Australian Information Security Management Conference

Conferences, Symposia and Campus Events

2017

A critical analysis of security vulnerabilities and countermeasures in a smart ship system

Dennis Bothur
Edith Cowan University

Guanglou Zheng
Edith Cowan University

Craig Valli
Edith Cowan University

A CRITICAL ANALYSIS OF SECURITY VULNERABILITIES AND COUNTERMEASURES IN A SMART SHIP SYSTEM

Dennis Bothur, Guanglou Zheng, Craig Valli
Security Research Institute, School of Science, Edith Cowan University, Perth, Western Australia
d.bothur@ecu.edu.au, g.zheng@ecu.edu.au, c.valli@ecu.edu.au

Abstract

It is timely to raise cyber security awareness while attacks on maritime infrastructure have not yet gained critical momentum. This paper analyses vulnerabilities in existing shipborne systems and a range of measures to protect them. It discusses Information Technology network flaws, describes issues with Industrial Control Systems, and lays out major weaknesses in the Automated Identification System, Electronic Chart Display Information System and Very Small Aperture Terminals. The countermeasures relate to the concept of "Defence-in-depth", and describe procedural and technical solutions. The maritime sector is interconnected and exposed to cyber threats. Internet satellite connections are feasible and omnipresent on vessels, offshore platforms and even submarines. It enables services that are critical for safety and rescue operations, navigation and communication in a physically remote environment. Remote control of processes and machinery brings benefits for safety and efficiency and commercial pressure drives the development and adaptation of new technologies. These advancements include sensor fusion, augmented reality and artificial intelligence and will lead the way to the paradigm of "smart" shipping. Forecasts suggest unmanned, autonomous ships in international waters by 2035. This paper is the starting point for future research, to help mapping out the risks and protect the maritime community from cyber threats.

Keywords: maritime cyber security, smart shipping, autonomous shipping, vulnerabilities, and countermeasures

INTRODUCTION

Geographical isolation exposes mariners to a set of unique challenges such as navigating through rough weather and evading pirate attacks. Technology on ships plays a significant role to help manoeuvring through those conditions and it enables communication in situations of emergency and distress. Unfortunately, any type of technology has the potential to be used for malicious purposes. Cyber security awareness and culture is new on the agenda of the maritime community, but it must be taken seriously to avoid catastrophic consequences.

Universal satellite and data connectivity is one of the major advancements in seafaring, but this brings along a myriad of new risks. For instance, many critical systems on board rely on the Global Navigation Satellite System (GNSS) for safe navigation, communication, emergency response, and traffic control. However, disrupted or manipulated Global Positioning System (GPS) signals can send ships off their course and cause collisions, groundings, and environmental disasters. In 2016, multiple ships outbound from the United States (U.S.) reported GPS interferences which prompted the US Coast Guard to issue "Safety Alert 01-16 – GNSS – Trust, but Verify. Report Disruptions Immediately" (United States Coast Guard, 2016). In 2017, reports emerged of more than 20 vessels which noticed spoofed GPS signals that placed them about 25 nautical miles inland (Hambling, 2017). The source of the attack was attributed to tests performed by a nation-state. Adversaries are "testing the waters" but they already have the knowledge, tools, and motivation to launch attacks with potentially devastating outcomes. It is very alarming when we consider that this applies to naval vessels carrying advanced weaponry as well as the commercial shipping sector, which is part of the critical infrastructure and accounts for more than 90% of cargo transported globally (National Institute of Standards and Technology, 2017).

A host of weak spots in ship- and shore-based cyber systems has already been exposed by research conducted in the field. Unawareness or ignorance of these flaws leads many organisations to taking shortcuts in regard to applying and policing appropriate security measures. Additionally, rapid cycles of product development, implementation, maintenance, and decommissioning are overwhelming for the majority of maritime stakeholders.

The following section outlines critical vulnerabilities in common IT systems and Industrial Control Systems (ICS) on board. It explains the risks related to the heavy reliance on navigation and communication systems such as the Electronic Chart Display Information System (ECDIS), the Automated Identification System (AIS), and Very Small Aperture Terminals (VSATs). The section *Countermeasures* lays out current procedural and technological strategies to protect maritime infrastructure from malicious attacks and it describes the concept of *Defence in Depth*.

VULNERABILITIES

Vulnerabilities are flaws in a system that have the potential to be exploited by malicious parties. This section outlines vulnerabilities of several technologies used in IT networks, industrial control systems, navigation, and communication systems.

The purpose of critical services in the maritime community is to ensure the safety of people, equipment, and the environment. For example, the Global Maritime Distress and Safety System (GMDSS) is a set of standards and components to aid search and rescue operations for vessels in emergency situations. Each component of the GMDSS (e.g. VSAT terminals, AIS transponders) comes with a set of potential vulnerabilities. Other services include voice communications, crew welfare and entertainment systems, guest Wi-Fi, and video monitoring. These systems are perceived to be less critical to safety and operations and thus routinely left unpatched and exposed to attacks. Figure 1 summarises critical on-board systems which could be vulnerable to cyber-attacks. The weaknesses of each of these systems are explained in the sections below.

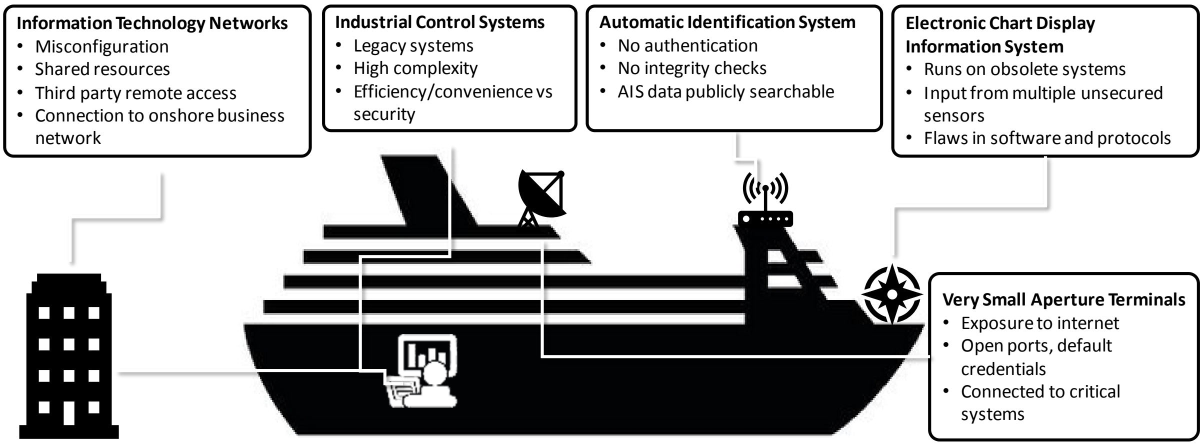
Information Technology Networks
• Misconfiguration
• Shared resources
• Third party remote access
• Connection to onshore business network
Industrial Control Systems
• Legacy systems
• High complexity
• Efficiency/convenience vs security
Automatic Identification System
• No authentication
• No integrity checks
• AIS data publicly searchable
Electronic Chart Display Information System
• Runs on obsolete systems
• Input from multiple unsecured sensors
• Flaws in software and protocols
Very Small Aperture Terminals
• Exposure to internet
• Open ports, default credentials
• Connected to critical systems

Figure 1 On-board systems where vulnerabilities could exist.

IT Networks

An Information Technology (IT) network is the fabric that integrates core business and operation systems on board and leverages shared databases and other systems. These systems can be used for accounting, cargo management, customs and shipping, human resource planning, and administration (Hudson Analytix Inc, 2017).

A malware outbreak in June 2017 paralysed IT networks across the world and caused significant business disruptions and loss of revenue. The worm "NotPetya" initially infected computers through a malicious update in an accounting software product. It then spread to attached systems, wiping or encrypting files and demanding ransom payments (Symantec Security Response, 2017). The Danish shipping company A.P. Moller-Maersk was one of the organisations that were hit the hardest and it reported a loss of $300M due to the significant system shutdowns and restoration efforts across its critical systems (Mimoso, 2017).

The event underlines that many organisations still lack a coherent approach to managing the cyber security of their systems. Business-critical software may be not updated or replaced because it is only compatible with other legacy systems or protocols. Some organisations do not have a regular patching or update regime and thus their antivirus software is outdated, or important application security updates are not patched. Networks are often inadequately segmented to manage access control, especially for third parties. IT systems should be scrutinised carefully as they provide a wide attack surface and many entry points for adversaries. All systems and endpoints must be secured, which in most cases does not happen. Third party access (e.g. for implementation, support and maintenance of equipment) further exposes vulnerable systems to the open world.

Critical control networks should be in a secured zone, isolated from the corporate IT network and the internet. However, economic pressure, regulations, and requirements for remote monitoring and control increase the need for a connection into the IT network. The design and configuration of the links between IT networks rarely consider authentication and encryption methods, thus exposing potential vulnerable and legacy system to the internet. IT systems on vessels are often connected with onshore facilities and this further increases the exposure to systemic and persistent threats (Baltic and International Maritime Council, 2017).

ICS – Industrial Control Systems

Industrial Control Systems (ICS) on ships assist to reduce human errors, increase resource efficiency, prolong equipment life, and ensure economic advantages (Wang & Zhang, 2000). ICS control and monitor parameters on board, including temperature, pressure, level, viscosity, flow control, speed, torque, voltage, current, machinery and equipment status (Zaghloul, 2014). An array of devices and protocols from different vendors and technological eras and are often “bolted together” to provide interoperability. Most of these components were designed and programmed without any security in mind and data is transferred in plaintext. The onus of *securing* the components should be shared between the vendor, who follows a secure development framework, and the operator, who configures the components in line with industry standards and recommendations. The reality is often that either party assumes that the other party is responsible and no-one does it at all, leaving many critical weaknesses for attackers to exploit (Shoultz, 2017). It is crucial for integrators, implementers, and operators of ICS to understand the system’s limitations and vulnerabilities of its components and protocols.

Primary control systems (hydraulic, electrical, automatic control) are vital to the ship’s safe voyage. They are exposed to difficult environmental challenges, such as pressure, vibration, and humidity. These control systems are integrated via the ship’s distributed IT network. A continuous link between IT networks and on-shore facilities enables remote access for monitoring, fault-finding, and troubleshooting, reduces site travel costs, and streamlines the collection and analysis of field data (Moxa Inc., 2017; Orbcomm, 2017). A major concern is that operators and engineers routinely bypass security for convenience and efficiency, which could have a cascading effect on the entire organisation (Zurich, 2014). This behaviour is attributed to the lack of awareness and skills, the commercial pressure to save time, and the plain non-adherence to security policies.

AIS – Automatic Identification System

The Automatic Identification System (AIS) is a ship- and shore-based Very High Frequency (VHF) radio broadcasting system. It is used for Vessel Traffic Services (VTS), search and rescue operations, accident investigation, and weather forecast (Australian Maritime Safety Authority). Reliance on the transmitted information is critical to situational awareness and collision avoidance at sea. AIS transponders communicate over the air without any authentication or integrity checks. Attackers can inject signals via a Software Defined Radio (SDR) and place fake “man-in-water” beacons, render the ship invisible and inject false weather reports (Balduzzi, Wihoit, & Pasta, 2013). Relying on the potentially incorrect information can lead to wrong decisions and catastrophic outcomes.

AIS data is publicly available via websites such as “Vesselfinder” (VesselFinder Ltd, 2017) and “Marinetraffic” (MarineTraffic, 2017). The International Maritime Organisation (IMO) has “condemned the regrettable publication on the world-wide web, or elsewhere” as it reveals a wealth of information on the vessel and its route which can be invaluable for a targeted attack (International Maritime Organisation, 2004).

ECDIS – Electronic Chart Display Information System

The Electronic Chart Display Information System (ECDIS) is mandated by the IMO for all commercial vessels and usually is installed on the bridge. ECDIS software implementations have an extensive list of weaknesses. Often the system runs on legacy computers (e.g. Windows XP desktops) for which no security updates are available. The maps are loaded onto the system either via the internet, or manually via USB or DVD. Sensor feeds comes from a multitude of other onboard systems such as Radar, Navigation Telex (Navtex), ICS, and satellite terminals. This provides a wide surface for a compromise. Dyryavyy (2014) audited commercial ECDIS software and highlighted some significant security risks that would allow an attacker to replace or delete files on the system or inject malicious content. Thus, tampered sensor data could be sent to ECDIS, which would influence decisions for navigation, and may cause collision or grounding.

VSAT – Very Small Aperture Terminal

A Very Small Aperture Terminal (VSAT) is a communications station used to send and receive data via a satellite network. The transceiver is installed above deck in line of sight of the satellite and a control unit below deck provides the interface to a PC. VSATs enable a range of communication and safety services including GMDSS, ECDIS, AIS, phone, internet, cargo management, vessel routing, radio integration, telemedicine, crew welfare, tele-training, and weather forecast. Santamarta (2014) tested a range of VSATs from multiple manufacturers and concluded that *all* the audited devices are vulnerable at the protocol and implementation level. They transmit in plain text without authentication, encryption, or integrity checks. This can allow an attacker to inject fake signals or malicious code to cause device to shut down or corrupt the system, disabling the ship from navigating safely.

A ship’s geolocation is publicly available via AIS aggregators, but the real risk is that VSAT network interfaces can be identified on the internet, e.g. via the “Shodan Ship Tracker” (Matherly, 2017)). This can reveal manufacturer names, product codes, and other data which is useful for a potential attack. Vendors generally publish default credentials on their websites and many terminals run with unchanged default factory settings, including administrator usernames and passwords. Once an attacker found an open VSAT interface, they can change GPS coordinates, settings, and upload malicious software. This allows for further compromise of the network and may give up an entry point to critical control systems (Morse, 2017).

It is concerning that these systems are widely used by NATO and across critical infrastructure, as their exploitation could lead to catastrophic consequences.

COUNTERMEASURES

The concept of cyber security is novel to many maritime stakeholders and it is timely to raise awareness about the existing countermeasures. It is essential to create a common understanding that includes the shared responsibility amongst maritime stakeholders. The following section outlines a strategic direction to securing cyber technology on ships.

Defence-in-depth

Security is neither a product that can be bought off the shelf, nor a procedural blueprint that every organisation can apply in the same way. Securing maritime IT environments "in depth" creates an all-encompassing protection mantle and builds resilience to external and internal threats. This layered approach is depicted in Figure 2 and includes procedural and technical countermeasures on each layer (outlined thereafter).

Policy: Defence begins with the organisation's leadership, where *strategies* are formed, and *policies* are made.

Physical security: Physical measures to prevent intruders from entering the vessel by using guards, locks, alarms, and technical access control.

Perimeter security refers to measures which block attacks from entering the network through external communication connections.

Network security is concerned with the design, configuration and implementation of security zones, network segments, and other network based defences.

The layer of *Host security* protects computers and other endpoints with measures such as antivirus software and host based firewalls.

Application security prevents attackers from exploiting software flaws and entails secure software development, authentication, access control, and application vulnerability management.

Finally, the *Data security* layer addresses how to protect the information itself, whether it is in use, in transit, or at rest. Each layer plays a significant role in the overall security of maritime critical infrastructure.

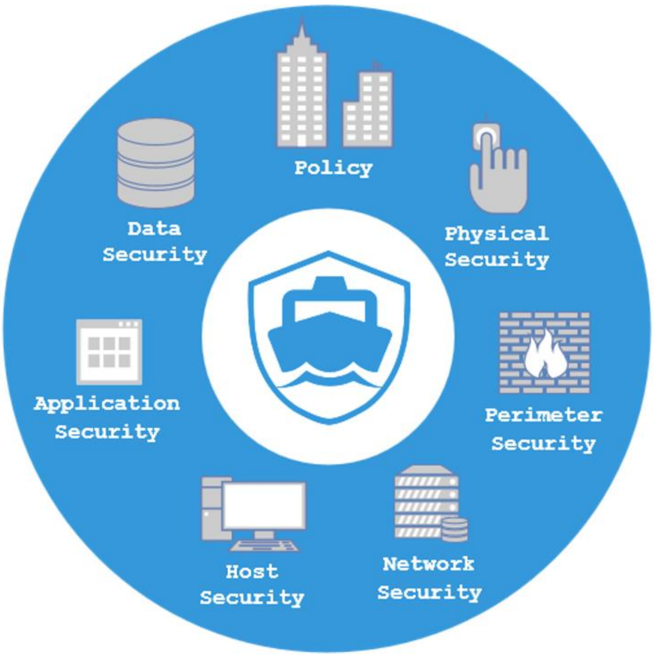

Figure 2 A systematic approach to defend the smart ship in depth

Security policies and procedures

The most important security asset on board is a vigilant employee. Policies and procedures give staff the necessary tools and guidance for their critical role within the organisation. Training and awareness programs enable staff to understand why and how each individual can help. Policy and procedural documents should be clearly communicated, published, and acknowledged. Policies must address how the content will be enforced and what the consequences are if ignored. The documents must be reviewed regularly to ensure they appropriately cover the organisation in a world of continuous technological advancements.

The policies should address and explain at least the following:

- Data recovery capability, backups, redundancy, business continuity and disaster recovery planning
- Administrator privileges, concepts of least privilege and the separation of duties
- Remote access control, use of encryption and Virtual Private Networks (VPN)
- Physical access, removable media controls, "Bring your own device" (BYOD)

- Acceptable personal use of IT systems
- Email, phishing, passwords rules
- Software upgrade, patch, and maintenance schedules
- Anti-virus/-malware software and signature updates
- White- or blacklisting and the use of third party software
- Onshore support and contingency planning
- Equipment disposal, and data destruction

(Baltic and International Maritime Council, 2017; International Maritime Organisation, 2016)

Technical security solutions

Policies require a physical or technical implementation to be monitored and enforced. Guards, locks, and security cameras protect equipment like the ECDIS and VSATs from unauthorised use. Secure network design and configuration should segment the network to prevent the direct exposure of devices and ICS to the internet. For example, a VSAT hub can act as an intermediate hop for remote connections to the terminal. Firewalls and intrusion prevention systems monitor and block the data traffic as it leaves and enters the ship's IT network. The dataflow between all nodes on the network, including ICS traffic and satellite and radio communications, should be mapped out and encrypted, e.g. by using a VPN. This way, even if signals were intercepted, the adversary could not easily read the message.

Network hardening refers to the secure configuration of hardware and software and the deactivation of unused features and accounts. It applies to firewalls, routers, switches, servers, voice communication equipment, and any other device on the network. Hardening includes disabling unused ports and services but also managing and installing updates, patches and bugfixes. Default usernames and passwords must be changed where possible. The use of complex passwords protects against automated port-scan and dictionary based login attempts, for example on the VSAT terminal. Access control systems should be configured and audited regularly to only allow users the access rights they need to perform their job.

X.509 certificate based authentication can secure the access to the ship's wireless network for authorised crew members and guests. It is recommended to create a separate wireless network (Virtual Local Area Network – VLAN) for guests to allow only minimal access to resources on the network. The usage of secure communications protocols like ssh, https, and sftp should be implemented and enforced where it is possible. Multi-Factor Authentication (MFA) can provide an additional layer of access security to sensitive systems and applications. Application whitelisting prevents staff from installing unapproved and potentially malicious programs. The threat of intentional or accidental data leakage can be mitigated with data-loss-prevention software (Mertens, 2014; Shoultz, 2017; Soullie, 2014).

DISCUSSION AND CONCLUSION

This paper analysed the current cyber security vulnerabilities and countermeasures in smart ship systems. It demonstrated that malicious attacks and incidents with devastating consequences are not only possible, but imminent. The maritime domain leverages cyber technologies to assure the safety and efficiency of operations at sea but vessels, platforms, satellites, and onshore facilities are increasingly interconnected, exposing them to an abundance of systemic and technology based threats.

The paper outlined the flaws in existing information technology networks on board and concluded that the high level of complexity and shared resources create a wide attack surface which should be segmented and secured systematically. Industrial Control Systems are often built on legacy infrastructure and implemented without security in consideration. Networking capabilities supplement these systems to allow remote control and troubleshooting but at the same time expose them to the IT network and its inherent vulnerabilities.

Vessel operators depend on the Automated Identification System for traffic and emergency services. Flaws discovered in the underlying hardware, software, and protocols would allow an adversary to manipulate the transmitted data and this could lead to navigational decisions with devastating outcomes. The Electronic Chart Display Information System equipment is equally unsecure and susceptible to malicious tampering. It often runs on legacy systems with well published vulnerabilities and the software itself can be misused to manipulate maps and sensor data which can compromise the safe navigation at sea.

Very Small Aperture Terminals provide geospatial capabilities for many critical services on board. The data flow between satellites and terminals is unencrypted and provides no integrity checks. Terminals can be tracked over the public internet and many interfaces are not locked down. An attacker could remotely log in to the exposed device and change critical information as well as using it as an entry point to pivot through the connected ship network.

The presented countermeasures were explained in the context of the multi-layered "Defence-in-depth" approach. Further recommendations were based on the implementation of security related policies and procedures. It was suggested that technical security solutions are needed to implement and enforce said policies, and examples were presented relating to each layer of the "Defence-in-depth" approach.

The maritime domain is moving fast towards the paradigm of "smart" transportation with more innovative technologies and AI driven decision-making. While this implies a wealth of benefits for economy, critical infrastructure, and military, it also increases the complexity of the threats to the maritime community before we have discovered and mitigated the flaws in existing systems and legacy technology. The current coverage of research in the field of maritime cyber security is sporadic and fragmented, leaving many stakeholders unaware of the risks and unprepared to treat them.

The cyber security community has the urgent obligation to support the shipping industry with research, tools, security assessments, and education programs. In doing so, we will enable organisations to make informed strategic decisions and effectively allocate resources to protect each member and the maritime community as a whole.

Future work based on the present paper will aim to map all identifiable risks and to establish a status quo of the cyber security posture of the maritime sector.

REFERENCES

Australian Maritime Safety Authority. Automatic Identification System (AIS). Retrieved 01/09/2017 from https://www.amsa.gov.au/navigation/services/ais/.

Balduzzi, M., Wihoit, K., & Pasta, A. (2013). *Hey captain, where's your ship? attacking vessel tracking systems for fun and profit*. Paper presented at the The Eleventh Annual Hack in the Box (HITB) Security Conference in Asia. http://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf

Baltic and International Maritime Council. (2017). *The Guidelines on Cyber Security Onboard Ships*. Retrieved from https://www.bimco.org/-/media/bimco/news-and-trends/news/security/cyber-security/2017/industry-guidelines-cyber-security---june-2017.ashx

Dyryavyy, Y. (2014). *Preparing for Cyber Battleships – Electronic Chart Display and Information System Security*. Retrieved from https://www.nccgroup.trust/au/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/

Hambling, D. (2017). Ships fooled in GPS spoofing attack suggest Russian cyberweapon. Retrieved 28/08/2017 from https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/#.WZy1mN2_kyQ.linkedin.

Hudson Analytix Inc. (2017). *Global Threats: Cybersecurity in Ports (Donald Duck, Daughters & Dollars)*. Paper presented at the Hemispheric Conference on Port Competitiveness & Security: Finding the Right Balance, University of Miami, Center for International; Business Education & Research. http://portalcip.org/wp-content/uploads/2017/03/Max-Bobys.pdf

International Maritime Organisation. (2004). *MSC 79/23 - Report of the Maritime Safety Committee on its Seventy-Ninth Session*. Retrieved from http://www.crs.hr/Portals/0/docs/eng/imo_iacs_eu/imo/msc_reports/MSC79-23.pdf?ver=2010-11-03-143734-000

International Maritime Organisation. (2016). *Measures to enhance Maritime Security: Report of the Working Group* (MSC 96/WP.9). Retrieved from http://12zc4845uhr73vbfjp3ubgkz.wpengine.netdna-cdn.com/wp-content/uploads/2016/05/Cyber-guidelines.pdf

MarineTraffic. (2017). marinetraffic.com. Retrieved 15/10/2017 from https://www.marinetraffic.com/en/p/contact-us.

Matherly, J. (2017). Shodan Ship Tracker. Retrieved 15/10/2017 from https://shiptracker.shodan.io/.

Mertens, M. (2014). Securing VSAT Terminals. *newtec.eu*. Retrieved 13/09/2017 from http://www.newtec.eu/article/article/securing-vsat-terminals.

Mimoso, M. (2017). Maersk Shipping Reports $300M Loss Stemming from NotPetya Attack. Retrieved 16/10/2017 from https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/.

Morse, J. (2017). Remotely hacking ships shouldn't be this easy, and yet ... *mashable.com*. Retrieved 12/09/2017 from http://mashable.com/2017/07/18/hacking-boats-is-fun-and-easy/#mjW1KLCj6aqb.

Moxa Inc. (2017). Industrial Ethernet for In-ship Communication. Retrieved from https://www.moxa.com/event/Net/2010/Maritime_microsite/In-ship_solution.htm.

National Institute of Standards and Technology. (2017). *Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1*. Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Orbcomm. (2017). SCADA System Monitoring. Retrieved 05/09/2017 from https://www.orbcomm.com/en/industries/natural-resources/scada-system-monitoring.

Santamarta, R. (2014). SATCOM terminals: Hacking by air, sea, and land. Retrieved 08/09/2017 from https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf.

Shoultz, D. (2017). Securely Connected Vessels: Vessel Communications and Maritime Cybersecurity. *maritimeprofessional.com.* Retrieved 07/09/2017 from https://www.maritimeprofessional.com/blogs/post/securely-connected-vessels-vessel-communications-and-maritime-15176.

Soullie, A. (2014). *Pentesting PLCs 101*. Paper presented at the Blackhat Europe 2014. https://www.blackhat.com/docs/eu-14/materials/eu-14-Soullie-Industrial-Control-Systems-Pentesting-PLCs-101.pdf

Symantec Security Response. (2017). Petya ransomware outbreak: Here's what you need to know. Retrieved from https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know.

United States Coast Guard. (2016). Safety Alert 01-16 - Global Navigation Satellite Systems - Trust, but Verify. Retrieved 06/10/2017 from http://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0116.pdf.

VesselFinder Ltd. (2017). Vessel Finder. Retrieved 15/10/2017 from https://www.vesselfinder.com/contact.

Wang, J., & Zhang, S. M. (2000). Management of human error in shipping operations. *Professional Safety, 45*(10), 23-28.

Zaghloul, M. S. (2014). Online Ship Control System Using Supervisory Control and Data Acquisition (SCADA). *International Journal of Computer Science and Application*.

Zurich. (2014). *Beyond data breaches: global interconnections of cyber risk*. Retrieved from https://www.jasadvisors.com/custom/uploads/2014/04/Risk-After-Next-Whitepaper.pdf