2019-04-10

The Importance of Information Sharing in the Creation and Enforcement of Maritime Cybersecurity Regulation

Hopcraft, Rory

The Importance of Information Sharing in the Creation and Enforcement of Maritime Cybersecurity Regulation

Rory Hopcraft
PhD Researcher
Information Security Group
Royal Holloway, University of London

Biography
Rory Hopcraft is a PhD researcher in the EPSRC-funded Centre for Doctoral Training in Cyber Security at Royal Holloway University of London [EP/P009301/1]. Prior to starting his PhD, he attained an M.Sc. in Geopolitics and Security, also from Royal Holloway. Rory is an interdisciplinary researcher and his PhD is co-supervised between the Information Security Group and the Geography Department. Rory's current research focuses on the regulatory aspects of maritime cybersecurity. Recent publications feature in the Journal of the Indian Ocean Region, and the Royal Institution of Naval Architects.

Abstract
The international community's response to Somalian piracy, shows how the maritime sector relies upon its community to share information about the threats it faces. The ratification of the Djibouti Code of Conduct, by the IMO, provides both training and information sharing centres to the East coast of Africa. NATO, through Operation Ocean Shield, provides a military platform to share information about the security of the region. These examples exemplify the importance of information sharing as a way to effectively manage risks in the maritime sector. This paper argues that for effective and enforceable maritime cybersecurity regulation to be created and implemented, a similar communal response is needed. The threats from cyberspace are a genuine concern for all stakeholders. Hence, if the international community comes together through the sharing of crucial information about the threats, targets, and mitigation practices, it could allow the creation of effective cybersecurity regulation. Regulation, created through the co-production of knowledge, could overcome the challenges that current practices and regulation cannot. The paper highlights the key challenges that maritime cybersecurity regulation must overcome, and argues it must utilise the knowledge base contained within the maritime community to do this. This knowledge must include input from the local, regional and international levels, suggesting the importance of both the public and the private sector in maritime cybersecurity discussions. Finally, the paper stresses the importance that this international community, and its information-sharing capabilities, will have on the enforcement of regulation, assisting in the continued safety and security of all users of the maritime space.

Introduction
Over the last two decades, the maritime industry has become dependent upon technology for the continued operation of everyday activities. This dependency on increasingly connected technology is expected to grow as the industry moves towards autonomous vessels. However, unlike many industries, the maritime has been slow to address the increased risks to which they are exposed through cyber-enabled technology.

In 2014 the International Maritime Organisation (IMO) received the first proposals from its members to create guidelines for maritime cybersecurity (IMO, 2014). In 2016, after much discussion within the IMO, the Interim Guidelines of Maritime Cyber Risk Management were circulated to all IMO members (IMO, 2016). Then, in 2017 the IMO affirmed that an

approved safety management system should take into account cyber risk management (IMO, 2017). By incorporating cyber risk management into a ship's safety certificate process, the IMO have allowed the international community to develop an understanding of what cyber risks it faces and feed this back into the regulatory process.

This paper highlights the importance of community and information sharing in the creation and enforcement of maritime cybersecurity regulation. The paper will suggest that to secure maritime cyberspace it requires a communal response. Firstly, the paper will look at what the maritime community is, and how it deals with international threats, like piracy. Secondly, the paper will address some of the key cybersecurity challenges that require cooperation by the international community to overcome. Finally, the paper will explore how, through collaboration within the IMO, the community will create robust and resilient cybersecurity guidelines and regulation.

The Importance of the Maritime Community

The maritime industry is sometimes described as the hidden industry because while it is responsible for 90% of the world's trade, it often goes unnoticed. However, regardless of the fact that the maritime industry is an international undertaking there is an important trichotomy between the international, regional and local, which is highlighted by the IMO's diverse membership, as discussed below.

The International Maritime Organisation

The IMO's membership includes 174 states. In addition, the IMO also includes 81 Non-Governmental Organisations and 64 Inter-Governmental Organisations, many of whom, represent the interests of the wider maritime community e.g. the different shipping associations. To commemorate their 70th birthday, in 2018, the IMO released a new logo for its World Maritime Day. Citing "Our Heritage", the new logo highlights the importance of a shared genealogy and a collective memory, as wells as a continued spirit of cooperation from its members. This also points to the notion that the IMO sees the international stakeholders that make up its membership as a community that is striving together towards "better shipping for a better future".

IMO 70th Anniversary World Maritime Day Logo

There are three reasons why the collaboration of the international community is essential to the IMO. The first is that the IMO is the primary regulator in the maritime domain. It therefore requires the input from the maritime community to ensure its guidance and regulation are effective. Secondly, as the IMO lacks enforcement capabilities, it relies upon the maritime community to enforce its regulation. This enforcement happens through the enactment of IMO regulation into national law, through the classification societies or the insurance companies, all of whom form part of the IMO membership. Thirdly, there is a diverse range of uses for the maritime domain including, fishing, cruise ships, tankers and offshore platforms. Therefore, the IMO requires representatives from those wide-ranging industries to understand the key challenges that they are facing.

Furthermore, by the IMO engaging with the wider maritime community, it acts as a conduit for information and expertise to be shared. By sharing information on common threats, it allows the international community to develop uniform mitigation processes that are mutually beneficial to the whole community.

The use of working groups, by the IMO, highlights how the expertise within its membership is fed back into the international community. The working groups are setup during meetings to discuss the finer technical details of guidance and regulation. Furthermore, members are actively encouraged by the IMO to bring technical experts within their delegations, specifically to attend these working groups.

This therefore means, that through the IMO the international community of states, technical experts, practitioners and academia can create and share knowledge about threats to the maritime space. This knowledge has a direct impact upon the regulatory process and on any implemented guidance and regulation. It is important that this knowledge is developed with an understanding of the threats, and capabilities, of all stakeholders within the community.

Piracy - Dealing with an International Threat

While the IMO plays an integral part of information sharing within the maritime community, it is only one example of how information is shared by the international community. The maritime community has often mobilised its communal spirit, creating collectives outside of the IMO, as a way to suppress undesirable, often counter-productive, or illegal activity. Glück (2015) suggests that threats, like piracy, have acted as a vehicle for the international community to work collectively to reduce the threat of undesirable activities.

Considering the increased transnationalism, driven by globalisation, of the maritime industry, these undesirable activities impact upon more stakeholders across the globe. As these stakeholders all share a common understanding of the threat, and require mitigation processes, it leads to collectives called security communities being formed (Bueger, 2015).

These security communities form a temporary sub-section of the wider maritime community and are made up of policy-makers, industry representatives, academia, law enforcement and sometimes the military. The individuals within these security communities then share their expertise with other members, providing the knowledge that decision makers lack. This allows the community to respond to threats in a manner that represents the concerns of international, regional, or local stakeholders.

The way in which the international community tackled the global piracy problem highlights how these security communities are formed, and utilise their shared beliefs and practices as a way to reduce a threat. Between 2008-2013 there was a sharp rise in the number of piratical attacks in the world's oceans, particularly off the East African Coast. This rise led to a response from a variety of these security communities.

The IMO, through the use of the Djibouti Code of Conduct, gained the signatures of more than 20 states alongside regional stakeholders, to tackle piracy in the region. Through this collaboration, the international community can now provide training, and information, to local states who then combine their enforcement capacities to better target piracy in the region. These regional security communities allow local stakeholders to target resources and information, from the international community, in a way that suits the operational environment of that region. Without this regional expertise, the international community would not have been able to apply their capacity in such a beneficial way.

Another example of an anti-piracy security community in the Indo-Pacific region focused is the North Atlantic Treaty Organization's (NATO) Operation Shield, in 2009. The Operation, fully mandated by the UN Security Council, provided support and information to regional stakeholders, to mitigate the threat of piracy in the region. NATO also provided naval capacity to the international community, by providing escorts for commercial vessels through

the region, and actively pursuing and arresting suspected pirates (NATO, 2016). By working with both local, regional and international stakeholders, NATO helped to ensure the safety and security of vessels, and their crews, without causing disruption in the region.

The use of global governance and the development of regional and local capacity allowed the reduction of piracy in the Indo-Pacific region. The Oceans Beyond Piracy Report (2014) highlighted the importance that the international community plays in maritime threat reduction. However, the report suggests that this input needs to be evaluated for effectiveness and resources redirected, through the local and regional communities. By redirecting resources in this way, it would ensure the development of local capabilities, while reducing the need for suppression capabilities by the international community.

These security communities, whether they are a collective of local states, or international navies, all value the information sharing that occurs within the broader maritime community. This information sharing works in both directions, between the local and international communities. By gaining local information and expertise, it assists naval operations, ensuring that they are targeted and appropriate within the region. Whilst sharing operationally sensitive information is challenging, military collectives like NATO highlight the importance of sharing information about threats in the maritime domain with regional and local stakeholders.

Drawbacks of the maritime community

While the diversity of the maritime community helps to bring knowledge and expertise into the policy-making process, it does have some drawbacks. Firstly, there is contention over the motivations of members of the community, which impact the way a threat is discussed and mitigated by the international community. InfluenceMap (2017) highlighted the significant control that commercial actors have over environmental pollution policy discussions at the IMO. By being present as both state delegates and industry representatives, commercial actors are able to steer the IMO away from stricter emissions regulations, as these are not in the commercial interest.

Secondly, the IMO operates on a consensus basis, with all states having an equal say and one vote each. This means that all guidance and regulation is heavily debated, and the final output is the lowest agreeable terms of all members. This limits the IMOs ability to regulate contentious issues, especially those that impact sovereign territory, as the community does not support international intervention within these areas.

Thirdly, because of the meeting structure of the IMO, there are limited opportunities for issues to be discussed by the international community. Therefore, it is often large newsworthy events that dominate the IMO's agenda, as the international community must be seen to be addressing these prevalent issues. This issue has been seen over the last few years where marine plastics and unsafe mixed migration have pushed cybersecurity off the agenda.

These three factors mean that there is a general unwillingness of the international community to change the IMO's procedures. If change must occur, it requires a long, drawn-out process, which, if desired by the community, can be slowed even further. It is therefore both a blessing and a curse to have a large community involved in the regulatory process. By sharing expertise and experience it offers the international community the ability to create regulation that is more representative. However, it comes at a price, as it allows members of the community to barter that knowledge for their own individual gains.

Key Cybersecurity Challenges

The increased dependence upon cyber-enabled technology with everyday practices has led to several key challenges. The international community, through the use of security communities, like the IMO, must overcome these challenges to ensure successful maritime cybersecurity

regulation can be created and enforced. The maritime community can no longer see itself as isolated from the outside world as it once did, and must work collaboratively with industry to overcome these challenges.

Littoral Expansion

The integration of technology into everyday maritime practices has seen an increase in both ship-based technology, and the land-based infrastructure to support it. Due to the interconnectivity between ship and shore-based systems there is a need to expand the maritime operating environment to beyond the standard littoral boundary (Fitton et al., 2015).

Traditionally maritime operations, especially those in a naval context, considered the maritime domain to only extend partly inland along the coast. However, due to this expansion of technology, there are other, traditionally terrestrial areas, that need to be considered within the maritime domain. Let us briefly consider INMARSAT, one of the largest satellite communications companies with maritime interests. A successful cyber-incident on their central London based headquarters could have a direct impact on the Global Maritime Distress Signal Service (GMDSS), and consequently on the safety of lives at sea. This therefore suggests that these terrestrial spaces, because of their ability to impact upon the maritime, need to be considered within the maritime operational domain.

The same littoral expansion can be witnessed in the composition of the engineering teams responsible for the support, operation, and maintenance of modern maritime systems. These teams, no longer solely based onboard a vessel, utilise expertise from vendors and third-party service providers, to ensure maritime systems are up to date, creating a 'virtual team' of service personnel (Berner et al., 2018). Again, the actions of these service teams, based outside the traditional maritime domain, can have a direct impact upon it.

Limitations of UNCLOS

This littoral expansion is a challenge that requires the international community to cooperate in order to overcome, as these terrestrial areas are excluded under existing maritime legal frameworks. The United Nations Convention on the Law of the Sea (UNCLOS) delineates the world's oceans and grants sovereign rights to coastal states within 12 nautical miles of the agreed baselines. This effectively excludes any terrestrially based infrastructure or systems from the IMO's regulatory remit.

As was seen with the A.P. Moller-Maersk incident in 2017, these excluded systems could have a significant impact upon the maritime domain. Starting on an office terminal in Ukraine, the not-Petya attack, not directly targeted at Maersk, spread through their global network and impacted ships, ports and enterprise systems across the globe. This cyber-enabled event highlighted that these systems hold operational significance, as they could cause widespread disruption to a states maritime interests.

By UNLCOS excluding these systems, there is an increased reliance on the international community to implement and enforce guidelines and practices within the sovereign space. This increases the reliance upon the sovereign state to work with the international community, and implement practices based on the guidance from the expertise within the community.

This challenge is only set to continue with the increased drive for digitisation and streamlining of maritime enterprise processes, like customs clearances. The digitisation of these processes all increases the amount of digital connectivity within the maritime domain. This reiterates the reliance on the international community sharing information about vulnerabilities and events from within the sovereign domain. This sits alongside the need to implement and enforce subsequent regulation and guidance, created by the international community, within that sovereign domain.

Exclusions under SOLAS

Most of the IMO's regulations are made mandatory by the Safety of Life at Sea Convention (SOLAS), which was created in the wake of the Titanic disaster in 1912. SOLAS however, only covers certain types of vessels including, passenger ships, cargo ships of 500 gross tonnage or mobile offshore drilling units. While these criteria mean SOLAS covers a large percentage of the worlds fleet, it fails to address the other users of the maritime space. These non-SOLAS vessels include fishing boats, pleasure craft or military vessels, all of which can be as, or more, connected than those covered by SOLAS.

The international community has already seen how smaller vessels can be utilised by determined individuals and groups. In October 2000, while refuelling in the harbour of Aden, the USS Cole was attacked by suicide bombers in a small boat laden with explosives. The explosion severely damaged the destroyer and killed 17 US sailors. More recent uses include the pirate skiff, where groups of pirates make use of small motorboats to aid the following and boarding of target vessels. This suggests that there needs to be some form of control over these vessels, as they could be used to target maritime cyberspace. E.g. GPS jamming or spoofing.

The exclusions under SOLAS means that the IMO has limited reach over the rules and regulations that determine non-SOLAS vessels behaviours. As there is a limited regulatory reach, there is also limited enforcement capabilities. This lack of enforcement means that there is a significant number of systems and uses that are not accounted for within the IMO. These systems however, could impact upon the safety and security of the marmite operational domain. Highlighting the of collaboration by the international community, as a way to share information about the risks that these non-SOLAS vessels pose.

A Systems Problem

Another key challenge for the international community to address is the complexity of systems found both onboard and onshore. While ship systems are starting to be discussed by the international community, onshore systems have received little attention. However, the issues with onshore systems are often more complicated, due to the need for these systems to be connected to other external companies, outside of a company's own digital boundaries.

Firstly, due to the time period set aside for the designing and building phase of a vessel, it means that the installed systems could be up to 10 years old before they start their service. Moreover, large shipping companies sell their vessels on towards the end of their lifecycle, often extending the recommended 25-year operational life expectancy (IMO, 2005). Alongside the logistical issues, and considerable costs associated with updating a vessels hardware, this ultimately leads to ships sailing the world's oceans with significantly out-of-date systems. By being out-of-date, it leaves these systems significantly predisposed to cyber-attack (Jones, Tam, & Papadaki, 2016).

Secondly, there is a significant number of vessels classes, all of which have their own specific requirements. While the International Association of Classification Societies (IACS) produce central rules, the individual classification societies still have the ability to create their own rules. This coupled with the multitude of operational requirements and environments means there is a significant number of different system designs and configurations, making each vessel unique. In an interview with Ship Technology the chief technology officer at SSI, Denis Morais, has argued that even in sister ship build projects, the equipment and systems being used are almost always massively different (Ship Technology, 2017).

The third and final challenge that the international community faces when dealing with the maritime cybersecurity problem, is the inherently unsecure systems found onboard vessels. Despite the design of these systems being mandated under IMO and ISO standards, they must remain insecure for operational reasons, as navigation and GMDSS relies upon it. Considering

that systems like GPS and AIS are open access, with these systems available to the public, opens them to the risk of cyber-attack, as highlighted by numerous groups (Kelion, 2018). These systems are then linked to a vessel's more secure ECDIS display, which has no capacity to determine if the data it is receiving is accurate. If these displays are presenting crew with misinformation, it could have a significant impact on the safety of both that crew and vessel.

Therefore, a greater level of detail about onboard and onshore systems and their capacities, is required to allow the creation of effective mitigation of cyber risks. It will be through the collaboration of the international community of states, commercial interests and technical experts that will allow this to happen.

Maritime Cybersecurity Regulation

This paper has argued that the collaboartion of the international community is vital to the successful mitigation of martime cyber risk. By creating robust and resiliant cybersecurity regualtion, it would ensure that the industry has a better minimum level of security, that forms a basis for cyber risk mitigation. This minimum level of security would reduce the risk of common vulnerabilities within maritime systems, whilst ensuring enforceable compliance. Comprehensive cybersecurity regualtion would also address the issue of the interconnectivity of onshore systems, which could have a diret impact on what is considered within the maritime operational domain. This new domain could require new approaches by stakeholders to ensure its continued security, which would need to be developed by the internaitonal community.

For maritime regualtion to be created it often requires a large newsworthy events that raises the threat onto the international communities agenda. Pomeroy & Earthy (2017) highlight several examples of this, which has led to the IMO being considered reactive rather than proactive in the creation of regulation. The only significant public maritime cyber event, the Maersk incident, has triggered the regulatory process, however, to a limited extent.

The incident has been a driver for the IMO to become proactive and consider the wide-reaching consequences of a cyber-incident within guidance and regulation. However, there is a sense from stakeholders in the industry, whilst publicly handled swiftly and smoothly, the consequences of the incident could have been significantly worse. Without examples from the international community of other significant cyber-incidents, the consequences of an incident remain relatively unknown.

From the discussion in the IMO, and the submitted industry papers, there seems to be a lack of a coherent understanding of the actual threats that cyber-enabled technology faces. This lack of common understanding inhibits the creation of regulation. To overcome this the IMO, through the use of the International Safety Management code (ISM), makes cyber risk management part of a ship's security practices. It will be through the associated risk assessments that greater detail of the cyber-threats to specific systems, vessel types, processes, or operational environments, will be developed.

Hopcraft & Martin (2018) argue that to effectively deal with maritime cybersecurity, it requires the creation of a Cyber Code. By the international community feeding the information, and management practices, gained from the cyber risk assessments, back into the regulatory discussion, it will allow the IMO to create regulation that effectively targets the industries cyber-threats.

The use of a Code by the IMO to target specific threats is not a new concept. In 2017 the International Code for Ships Operating in Polar Waters (Polar Code) came into force. The Polar Code is designed to deal with the specific threats that vessels operating in ice covered waters face. The use of a Code allows additional requirements to be added to existing regulations, and make them mandatory for a specific subset of vessels or systems. The same would be true of a Cyber Code. By utilising the information gained from the IMO's cyber risk assessments, it would allow the IMO to target specific systems or vessel types with common

vulnerabilities. This process would help to increase the minimum level of security of those systems.

Following the Polar Codes structure, where Section A is mandatory and Section B voluntary, a Cyber Code could overcome some of the challenges discussed earlier. By including guidelines and best practices that impact sovereign territory, within the voluntary section, allows states to decide if they wish to implement those practices. Moreover, the IMO's use of Goal-based standards also offers a way for states to implement practices in the way they see fit, while still attaining the overall goal. This could help to aid the uptake of regulation and increase the minimum level of security of onshore systems which could impact the maritime operational domain.

Moreover, the Polar Code also makes a Polar Water Operational Manual (PWOM) mandatory on all polar vessels (IMO, 2015). The manual is designed to include specific procedures that the crew must follow in the event that the operating conditions exceed the capabilities and limitations of the vessel. Within a Cyber Code the international community could implement a similar Cyber Operations Manual. This manual like the PWOM would highlight the specific procedures that need to be followed if a ship's systems are operating outside of their capabilities. For example, what the crew must do if they think that the navigation systems are compromised etc.

By utilising and expanding existing regulations, based on the international communities shared knowledge of cyber-threats, would allow the creation of effective and enforceable cybersecurity regulation. The use of a Cyber Code would allow different parts of the regulation to be updated as technology change, without reducing the effectiveness of the Code. Therefore, a Cyber Code requires the collaboration of all parts of the international community in its creation and maintenance.

Conclusion

This paper has discussed the importance of the maritime community in the understanding, and mitigation, of threats to the maritime domain. By using the example of piracy and shipping in the Polar regions, this paper has highlighted that through an international forum, the maritime community can share vital information to mitigate maritime threats successfully. The community plays three important roles within the creation of maritime cybersecurity regulation.

The first role that this community plays is in understanding the threat. The diversity of the maritime community's membership allows discussions to include local, regional and international stakeholders, as well as the required technical expertise. Through this collaboration of stakeholders, it allows the maritime community to understand the threat from all perspectives internationally.

The second role of the community is understanding the type of regulation that needs to be created. By the IMO engaging with the maritime community, it ensures that regulation and guidance that it creates is acceptable by the community. If the community does not accept the regulation or guidance, there will be little uptake, which will do little to reduce the risks to cyber-enabled technology.

The third and final role the community will play is through the enforcement of the regulation. When ratified and entered into force the Classification Societies and insurance companies will play a central role in ensuring that the regulation is adhered to and enforced. It is then through the compliance process that issues and concerns will be noted and fed back into the IMO, ensuring that amendments are made to safeguard the continued effectiveness of maritime cybersecurity regulation.

Bibliography

Berner, G., Hopcraft, R., Scanlan, J., Lutzhoft, M., & Earthy, J. (2018). A Virtual Teams Model for Supporting Maritime Technology Management. *The Royal Institution of Naval Architects Human Factors Conference*, (pp. 81-86). London.

Bueger, C. (2015). What is maritime security? *Marine Policy*(53), 159-164.

Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). *The Future of Maritime Cyber Security.* Retrieved from Lancaster University: http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf

Glück, Z. (2015). Piracy and the production of security space. *Environemnt and Planning: Society and Space, 33*(4), 642-659.

Hopcraft, R., & Martin, K. M. (2018). Effective Maritime Cybersecurity Regualtion - the Case for a Cyber Code. *Journal of the Indian Ocean Region*, 354-366.

InfluenceMap. (2017, October). *Corporate Capture of the International Maritime Organisation.* Retrieved from InfluenceMap: https://influencemap.org/site/data/000/302/Shipping_Report_October_2017.pdf

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

International Maritime Organisation. (2014). *Measures Toward Enhancing Maritime Cyber Securty. MSC94/1/1.* Retrieved February 2019, from https://docs.imo.org/Search.aspx?keywords=MSC%2094%2F4%2F1

International Maritime Organisation. (2015). *MEPC 68/21/Add.1 - INTERNATIONAL CODE FOR SHIPS OPERATING IN POLAR WATERS (POLAR CODE).* Retrieved from International Maritime Organisation: http://www.imo.org/en/MediaCentre/HotTopics/polar/Documents/POLAR%20CODE%20TEXT%20AS%20ADOPTED.pdf

International Maritime Organisation. (2016). MSC.1/Circ.1526 - Interim Guidelines on Maritime Cyber Risk Management. London.

International Maritime Organisation. (2017). *Maritime Cyber Risk Management in Safety Management Systems.* Retrieved from International Maritime Organisation: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf

Jones, K. D., Tam, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security. *Engineering & Technology Reference, 1*(1).

Kelion, L. (2018, June). *Ship hack risks chaos in the English Channel.* Retrieved from The BBC: https://www.bbc.co.uk/news/technology-44397872

NATO. (2016). *Operation Ocean Shield.* Retrieved from Operations Archive, Allied Maritime Command: https://mc.nato.int/missions/operation-ocean-shield.aspx

Oceans Beyond Piracy. (2014). *The State of Maritime Piracy 2013.* Retrieved from Oceans Beyond Piracy: http://oceansbeyondpiracy.org/sites/default/files/attachments/SoP2013-Digital_0.pdf

Pomeroy, R. V., & Earthy, J. V. (2017). Merchant Shipping's Reliance on Learning from Incidents - A Habit that needs to Change for a Challenging Future. *Safety Science*(99), 45-57.

Ship Technology. (2017, November). *Sister ships: a builder's biggest challenge*. Retrieved from Ship Technology: https://www.ship-technology.com/features/sister-ships-builders-biggest-challenge/