Scientific and Technical Journal

Safety & Defense 5(1) (2019) 46–48

Commercial Maritime and Cyber Risk Management

Akash RANA

Independent international maritime expert, United Kingdom; rana.aakash@gmail.com
ORCID: 0000-0003-3706-8204

Abstract

The starting point of the paper is the recognition of the growing threat of cyber-attacks to commercial maritime. Constantly growing dependency on technology has obvious advantages, on the other hand, however, it makes commercial maritime vessels progressively more vulnerable to cyber-crime, including GPS signal interference, malware attacks or even gaining control over ships' systems and networks. The main objective of the paper is to present and discuss the Guidelines on Cyber Security Onboard Ships developed by the International Maritime Organization, including best practices for implementation of cyber risk management. The article's goal is to summarize the guidelines and to familiarize the reader with the reasons why and the methods how they should be implemented. The paper is concluded with an example how the Guidelines can be adopted by national authorities, i.e., a brief presentation of "Code of Practice: Cyber Security for Ships" – a document developed by the British government that transposes the IMO guidelines.

Keywords: commercial maritime, cyber threat, cyber risk management, maritime security, security

1. Introduction

In an increasingly connected and technologically dependent world, new areas of vulnerability are emerging. However, this dependency increases the ship's and port's presence in the cyber domain, increasing the chances of being targeted and offering new vectors for such attacks. There needs to be a fundamentally different and robust cyber risk management of the entire maritime infrastructure. In the current climate of geopolitical uncertainty, it has never been more important to have the maritime sector equipped to deal with threats to security.

Cyber-attacks are much stealthier and have a range of potential implications including business disruption, financial loss, damage to reputation, damage to goods and environment, incident response cost, international sanctions, fines and/or legal issues. IPv6 has some 3.4 x 10^{38} addresses possible, to scan them all at 1 million/sec it would take more 5000 years. As per World Bank, in Russia alone there are some 40 odd organized networks of cyber-crimes.

The vast majority of marine vessels have two significant capabilities, each supported with specific hardware and software. First, all vessels must have systems for navigation and propulsion. Significant technological advances in these areas are becoming more ubiquitous, providing the crew with a more comprehensive view on what is happening inside and outside of the ship, often in real time. These capabilities include, but are not limited to, global positioning systems (GPS), marine Automatic Identification Systems (AIS), and the Electronic Chart Display and Information Systems (ECDIS) and the associated digital nautical charts. As a result, fewer human crewmembers are needed to man modern day ships. However, this dependency on technology increases the vessel's presence in the cyber domain, increasing its chances of being targeted and offering new vectors for such attacks. For example, the global navigation satellite system (GNSS) signals of GPS tend to be very weak and thus deliberate or unintentional interference of

the signal can easily deter signal recovery or even overload receiver circuitry. While this may not normally be an issue for a marine vessel on the open sea, if an attacker were to introduce an interference device, disguised and loaded as cargo, this GPS vulnerability may be exploited. Furthermore, it has been speculated that such a device may cost as little as £40 to build and may be easily obtained and utilized by an inexperienced hacker. Researchers at University of Texas at Austin (UT Media, 2013) managed to exploit the lack of authentication of satellite GPS signals, and successfully divert the course of a $80 million yacht with a GPS spoofing device. As the GPS receivers of the vessel did not authenticate incoming signals, it was possible to slowly overpower the authentic ones, and eventually gain control of the vessel's navigational system without being detected or raising any alarms. Low cost GPS spoofing devices have already emerged, with notable example the GPS emulator by Qihoo 360, presented in Defcon 2015 and estimated at a cost of $300 (Jones et al., 2016, p. 3). It is a well-known fact that technological advances always precede at an exceptional rate whilst the regulation at best can follow linearly.

2. Cyber Threat to Commercial Maritime

Ships are increasingly using systems that rely on digitization, integration, and automation, which calls for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet. This brings the greater risk of unauthorized access or malicious attacks to ships' systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media. The safety, environmental and commercial consequences of not being prepared for a cyber incident may be significant. Responding to the increased cyber threat, a group of international shipping organizations, with support from a wide range of stakeholders have developed these guidelines, which are designed to assist companies develop resilient approaches to cyber security onboard ships. Approaches to cyber security will be company- and ship-specific but should be guided by appropriate standards and the requirements of relevant national regulations. The guidelines provide a risk-based approach to identifying and responding to cyber threats. An important aspect is that relevant personnel should have training in identifying the typical modus operandi of cyber-attacks.

IMO – the International Maritime Organization – is the United Nations specialized agency with responsibility for the safety and security of shipping has developed guidelines that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines on Cyber Security Onboard Ships are aligned with the IMO guidelines and provide practical recommendations on maritime cyber risk management covering both cyber security and cyber safety (BIMCO et.al., 2018).

3. Guidelines on Maritime Cyber Risk Management

3.1. Scope

The Facilitation Committee of the IMO, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the Guidelines on maritime cyber risk management as set out in the annex to Guidelines on Maritime Cyber Risk Management:

- *These Guidelines provide high-level recommendations for maritime cyber risk management. For these Guidelines, maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.*
- *Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.*
- *For details and guidance related to the development and implementation of specific risk management processes, users of the Guidelines should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.*
- *Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.*
- *Predicated on the goal of supporting safe and secure shipping, which is operationally resilient to cyber risks, these Guidelines provide recommendations that can be incorporated into existing risk management processes. In this regard, the Guidelines are complementary to the safety and security management practices established by this Organization* (MSC FAL.1/Circ. 3, 2017, p. 1).

3.2. Application

- *These Guidelines are primarily intended for all organizations in the shipping industry and are designed to encourage safety and security management practices in the cyber domain.*
- *Recognizing that no two organizations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application.*
- *Ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.*
- *These Guidelines are recommendatory* (MSC FAL.1/Circ. 3, 2017, p. 2-3).

4. Best Practices for Implementation of Cyber Risk Management

The annex to Guidelines on Maritime Cyber Risk Management defines also the best practices for implementation of cyber risk practices:

- *The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyberthreats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.*
- *Additional guidance and standards may include, but are not limited to:*
  - *The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.*
  - *ISO/IEC 27001 standard on Information technology – Security techniques –Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).*
  - *United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).*
- *Reference should be made to the most current version of any guidance or standards utilized* (MSC FAL.1/Circ. 3, 2017, p. 4).

5. Developing National Best Practice Guidance to Transpose IMO Guidelines

In 2017, the British Department of Transport published "Code of Practice: Cyber Security for Ships," where British government presents "two sets of guidance that are generally applicable to organizations, the 10 Steps to Cyber Security and the Cyber Essentials scheme. The latter addresses basic technical control that all organizations should have in place to mitigate common cyber security issues" (DfT, 2017, p. 20). The document was developed by the UK government by collaboration and partnering with Institution of Engineering and Technology, London, United Kingdom, Department for Transport (DfT) and Defense Science and Technology Laboratory (Dstl).

The document states that "this Code of Practice should be read by board members of organizations with one or more ships, insurers, ships' senior officers (for example, the Captain/Master, First Officer and Chief Engineer) and those responsible for the day-to-day operation of maritime information technology (IT), operational technology (OT) and communications systems. It does not set out specific technical or construction standards for ship systems, but instead provides a management framework that can be used to reduce the risk of cyber incidents that could affect the safety or security of the ship, its crew, passengers or cargo" (DfT, 2017, p. 5).

The "Code of Practice" provides also actionable good practice advice on areas such as:

- *Developing a Cyber Security Assessment and Plan*
- *Devising the most appropriate mitigation measures*
- *Having the correct structures, roles, responsibilities and processes in place*
- *Managing security breaches and incidents*
- *Highlighting the key national and international standards and regulations that should be reviewed and followed* (DfT, 2017, p. 73).

6. Conclusion

It is a fact that IT technology development and democratization strongly contributes to growing vulnerability of maritime commercial vessels to various kinds of cyber-attacks. The International Maritime Organization has recognized that peril and developed guidelines how to manage the risks as well as best practices how to implement them. The paper introduces and describes the new code as presented in the "Guidelines on Cyber Security Onboard Ships" and best practices how to deploy them. This new code will be of real value to all those responsible for ship security and business continuity and can be used as an integral part of an organization's overall risk management system.

Bibliography

[1] Jones, K.D., Tam, K., Papadaki, M. (2016). Threats and Impacts in Maritime Cyber Security. Engineering & Technology Reference, 2016, doi: 10.1049/etr.2015.0123.
[2] BIMKO et al. (2018). The Guidelines On Cyber Security Onboard Ships, Version 3, retrieved from: https://iumi.com/uploads/2018-Cyber_Security_Guidelines.pdf (16.06.2019.).
[3] MSC FAL.1/Circ. 3. [International Maritime Organization] (2017). Guidelines on Maritime Cyber Risk Management (5 July 2017), 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 (16.06.2019.).
[4] DfT. [Department of Transport] (2017). Code of Practice: Cyber Security for Ships, retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf (16.06.2019.).
[5] www.theiet.org/standards
[6] UT Media. (2013). UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea (29 July 2013), retrieved from: https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/ (16.06.2019.).