convention. Codes create standalone guidance and regulation that is specific to one certain aspect of the maritime industry. For example, the International

Code for Ships Operating in Polar Waters (Polar Code), which outlines regulation that applies only to vessels operating in polar waters, has mandatory sections that are enforceable under both SOLAS and maritime pollution conventions.

By using Codes, the IMO can highlight long-term and specific risks that are unique to a process or environment that the code pertains too. It creates an unambiguous reference to how the overarching conventions still apply, regardless of the uniqueness of a process or environment. The Polar Code outlines the requirements on safety equipment, such as life jackets and ice axes, that are distinctive to the operational environment and that are required to ensure continued compliance with SOLAS. In other words, as well as reiterating requirements, Codes allow additional requirements, above and beyond the basic requirements of compliance to be added to the overarching convention. The Polar Code outlines stringent hull specifications that vessels wishing to be classified as 'Icebreakers' require. Such a classification applies to ships constructed of steel and intended for independent navigation in ice-infested polar waters. This then allows the IMO to restrict the scope of aspects of compliance, to specific practices and process when required.

The use of Codes also allows for the harmonization of the different and discrete rules that regulate shipping. Again, taking the Polar Code, it creates a consistent regulatory framework that incorporates parts of both IMO frameworks and those of the Arctic Council (Bai, 2015). This allows other administrations' requirements, local authority law and expertise all to be incorporated into wider IMO regulations and standards. Such a uniform approach ensures there is no unfair advantage given to ships under certain administrations (Schröder-Hinrichs & Hebbar, 2006).

Additionally, this harmonization occurs between the various councils that form the IMO. It allows each council to use their technical expertise to develop holistic regulations through a better decision-making process. Through the use of working groups, each council will consider regulation and guidance that ensure the reduction of the risks present in relevant specific environments, such as in known regions of high piracy. These recommendations are then collated under the IMO parent committee, normally the Maritime Safety Committee, to develop a single code that includes all the recommendations.

Codes allow a wide and varied IMO membership (via its member states, various think tanks, shipping associations and Non-Governmental Organizations) to share their expertise and experiences to the decision-making process. This collaboration is aided by Shipping Associations who work on behalf of smaller bodies that do not have their own seats within IMO discussions. This means that the smaller parties, that are the practitioners within the maritime community, can have a sense of ownership among all actors as their interests feed into an equally-beneficial governance process. This allows the decision-making process to consider not only the broader industry risks, but also the more nuanced risks that only a specific section of the industry might face. Codes thus facilitate information sharing, promote engagement within the maritime community, encourage greater awareness among public stakeholders, and ensure a better co-ordinated decision making process to support relevant cross-sector maritime regulation.

The case for a cyber code

There is no one regulation or standard for maritime systems and cyber security. And as discussed earlier, maritime cybersecurity poses a unique set challenges for regulators to

consider. The establishment of a Cyber Code is needed to speed up the development of cyber security standards and support effective and holistic maritime cyber risk management.

Overcoming system complexities

Vessel and port systems are complex and differ vessel to vessel, therefore it is vital that the IMO draw together all the relevant security assurance regulations. This ensures that operators are aware that even when cyber is not explicitly mentioned, it might still be relevant to a specific regulation.

A Code would allow the harmonization of these numerous regulations into one succinct benchmark document, which is easier to monitor and enforce. In general terms, cybersecurity management encompasses a wide variety of regulations already in place, including navigational aids, operating systems and ballast water systems. A standalone Cyber Code would allow the IMO to draw attention to these systems, which are universal across vessels, and ensure the operators and crew are fully aware of existing vulnerabilities and the wider consequences of a cyber-incident.

A Code would also facilitate harmonization between a number of existing best practice cybersecurity standards that are relevant to, but not explicitly targeted at, the maritime sector, like the internationally-adopted US National Institute of Standards and Technology (NIST) framework (NIST, 2018), which aims to standardize practices to ensure uniform protection of cyber assets. As these existing standards already have international acceptance, compliance should meet less resistance from the IMO membership. Moreover, a single Cyber Code document makes it easier to update regulations, since the IMO would be able to more readily review and modernize regulations as new technology or processes are introduced. Such a process was evident by the 2018 'e-waste' amendments to the Maritime Pollution Convention, which has acted to ensure the correct disposal of maritime electrical equipment (IMO, 2018b).

Enabling enforcement

The creation of a Cyber Code would increase the ability to enforce cybersecurity regulation from within the maritime industry itself. The Code would highlight the authority of authorized members to carry out inspections to ensure the continued compliance with these regulations. A vessel in breach of these regulations could be detained.

Enforcement authorities within the maritime industry, such as Flag Administrations and Classification Societies, would be party to discussions about establishment of a Cyber Code. This would provide the necessary leverage to develop a cohesive enforcement structure. The Code would serve to create a framework for states to use entering regulations into national law and in ensuring the consistency of these across the international community and relevant third party stakeholders.

In 2017, the IMO amended two of their general security management codes to explicitly include cybersecurity. The International Ship and Port Facility Security Code (ISPS) and International Security Management Code (ISM) detail how port and ship operators should conduct risk management processes. Making cybersecurity an integral part of these processes should ensure that operators are at least conscious of cyber-risks.

Hopefully, the above developments could initiate a more holistic approach to maritime cybersecurity regulation. The knowledge gained from these new cyber-risk assessments may enable the IMO to develop a broader set of cybersecurity regulations. Readily attainable is, for example, the harmonizing of some equipment requirements with existing cybersecurity standards adopted by other sectors.

The inclusion of cyber risk management into both the ISM and ISPS security assessments will allow administrations to have the enforcement capabilities required to ensure compliance, and thus increase the security of maritime cyberspace. As part of a Cyber Code these requirements are not left as standalone assessments, but would form part of a wider assessment and mitigation process that includes compliance with other standards and regulations, thus ensuring that all systems have a basic level of security. There also seems to be a lack of urgency to get the house in order. It is also worth noting that the cyber-specific amendments to the ISM and ISPS do not come into force until January 1 2021 and they only represent starting point to move towards a more holistic approach to maritime cybersecurity regulation.

Overcoming sovereign resistance

A Cyber Code would, like the IMO's other Codes, have mandatory and voluntary components. The mandatory section would include regulation that ensures the continued safety and productivity of modern shipping. It would do this by drawing together the expertise and combining this input with other existing regulations and standards. This would ensure that the relevant parts of these other regulations are applicable to cyber risk and are brought to the attention of stakeholders.

Many of the IMO regulations do not specify cyber-security principles but are broad enough to be considered within them. This is similar to other sectors, for example by the application of a modern understanding of cyber-security to traditional definitions of broadcasting in the United Nations Convention of the Law of the Sea (UNCLOS) by the Tallinn Manual 2.0 (NATO, 2017). In providing advice regarding the international law of cyber operations,

> … .understanding the points about which application and interpretation are subject to disparate views allows States to focus their efforts where clarification of the law is needed and in their national interest. Such clarification will help deter other States from exploiting these grey zones in the law of cyberspace (Schmitt, 2017).

Given a major obstacle is that maritime surveillance is strongly linked with national sovereignty, the voluntary section of the Code would allow the IMO to build in recommendations that states could enact into national law. This combination of mandatory and voluntary elements would allow minimum standards to be set by the mandatory section, with additional security supplemented through the voluntary section. This voluntary section permits states to implement additional security in ways that they see fit, but which might be seen as too prescriptive in other legal jurisdictions. By including these regulation as voluntary, with no obligation to implement, states with reservations can still agree to the Code, allowing it to enter into force.

As discussed previously, maritime cyberspace is closely connected to terrestrial infrastructure, which falls under the individual sovereignty of states. Within IMO discussions,

issues that are seen to infringe on state sovereignty, like submarine cabling, are often met with resistance and outright rejection of the suggested regulation. Therefore, creating a Cyber Code which is goal-based, a concept the IMO has utilized since the early 2000s, could help overcome some of this resistance. This is because goal-based standards do not specify a means of achieving compliance, but rather set flexible goals permitting alternative ways to achieve compliance (Hoppe, 2005). This would allow sovereign states the freedom to implement practices that fit in with their national guidance, as long as the overall goal is met, and are included in operational security assessments, to be assessed by the Flag Administration This would involve controlling checking all the security navigation documentation and having direct control on the compliance of foreign-registered vessels calling at domestic ports.

The establishment process of a cyber code

The IMO has currently made little progress in the creation of cybersecurity regulation, as there has been only ad hoc attention paid to it within major policy discussions. In 2014, the IMO opened a cybersecurity discussion at a supranational level, by engaging not only with its member states but also the broad spectrum of consultative Non-Governmental Organizations within its membership regarding cybersecurity regulations and policies (IMO, 2014b). Yet the resulting cybersecurity guidelines, which act as a precursor for regulation, addressed only a broad set of non-maritime specific cyber risks.

Before a specific set of cybersecurity regulations, or dedicated Cyber Code, can be formed more work is required to understand the cybersecurity risks faced by the maritime industry. From previous experience, the IMO has a timeline for the establishment of a Code. But is still a way to go before the sustainable creation of a Cyber Code occurs. Significantly, it is often a specific newsworthy event, or disaster, which acts as a catalyst for discussion and change within the IMO. It is through these discussions that the experience and expertise present within the IMO's membership help create a Code.

One such event was the sinking of the Titanic in 1912. The tragic loss of life was a catalyst for the international maritime community to create a holistic set of regulations to ensure the safety of life of both seafarers and passengers at sea. The discussion led to the International Convention for the Safety of Life at Sea (SOLAS), which has become one of the single most significant conventions within the IMO relating to life saving appliances and arrangements. The Deepwater Horizon explosion in 2010 – the largest marine oil spill in history – also led to the instigation of numerous amendments to IMO regulations relating to oil spills because existing regulations had applied to tankers and not drilling platforms (Smith, 2011).

Yet it would seem unlikely that an incident on the scale of the Titanic or Deepwater Horizon is likely to arise from cyber threats to the maritime industry. The significant attack on A.P. Moller-Maersk's land-based systems in 2017 did not involve loss of life and operations were restored within one week, although they suffered a $300 million loss in the relevant financial quarter (Novet, 2017). Therefore, a better example for the establishment of a Cyber code would be the sinking of the Polar passenger ship 'The Explorer' in 2007. The sinking did not result in a catastrophic loss of life, however, the reaction of the maritime community, through the IMO, was the creation of the Polar Code (Basarn, 2015). Again, this

addressed the unique challenge of strengthening existing conventions in a way where compliance was only required by those who operated within that specific environment.

The process of a code creation

The blueprint for the establishment of a Code provided by the Polar Code does suggest a three-phase process. Firstly, a threat or danger is formulated. Following this is a 'negotiation' phase, which allows the IMO membership to come to a consensus regarding the threats, the impacts and the subsequent management of that threat. The final stage is the ratification of the Code, which embodies the agreement by IMO committees to the regulations built from its members' comments and opinions.

For cybersecurity, the formulation of the risk came in 2014, when the IMO engaged with their membership to raise awareness of common cyber vulnerabilities on board existing ships. This put cybersecurity on the Maritime Safety Committee's agenda, which can be seen as the first step towards establishment of a Cyber Code. This has occurred without an obvious referent object or disaster that has commonly been the catalyst for regulatory discussions

The second phase, the negotiation stage, started with the production of the IMOs *Interim Guidelines on Maritime Cyber Risk Management* (IMO, 2016). Like the Circulars which acted as the pre-curser to the Polar Code, it only contains recommendations, with no binding and uniform acceptance (Bai, 2015). However, these allow all parties to be able to influence the decision-making process ahead of ratification of regulation into a formal Code. Yet more work is required to appreciate the growing cybersecurity risks faced by the maritime industry before negotiations can continue.

As mentioned, in 2017, the IMO had highlighted the relevance of both the ISM Code (IMO, 2018a) and the ISPS Code (IMO, 2012) within this negotiation phase. By including cyber risk assessments as an integral part of the security certificate of compliance for both port facilities and vessels, all operators are made aware of the risks that their systems and processes represent, and are required to communicate this back to the IMO.

This process goes beyond a general understanding of the systems and possible threats and must indirectly include mitigation measures contained in security plans. The IMO does not suggest specific and definitive methods for mitigating cyber risk, but rather suggests that organizations become more aware of the inherent vulnerabilities that their systems and practices have, and design their own appropriate mitigation practices. This process ensures that there is collaboration with all parties and practices that are in some way invested with day-to-day maritime cyber-security, leading to a better-informed negotiation phase.

For the third and final stage of the ratification of a Cyber Code to occur, there must be a baseline agreement on the basic structure and content at a legal and technical level. This basis for this would not need to be created from scratch, but rather, by utilizing Article 30 of the Vienna Convention on the Law of Treaties (UN, 1980). So it would be formed from other previous, legally binding conventions. This subsequent governance basis would be supplemented by the additional outputs and decisions identified in the negotiation phase and then eventually ratified by the IMO Assembly. It should be noted that before any convention does come into force – that is, before it becomes binding upon governments which have ratified it – it has to be accepted formally by individual governments.

Overall, the bulk of the cyber-specific regulations that would be included in a Cyber Code are directly formed from the initial information gained through ISM and ISPS assessments. It can be argued that the voluntary incorporation of these assessments will form a much better stimulant for development of a Code rather than being reactive and knee-jerk. Instead, such an assessment process will allow the industry to utilize the strength of its collective participants to develop comprehensive regulation based from best practice and not be reliant on intentions based from past experiences.

There is no inevitability that a Cyber Code will be created from this process. However, as this research note has outlined, it would be the logical and productive step. Currently, there does seem a trend from the maritime industry not to want a Cyber Code, but this may come from the lack of appropriate risk management regime across shipping organizations. With an increased clarity about applicable risk boundaries and the threats to systems or services posed by digitization and integration, the industry might tap into new opportunities to drive an international standard. This standard, in the form of a Cyber Code, would then act to ensure a uniform and parallel approach is adopted while increasing the cost and consequences of non-compliance.

Conclusion

The maritime industry is undoubtedly behind other transportation sectors, such as aerospace, in cybersecurity terms. The co-operative establishment of a holistic Cyber Code by the maritime community would allow the development of robust maritime cybersecurity regulations. These would equip the sector with the capability and adaptability to address whatever future cyber security challenges arise.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

The research of Hopcraft was supported by the EPSRC as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London [EP/P009301/1].

Notes on Contributors

Rory Hopcraft is a Ph.D. student from the Centre of Doctoral Training in Cyber Security within the Information Security Group at Royal Holloway University of London. Prior to starting his Ph.D., he attained his M.Sc. in Geopolitics and Security from Royal Holloway. Rory is co-supervised by both the Information Security Group and the Geography departments. Rory's current research focuses on the regulatory aspects of maritime cybersecurity.

Professor Keith M. Martin B.Sc. (Glasgow), Ph.D. (London), CMath FIMA, is Professor of Information Security. He received his B.Sc. (Hons) in Mathematics from the University of Glasgow in 1988 and a Ph.D. from Royal Holloway in 1991. Between 1992 and 1996 he held a Research Fellowship at the University of Adelaide, investigating mathematical modeling of cryptographic key distribution problems. In 1996 he joined the COSIC research group of the Katholieke Universiteit Leuven in Belgium, working on security for third generation mobile communications. Keith rejoined Royal Holloway in January 2000, became a Professor in Information Security in 2007 and was Director of the

Information Security Group between 2010 and 2015. Keith's research interests include cryptographic applications and geopolitical aspects of cyber security. He is the author of Everyday cryptography by Oxford University Press. In addition to conventional teaching, Keith is a designer and module leader on Royal Holloway's distance learning M.Sc. Information Security program, and regularly presents to industrial audiences and schools.

ORCID

Rory Hopcraft http://orcid.org/0000-0003-1962-6903

References

APT. (2017, May 14). Manhunt for hackers behind global cyberattack. *Seychelles News Agency* [online]. Retrieved from http://www.seychellesnewsagency.com/articles/7262/Manhunt+for + hackers +behind+global+cyberattack

Bai, J. (2015). The IMO polar code: Emerging rules of Arctic shipping governance. *The International Journal of Marine and Coastal Law*, *30*(4), 674–699. doi:10.1163/15718085-12341376

Basarn, I. (2015). *IMO-polar code: History, content, and shortcomings*. Arctic Summer College 2015 Contributions [online]. Retrieved from https://arcticsummercollege.org/sites/default/files/ASC%20Paper_Basaran_Ilker.pdf

BIMCO. (2017). *The guidelines on cyber security onboard ships* [online]. Retrieved from http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

Bueger, C. (2015). What is maritime security? *Marine Policy*, *53*, 159–164. doi:10.1016/j.marpol.2014.12.005

ESC Global Security. (2015). *Maritime cyber security white paper – safeguarding data through increased awareness* [online]. Retrieved from http://www.escgs.com/files/WP_ESC_Safeguarding%20data%20through%20increased%20awareness.PDF

Glück, Z. (2015). Piracy and the production of security space. *Environment and Planning D: Society and Space*, *33*(4), 642–659. doi:10.1068%2Fd14245p

Hoppe, H. (2005). Goal-based standards – a new approach to the international regulation of ship construction. *WMU Journal of Maritime Affairs*, *4*(2), 169–180. [online]. doi:10.1007/BF03195072

Institute of Engineering and Technology. (2016). *Code of practice – cyber security for ports and port systems* [online]. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546160/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

International Maritime Organisation. (2005). *Report of the maritime safety committee on its eightieth session*. MSC 80/24 [online]. Retrieved from https://docs.imo.org/Shared/Download.aspx?did=31865

International Maritime Organisation. (2012). *ISPS code - guide to maritime security and the ISPS code*. London: IMO Publishing.

International Maritime Organisation. (2014a). *Implications of the United Nations convention on the law of the sea for the International Maritime Organization*. LEG/MISC.8 [online]. Retrieved from http://www.imo.org/en/OurWork/Legal/Documents/LEG%20MISC%208.pdf

International Maritime Organisation. (2014b). *Measures toward enhancing maritime cyber security*. MSC 94/4/1 [online]. Retrieved from https://docs.imo.org/Search.aspx?keywords=MSC%2094%2F4%2F1

International Maritime Organisation. (2014c). *SOLAS - safety of life at sea*. London: IMO Publishing.

International Maritime Organisation. (2016). *Interim guidelines on maritime cyber risk management*. MSC.1/Circ.1526 [online]. Retrieved from http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC.1-CIRC.1526%20(E).pdf

International Maritime Organisation. (2017a). *Guidelines on maritime cyber risk management*. MSC-FAL/Circ.3 [online]. Retrieved from http://www.imo.org/en/OurWork/Security/Guide_to_

Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf
International Maritime Organisation. (2017b). *Reports on acts of piracy and armed robbery against ships*. Circ.245 Annex 4 [online]. Retrieved from http://www.imo.org/en/OurWork/Security/PiracyArmedRobbery/Reports/Documents/245%20Annual%202016.pdf
International Maritime Organisation. (2018a). *ISM code - international safety management code*. London: IMO Publishing.
International Maritime Organisation. (2018b). *MARPOL amendments enter into force*. IMO Press Briefing [online]. Retrieved from http://www.imo.org/en/mediacentre/pressbriefings/pages/04marpolamendments.aspx
Jones, K. D., Tam, K., Papadaki, M. (2016). Threats and impacts in maritime cyber security. *Engineering & Technology Reference*, *1*(1). doi:10.1049/etr.2015.0123
Kelion, L. (2018, June 7). *Ship hack 'risks chaos in English Channel*. The BBC [online]. Retrieved from https://www.bbc.co.uk/news/technology-44397872
Latarche, M. (2018, June 6). *Shpping lags behind in new tech adoption, but change is inevitable Posidonia 2018 experts agree*. Shipinsight.com [online]. Retrieved from https://shipinsight.com/articles/shipping-lags-behind-in-new-tech-adoption-but-change-is-inevitable-posidonia-2018-experts-agree
National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* [online]. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
NATO. (2016). *Operation OCEAN SHIELD*. Operations Archive, Allied Maritime Command, Northwood UK [online]. Retrieved from https://mc.nato.int/missions/operation-ocean-shield.aspx
NATO. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press.
Novet, J. (2017, August 16). *Shipping company Maersk says June cyberattack could cost it up to $300 million*. CNBC [online]. Retrieved from https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html
Remuss, N. (2010). Space & maritime security – strategies for countering pirates. *Space Policy*, *26*(2), 124–125. doi:10.1016/j.spacepol.2010.02.013
Saul, J. (2017, June 29). Global shipping feels fallout from maersk cyber attack. *Reuters* [online]. Retrieved from https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19K2LE
Schmitt, M. (2017). Tallinn manual 2.0 on the international law of cyber operations: What it is and isn't. *Just Security* [online]. Retrieved from https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/
Schröder-Hinrichs, J., & Hebbar, A. (2006). International standard setting through the IMO. *Baltic Master Issue Brief*. World Maritime University [online]. Retrieved from https://www.researchgate.net/publication/237258882_International_Standard_Setting_through_the_IMO
Smith, M. (2011). The deepwater horizon disaster: An examination of the spill's impact on the gap in international regulation of oil pollution from fixed platforms. *Emory International Law Review*, *25*, 1477–1516. Retrieved from http://law.emory.edu/eilr/_documents/volumes/25/3/comments/smith.pdf
TRANSAS. (2016). *Connected ships and cybersecurity*. Frank J Coles CEO [online]. Retrieved from https://docs.wixstatic.com/ugd/9491c8_5fbc6ff941df40f8a5b90d703de4a64b.pdf
United Nations. (1980). *Vienna convention on the law of treaties*. General Assembly [online]. Retrieved from https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf
United Nations. (1982). *Convention on the law of the sea*. General Assembly [online]. Retrieved from http://www.un.org/depts/los/convention_agreements/texts/unclos/closindx.htm
United Nations Conference on Trade and Development. (2017). *Review of maritime transport 2017* [online]. Retrieved from http://unctad.org/en/PublicationsLibrary/rmt2017_en.pdf
University of Texas at Austin. (2013). *UT Austin researchers spoof superyacht at sea* [online]. Retrieved from http://www.engr.utexas.edu/features/superyacht-gps-spoofing