Received 17 August 2018
Accepted 22 September 2018

Cyberattacks on ships: a wicked problem approach

Joan Mileski
Department of Maritime Administration, Texas A&M University at Galveston, Galveston, Texas, USA

Christopher Clott
Department of Marine Logistics and Transportation, SUNY Maritime College, New York, USA, and

Cassia Bomer Galvao
Texas A&M University at Galveston, Galveston, Texas, USA

Abstract

Purpose – The maritime industry is increasingly impacted by the Internet of things (IoT) through the automation of ships and port activities. This increased automation creates new security vulnerabilities for the maritime industry in cyberspace. Any obstruction in the global supply chain due to a cyberattack can cause catastrophic problems in the global economy. This paper aims to review automatic identification systems (AISs) aboard ships for cyber issues and weaknesses.

Design/methodology/approach – The authors do so by comparing the results of two receiver systems of the AIS in the Port of Houston; the JAMSS system aboard the Space Station and the "Harborlights" system for traffic control in the Port.

Findings – The authors find that inconsistent information is presented on the location of same ships at the same time in the Port. Upon further investigation with pilots, the authors find that these inconsistencies may be the result of the strength of power with which an AIS is transmitted. It appears the power may be reduced to the AIS in port but that it varies within port and varies by pilot operators. This practice may open the AIS system for tampering.

Originality/value – Further, this inconsistency may require further policy regulation to properly address cyber information in a port.

Keywords Wicked problem, Cyberattack, AIS, Maritime cybersecurity, Ship automation

Paper type Research paper

1. Introduction

The Internet of things (IoT) is the internet workings of physical devices, vehicles, buildings and other items – embedded with electronics, software, sensors, actuators and network connectivity – that enable these objects to collect and exchange data (Xia *et al.*, 2012). Often, these devices are also referred to as "connected devices" and "smart devices." The maritime industry is increasing impacted by the IoT (Murrison, 2016).

The IoT manifests itself in ships and port through increasing automation and maintenance (Ingham, 2014). Although the systems provide increased safety for ships, many of the systems on a ship or port are interdependent (Smierzchalski, 1999). For example, the

Maritime Business Review
Vol. 3 No. 4, 2018
pp. 414-430
Emerald Publishing Limited
2397-3757
DOI 10.1108/MABR-08-2018-0026

automatic identification system (AIS) has several (in some cases up to seven) key systems dependent upon it, including radar and the chart plotter (Clancy *et al.*, 2017).

Further, the human control of the ship and port is being reduced while the IoT plays an increasing role in ship and port governance, surveillance and monitoring systems (Ingham, 2014). The state-of-art ship technology minimizes traditional navigation and communication systems and the role of officers and engineers of modern merchant ships is deferred to monitoring (Fitton *et al.*, 2015).

This increased automation and the decrease of human intervention on ships and in ports provides fertile ground for security breaches. Cybersecurity on ships and in ports now becomes of paramount importance (Fitton *et al.*, 2015). Cyberspace is a:

> Global domain with the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Radgowski and Tiongson, 2014).

> Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities developing capabilities to disrupt, destroy, or threaten the delivery of essential services (dhs.gov/topics/cybersecurity, 2017).

Security issues and potential of cyberattacks have several facets, but their economic impact on the shipping industry and port operations is huge. For example, the USA is strongly dependent on maritime transport, with 90 per cent of all export-import goods transported by water (George, 2013). The maritime trade is so crucial that any obstruction in the global supply chain eventually causes catastrophic problems in both a national and the global economy (Masala and Tsetsos, 2015).

A cyberattack can mislead ship as to its direction or as to the location of the port. For example, in 2016, two US Naval ships were misled via a cyberattack in the Persian Gulf (King, 2016). Another example is the hacking into the Port of San Francisco Electronic Information System, "moving the port" in cyberspace twenty miles north which became problematic in the foggy weather (Kramek, 2013). An uncontrolled or misled ship can interfere with essential maritime traffic in a waterway. Depending on the time the waterway is not functional and/or the amount of damage caused by the interference, critical goods may not arrive intact and on time. This lack of product supply impacts not only retail market items but also emergent needs including medicine, fuel and food.

Security of the waterways may seem as merely a safety problem. However, it is much more than the safety circumstance. The side effects of disasters caused by a hacked port system or deluded on-board ship system include environmental threats. Serious damage resulting in closure of trade ways leads to complications including shifting of long-term trade and shipping routes and may require rebuilding the infrastructure such as locks and dams as well as commercially established networks. The key to security of the waterways is agility and constant paradigm shifting to outmaneuver those who do the maritime transportation system (MTS) harm (Radgowski and Tiongson, 2014).

As the internet becomes more and more part of port operations and as the internet enters all commercial ships beginning in 2017, the AIS aboard ships will be increasingly more vulnerable to cyberattacks. Ship owners and port directors will have to make decisions on cybersecurity. They must be a balance of the cost and strength of enhancement of cybersecurity with the increased complexity on the ship and in the port of these enhanced systems. This balance is a "wicked problem." A wicked problem is one where the planning for adverse events such as a security breach is difficult or impossible to solve because of

incomplete, contradictory, and changing requirements that are often difficult to recognize. This "wicked problem" context forces port managers and shipping companies to view decisions made on security in terms of mitigation and minimization of the extent and duration of the negative consequences associated with major disruptions. There is no ability to fully solve a wicked problem such as cybersecurity because wicked problems are multilayered and persistent. These problems represent a constellation of linked problems embedded in the fabric of multiple perceptions of the problem and potential solutions.

This paper addresses the "wicked problem" of maritime cybersecurity breaches by trying to identify any inconsistencies in two AIS receiver systems used by ships through a unique methodology known as "Ask, JOAN." JOAN is the acronym for Joint Operational Authenticity Network. Cybersecurity experts have stated that joint authentication is an excellent tool for enhancing security, something which will be explained further in Methodology. We test the potential cyber breaches with the methodology of "Ask, JOAN" by verifying the AIS identification and location data of ships obtained in the Port of Houston using JAMSS America, Inc.'s proprietary ship movement data collected from the Space Station Project and comparing the data collected through the Port of Houston AIS Harborlights system. Knowing whether ships and ports are receiving credible identification and positioning data is vital for safety and security.

> In order to address port and ship resilience planning, this research proposes a conceptual framework addressing this wicked problem which focuses on understanding the complex driver of risks to ports and ships, understanding core infrastructure vulnerability of ports, understanding the functional vulnerability of ports including broad risk elements such as workforce and other economic elements, and addressing mitigation strategies. [. . .] The objective is to help port authorities, regional transportation agencies in which ports are located, and other associated ship stakeholders minimize the extent and duration of major disruptions, and to bring the ports' operating systems back to pre-event levels. [. . .] Decision-making and policy-making approaches must be altered under the "wicked problem" context, emphasizing that the problem cannot be solved overnight but can be mitigated overtime with the collaboration of stakeholders (Ghareghozli *et al.*, 2016).

This paper continues as follows: Section 2 discusses the current state of literature in the area of maritime cybersecurity and the wicked problem framework. Section 3 discusses the methodology for "JOAN" verification and the sample selected of ships in the Port of Houston. Section 4 discusses the results of the sample using "Ask, JOAN." Section 5 discusses strategies of this "wicked problem" for port and ships to balance the "wicked problem" of enhance cybersecurity measures. Section 6 reports the conclusions and implications for managers.

2. Maritime cybersecurity and the "wicked problem"

There are cyber vulnerabilities throughout the MTS. Many of which are caused by the industrial control systems (ICS) embedded in the system accessed through the internet (Volpe, 2013). Cybersecurity vulnerabilities can be exploited by hostile agents and the consequences of which include disabling vessels, closing navigational channels or incapacitating cargo terminals disrupting the global supply chain (Volpe, 2013).

Given the increasing frequency of cyberattacks in the maritime domain, cyber assets in need of protection first and foremost encompass:

- critical digital traffic/communication systems;
- critical information/databases;

- automated terminal and vessel systems; and
- critical infrastructures (Masala and Tsetsos, 2015).

Although the maritime industry assets have been largely mechanical with the major threat being corrosion, the maritime environment is not immune to the disruptions from digital and internet communication and technology (Fitton *et al.*, 2015). For example, the maritime community is not cyber resilient and has no specific guidelines or responses in place to deter or prevent a major cyberattack on the USA (Hayes, 2016). Indeed, the research from Direnzo *et al.* (2015) has called attention to the seriousness of the cyberattacks in the maritime sector and to the fact that there is little or no knowledge about the vulnerabilities. Brand new research by Van Niekerk (2016) shows that the maritime sector is the most affected among all transport modes in number of incidents reported in the period studied. Still, as per Van Niekerk (2016) the main impacts in the maritime sector are related to operation disruption and loss of data confidentiality.

To address maritime cybersecurity and the vulnerabilities to the cyber maritime infrastructure, we review the current literature. We categorize the literature in four ways. First, we address the challenges due to the nature of the industry, i.e. numbers and sophistication level of user and stakeholders interacting in a seaport. Second, we look at the literature on maritime legal issues as they relate to cybersecurity. Third, we review how the industry assesses cybersecurity risk. Fourth, we follow the evolution of automation in maritime critical infrastructure and how this presents an increasing opportunity for cyber threats.

The nature of the industry provides many challenges particularly with many operators and users. A terminal operator may be concerned about a large number of local agents, ships and operators that have shared access to key backend systems (Jensen, 2015). This shared access inadvertently gives users an ability to penetrate the terminal operators overall corporate systems. For example, in the Port of Houston oil company terminal operators are concerned over the potential of ships not in their own fleet accessing corporate data through the systems in the terminal. In addition to shared access, each user may have their own cyber infrastructure platforms which may interfere with the terminal operators' platform (Jensen, 2015). Burton (2016) notes that cooperation between influential players provide cybersecurity shared norms and assists with combating cyberattacks and maritime situational awareness. Further, Odderstol (2014) notes that community approach to maritime cyber resilience where maritime facilities join together and take advantage of mutual technical assistance. Nagurney and Shukla (2016) confirm the cooperation models for cybersecurity.

This community approach is the only way to address the malware threat. Maritime control systems or navigation technologies have been impacted by malware. For example, an oil rig off the coast of Africa tilted and a control system was brought to a standstill during a relocation of a rig due to malware infections (Csorba and Husteli, 2014). Further, GPS "spoofing" (sending false signals to a vessel's navigation system) can change the direction of a vessel. This weakness in the AIS system can be exploited with a $100 off-the-shelf radio kit (Csorba and Husteli, 2014). The community approach such as cybersecurity auditing can address weakness by involving all parties in the cyber network (Csorba and Husteli, 2014).

The maritime legal issues as they relate to cybersecurity are complex. The advent of more automation and internet usage in the maritime environment brings a fundamental change in the way commerce is done and communication is accomplished. Stahl (2011) states "Acts of cyberaggression, like piracy, are carried out in an environment where

jurisdiction is unclear." Attacks do not typically occur in a place (cyberspace) where a nation may have criminal jurisdiction. Further, the current role of government tends to emphasize technological measures and awareness raising (Van Eeten *et al.*, 2006).

International maritime law as well as country maritime regulation currently falls short of addressing cybersecurity. For example, the International Ship and Port Facility Code and the USA Maritime Transportation Security Act of 2002 "do not make specific references to cybersecurity, which remains a major concern within the critical infrastructure of [the USA] (Shah, 2004). Currently, there is an attempt to address industry guidelines on cybersecurity aboard ships intended to be applied by shipowners, managers and seafarer to mitigate maritime cybersecurity risk. At the 96th session of the Maritime safety Committee of the International Maritime Organization, interim guidelines on maritime cyber risk management are make public. The recommendations include guidance on adopting best practices developed by industry groups (BIMCO, 2016), and that organizations should adopt a risk management framework to identify, protect, detect, respond and recover from cyber threats (IMO, 2016).

Further, the 58th session of the International Maritime Organization (IMO) Sub-Committee on Safety of Navigation agreed to the development of guidelines for the harmonization of e-navigation testbeds. The e-Navigation Underway 2013 Conference (January 2013) identified the need for a body to coordinate the harmonization of testbed results. The conference concluded that IALA could consider taking on this role and submit its results to the IMO. IALA stands for International Association of Marine Aids to Navigation and it is a non-for-profit, international technical association. (IALA, 2013).

In assessing cyberattack risk in the USA, the US Coast Guard is the sector-specific agency working on the maritime transportation part of the cybersecurity initiatives across agencies (Johnson, 2014). It is their job to provide institutional knowledge and specialized competencies (Parker and Gray, 2014). The maritime industry is not well aware of the Support Anti-Terrorism by Fostering Effective Technology (SAFETY) Act. It provides some protections for liability from cyberattacks (Dickman *et al.*, 2014).

How the maritime industry assesses and reacts to cybersecurity risk has also been evaluated by the European Network and Information Security Agency (ENISA) in 2011.

> Some key findings are: (1)Maritime cyber security awareness is currently low to non-existent, (2) Due to the complexity of Information and Communication Technology (ICT), it is a major challenge to ensure adequate maritime cyber security. A common strategy and development of good practices for the technology development and implementation of ICT systems would ensure "security by design" for all critical maritime ICT components. (3)As current maritime regulations and policies consider only physical aspects of security and safety, policy makers should add cyber security aspects to them. (4)A holistic, risk-based approach and assessment of maritime specific cyber risks, as well as identification of all critical assets is recommended. (5)The International Maritime Organization together with the EU Commission and the [other] Member States should align international [. . .] policies in this sector. (5)Better information exchange and statistics on cyber security can help insurers improve their actuarial models, reduce risks, and offer better contractual insurance conditions for the maritime sector. Information exchange platforms should be also considered. (Cimpean *et al.*, 2011).

The evolution of the automation in the maritime industry can be seen in the cyber-physical control systems, traffic control, logistics, network operations and safety management that represent the tools to keep the increasingly interconnected global economy effective, profitable and efficient (Masala and Tsetsos, 2015). The use of automated systems in maritime critical infrastructure for ports (terminal automation) and ships (vessel automation) is increasing and, as a result, the opportunity for cyber vulnerabilities is also

increasing (Wilshusen, 2015). Some commenters note that awareness about cybersecurity in the maritime sector has been comparatively low verses other transportation sectors (Göge and Enge, 2015). Further the upgrading critical communication, navigation and operational components on bridges and infrastructure are slower in seaports than in certain other industrial sectors (Göge and Enge, 2015).

Cyber security of the entire supply chain is also a rising risk (Polemi and Papastergiou, 2015). In fact, the research from Khan and Estay (2015) has identified that cyber resilience and cyber risk is a complete new topic in the supply chain research agenda. One of their main conclusion points was that there are no specific frameworks to deal with cyber resilience problems in this industry and thus, they provide relevant insights for both academicians and industry members to tackle the problems of cyberattacks. In the case of Boyes (2015), the author built up on the supply chain literature by investigating the cybersecurity attributes that affect cyber resilience using a Parkerian hexad as a model. The author argues "achieving cyber-resilience will involve a holistic approach to security, given that purely technical solutions are unlikely to address the breadth of potential threats and vulnerabilities." (2015, p. 33).

In both cases, Boyes (2015) and Khan and Estay (2015) are not dealing with port or maritime supply chain, but their conclusions and recommendations are valid for our study. Vessels, along with ports, are susceptible to attacks, especially in navigation and identification systems (Newberry, 2014), because these systems are more integrated and complex (Odderstol, 2014). For example, a mere USB stick plugged into a vessel's local area network could cause the Electronic Chart Display and Information System to be compromised.

Cybersecurity breaches in the maritime industry often cover other nefarious acts such as smuggling of drugs (Klocker, 2015). Also, maritime security focus has been on terrorism and piracy and not cyberattacks. The focus on cyber has been more recent. Originating from accident investigation, safety aspects also concentrate on the infrastructure for prevention of environmental pollution and accident mitigation, such as ship collisions and vessel survivability, rather than cybersecurity for the network-operated, information and communication technology systems on which the safety systems rely (Masala and Tsetsos, 2015). Further, insurance for these security risks is not addressed in many maritime policies (Klocker, 2015).

Newberry (2014) groups the potential threats to the maritime infrastructure into five categories: national governments, terrorists, industrial spies and organized crime groups, hactivists (politically active hackers) and hackers. The main issue is that with more automation there are less people available for vigilance. There have been several incidence to date including the Port of Antwerp attacks to hack systems to identify drug filled containers (Newberry, 2014).

There is a great deal of consternation over the lack of preparedness of the industry and infrastructure in the literature. Some analysts note that the maritime industry is somewhere between 10 and 20 years behind the curve (Caponi and Belmont, 2015). The unique challenges of maritime cybersecurity include the issues with securing vessels at sea, together with the shore based infrastructure supporting this industry, in particular, the cyberattacks possible on maritime-related systems for navigation, propulsion and cargo (Jones *et al.*, 2016). The Electronic Data Interchange standards exist for the individual transportation sector, but the standards are not compatible across all modes of transportation, and authentication protocols are not keeping up with the standard or threats (Wong, 2015). Furthermore, pirates exploit cybersecurity weaknesses in the maritime industry (Frodl, 2012).

Industry is trying improve, but both state and private actors still need to address the emerging risks and vulnerabilities in a holistic manner (Masala and Tsetsos, 2015). For example:

> The Europe's e-Maritime initiative focuses primarily on the shore-based facilitation and on the development of electronic technology, processes and services to facilitate the flow of goods over sea, and consequently the ships that carry these goods to and from and around Europe. The European Commission supports the development of applications for administrations, ship operations, ports/terminals, transport logistics and improving life at sea and promoting seafaring" (Morrall *et al.*, 2016).

However, as systems are developed for efficiency, not much focus has been on the vulnerabilities that these systems cause.

Further, the US Department of Homeland Security (DHS) has launched the Critical Infrastructure Cyber Community (C3 or c-cubed) voluntary program, which is a public/private partnership that aligns critical infrastructure owners and operators with resources to help them use the cybersecurity framework and manage their cyber risks (Odderstol, 2014). DHS also does a cyber resilience review (CRR) which is a nontechnical assessment that evaluates an organization's operational resilience and cybersecurity practices (DHS, 2017).

Additionally, DHS has adopted continuous diagnostics and mitigation program which focuses on, for the MTS, protecting end-point devices, making sure that users only have access to the information for which they are authorized, and rapidly identifying and mitigating the cybersecurity issues and threats (Goldstein and Kneidinger, 2014). Furthermore, DHS is working with each transportation sector to improve cybersecurity standards on ICS (Kaiser, 2013). "Cybersecurity and physical security are increasingly interconnected. Consequently, close collaboration among cyber analysts and physical security professionals is essential for maritime transportation and other critical infrastructure sectors" (Liu *et al.*, 2014).

Cyber resilience in the MTS is preparing for, withstanding evolving threats and hazard and recovering rapidly from disruptions (Volpe, 2013). The term "port resiliency" has specific meaning in maritime cybersecurity. Preventing loss and returning to normal operations as quickly as possible involves:

- identifying key cyber assets;
- assessing the threat, vulnerabilities and consequences from a cyber-attack;
- inventorying cybersecurity assets;
- inventorying hard assets protecting cyber assets;
- planning and training;
- possessing and being able to deploy resources to recover from an attack; and
- establishing and communicating across the community affected (Danos, 2014).

There is also an understanding that technology alone cannot save a port from an attack. Systems used to monitor other systems may need human audits regularly. Furthermore, many ports patch older systems to more modern undermining the newer systems (Konon, 2014).

Port cyber resilience leads to the discussion of the "Wicked Problem." Gharehgozli *et al.* (2016) best discusses the concept or the "wicked problem" and port resilience:

> Protecting ports from the impact of adverse events, considering all stakeholders and variables involved, is a "wicked problem." A wicked problem is one where the planning to address adverse events is difficult or impossible to solve because of incomplete, contradictory, and changing requirements that are often difficult to recognize. Wicked problems are generally seen as complex,

open-ended, and intractable (Head, 2008). They can be defined in several ways, and have multiple characteristics (Camillus, 2008). Past decisions, historical trends, and current industry knowledge may not be useful in addressing wicked problems compared to other events (Rittel and Webber, 1973; Koelsch, 2014). Wicked problems are influenced by many economic, social, and political factors, and biophysical complexities: and the cause and effect of these factors and complexities are difficult to determine (Batie, 2008; Koelsch, 2014).

The wicked problem context has not been widely adopted in management. This may be due to the fact that wicked problems are viewed as unsolvable because of their complexity (Rittel and Webber, 1973). However, wicked problems can become better mitigated with proper identification of issues, requirements, and constraints (Koelsch, 2014). The port is a conglomeration of many stakeholders in an ever changing environment. According to Roberts (2000), in such a situation, the helpful mitigations to cope with the wicked problem are collaborative, authoritative (vesting responsibility), and completive (pitting different points of view). Generally, the problem of protecting the port is mitigated through the measure of resilience which has become an essential concept in the field of crisis management and critical infrastructure protection (Boin and McConnell, 2007; De Bruijne, 2006; De Bruijne and Van Eeten, 2007). Multiple definitions in the literature exist regarding the concept of resilience (Manyena, 2006; Moteff, 2012). Some authors break resilience down into four dimensions (Bruneau *et al.*, 2003; MCEER, 2008; Zobel, 2011; Gibson and Tarrant, 2010): (1) Technical resilience, the ability of the organization's physical system; (2) Organizational resilience, the capacity of crisis managers to make decisions and take actions; (3) Economic resilience, the ability of the entity to face the extra costs; (4) Social resilience, the ability of society to lessen the impact of a crisis. Alternatively, some authors set the following characteristics as the main features of resilience (Bruneau *et al.*, 2003; MCEER, 2008; Zobel, 2011): robustness, redundancy, resourcefulness, and rapidity. Finally, Labaka *et al.* (2011) define resilience as the system's ability to reduce the probability of failure, the consequences from failure and the response and recovery time. Following these studies, we define resiliency as the port's ability to resume normal operations at pre-disruptive performance levels after a disruptive adverse event. In addition, port resiliency includes a port's ability to maintain normal operations and performance over a long period of change such as sea level rise. One of the key elements in this regard is learning from past experience.

Port and ship decision-makers require quality theoretical analysis, highly innovative assessment methodologies, and insightful empirical experiences to identify the best practices, plans, and appropriate policies to effectively develop and adopt resilience measures to minimize adverse impacts on ports (Ng and Becker, 2015).

This conceptual framework can contribute to the maritime transportation industry's ability to perform at optimal levels as rapidly as possible after cyberattack. This impact will ripple through all transportation nodes. The ability to mitigate delays caused by adverse events allows supply chains, individuals, and firms to continue operating as efficiently as possible. The main objective in creating this framework is to aid port and ship stakeholders tools to prevent and mitigate cyberattacks (Ghareghozli *et al.*, 2016).

To complicate the "wicked problem" further, there is generally an emphasis on external threats. There is the potential danger posed by a disgruntled, malicious, or traitorous employee (O'Connell, 2014). The threat from such employee can be to maritime infrastructure, technology and security.

3. Methodology of testing cybersecurity and the JOAN system

The prevailing theme in addressing cybersecurity threats today is dual authentication. We begin to address mitigating the "wicked problem" of cybersecurity in ports and on ships

through testing these of systems and developing strategies to improve the systems. We do this by testing the receipt of data from the AIS for a given ship from two receiving systems. Designs of many maritime cybersecurity systems strongly rely on electronic sensing and data exchange. To build resilience in these security systems, joint situational awareness can enhance joint decision making with regard to a security event (Gunther, 2015). What does this mean? As stated above, community and cooperation make maritime cybersecurity systems more resilient. Ask, JOAN is an acronym for Joint Operational Authenticity Network, a method of dual authentication. The Ask, JOAN methodology is a system of cybersecurity that utilizes a form of dual authentication and relies on joint situational verification from more than one cyber system to confirm what is actual going on physically in a port.

In the Ask, JOAN methodology in this paper, we confirm a ship's location in the Port of Houston through AIS but using two different reception systems. The aim of this process to complete dual authentication is to crosscheck and verify the data collected on the ground by area pilots to that collected by NASA's (NASA: National Aeronautics and Space Administration) International Space Station (ISS). We utilized a manual method to search in an operation similar to taking physical inventory, thereby not solely relying on an electronic inventory system. We manually reconcile the differences in an attempt to isolate and further investigate the inconsistencies. This process begins by taking physical data collected from the ground and attempting to match it with NASA's data collected by the International Space Station to match the outputs. We successfully match one ship's journey, but only up until the anchorage area outside of the Port of Houston. Upon only being able to track until this point we further examine the systems and methods of data collection in place. Further research needs to be explored to determine where the inconsistencies arose in the NASA's collection systems, and the port systems, and the users of the AIS systems on the ships to determine the root cause of the inconsistencies.

We begin to address mitigating the "wicked problem" of cybersecurity in ports and on ships through testing of systems and developing strategies to improve the systems. We do this by testing the receipt of data from the AIS for a given ship from two receiving systems. Designs of many maritime cybersecurity systems strongly rely on electronic sensing and data exchange. To build resilience in these security systems, joint situational awareness can enhance joint decision making with regard to a security event (Gunther, 2015). What does this mean? As stated above, community and cooperation make maritime cybersecurity systems more resilient. The Ask, JOAN methodology is a system of cybersecurity which rely on joint situational verification from more than one cyber system to confirm what is actual going on physically in a port.

In the Ask, JOAN methodology in this paper, we confirm a ship's location in the Port of Houston through AIS but using different reception systems. In a period from October 2016 to January 2017, data were gathered globally from NASA's ISS payload and regionally by ground-based systems for analysis of tens of thousands of data points daily regarding ship movements. The ISS travels at an orbital speed of 17,700 miles per hour at an altitude of 225 miles above the earth's surface. Dynamic and static data collected can be affected by payload position, weather, atmospheric conditions, signal strength and ability to match corresponding IMO number, AIS recognition number, and ship name, among other factors. AIS is an important system because it is a system designed to provide a ship's own position and course to neighboring ships to prevent collision. Further, it impacts many of the bridge systems on a ship. Gunther (2015) describes the use and vulnerabilities of the AIS:

> The [ship's] position can either be determined using GPS or using multisensory receiver. Additionally, AIS may also be used by coastal systems to mark the location of buoys, rocks, or shallow waters, so-called Aids to Navigation (AtoN). In this case, the information is transmitted to a centralized installation. Finally, AIS marks locations of ships in distress or of men over board. The associated equipment is called AIS Search and Rescue Transmitter (AIS-SART). The risks for manipulation of the AIS is: The ship is in anoth804er location. The ship is not the ship it transmits that it is. The ship disappears from all receivers. The ship's signal is hijacked. The AIS signal is confused potentially causing collisions.

The manipulation to the AIS system is often "spoofing." Spoofing occurs when either the authentic AIS is overlaid with a signal of greater power and of different content to capture the receiver or the AIS is simply jammed by generating a cluster of false AIS messages and create a new message at another time delay and/or frequency (Gunther, 2015).

We approach the testing of the cybersecurity system in this paper by verifying information from the AIS system by comparing to receiver systems for the same ship's AIS signal. We cannot check in this study whether the signal transmitted from the ship has been tampered. Other AIS vulnerabilities include the AIS websites insecurity, radio frequency transmissions insecurity and spoofing the signal (Middleton, 2014).

It is always possible that the AIS monitoring system disappears due to cutting or reducing electrical power on the ship. Further, when electrical power is manipulated the AIS system may send the wrong information. For example, TX A and M University training ship showed a false heading on the AIS system this past year while underway in the Gulf of Mexico. The reason for the false reading was determined to be low/incorrect voltage to the AIS system. Further, many of the systems on the ship are integrated into the AIS system (Clancy *et al.*, 2017).

As stated above, the maritime industry has seen exactly how critically important proper operations can be and the tragic results failures to do so yield. The International Maritime Organization states:

> As a result of the attack on the USS Cole, the events of Sept. 11, 2001 and the suicide bombing of the oil tanker Limburg, the IMO held a Diplomatic Conference on Maritime Security in December 2002. At the conference, it adopted a number of measures aimed at enhancing the security of ships and port facilities. In addition to the creation of the well-known ISPS Code, the conference also included a modification to SOLAS Regulation XI-1/3 to require ships' identification numbers to be permanently marked in a visible place either on the ship's hull or superstructure." This measure does not specifically address cyber threats. There is guidance on cyber in the interim guidelines released in 2016 (See above). Further, SN.1/Circ.289, Guidance on the Use of AIS Application-Specific Messages, June 2, 2010, IBR approved for § 164.46 addresses AIS systems.

Upon establishment of these new regulations, continuous improvement processes are encouraged. One of the primary methods successfully used and replicated across other sector systems to protect and secure cyber systems is that of dual authentication. Ask, JOAN is a form of dual authentication.

The dual authentication process used here is as follows:

- First, we gather ship location data from October 2016 to January 2017 from two sources – the JAMSS America Inc. proprietary global AIS system and the Port of Houston proprietary "Harborlights" port tracking AIS system.
- Second, we randomly select 50 vessels reported in the JAMSS system as present in the Greater Houston area, including Freeport, Galveston, Texas City, Sabine,

Matagorda, Brownsville and Corpus Houston Christi and note time. Each report reflects the IMO numbers of the respective vessels.

- Third, we match the vessels to the Harborlights system using the IMO numbers between various reports while cross-checking certain days.
- Fourth, we then widened the search to entire fleets of vessels. Randomly selecting December 1-December 7, 2016, we compare movement of a large tanker fleet. We track ships' voyages and began plotting their respective courses.
- Fifth, we repeated Step 4 with a randomly selected passenger ship fleet over the entire month of November 2016. The Greater Houston area does host passenger vessels.
- Sixth we plot the courses of the vessels based on the information provided by the JAMSS and compare it to the Harborlights system.

4. The results of ask JOAN

Under Steps 2 and 3 of methodology, no matches are identified. Under Step 4, the entire tanker fleet appears to encompass 20 ships. Of this fleet, one single ship is identified in both JAMSS and Harborlights. We continued to track the ship for its reported course in the JAMSS system which initially showed the ship off the coast of Rio de Janeiro on November 19 and ended with it off the coast of Houston on December 5.

Under Step 5, we search the selected passenger ship fleet noting that the entire passenger fleet appears to encompass seven ships. Of this fleet, two matches are found in both JAMSS and Harborlights.

These findings require further inquiries and investigation into why the data do not match with more consistency in these reports. Informal interviews with a US State Maritime Academy reveals the practice of turning down the power to the AIS system while in port (Clancy *et al.*, 2017). This leads to a reduction in fuel used; however, the AIS is only visible is a shorter range such as three miles, making reliance of the system spotty.

To secure the ships, our ports and our maritime logistics chain, we must be able to properly identify ship movements to ultimately authenticate their presence. We cannot tell from this study whether the inconsistencies are due to cyber problems or crew practices. Policies of the use of AIS in ports may need to be addressed.

JOAN as a system used here goes further to address the needs of AIS system reliance in ports. Whether this tool is instrumental in blocking cyberattacks remains to be seen. Dual authentication, however, is only as effective as their proper use of the system. Without proper use, overall security may be compromised.

As cybersecurity concerns are brought to the forefront of the maritime industry, it is imperative that employees operate according to the regulations put in place to protect ports and ships. Two of the key components to successfully navigating high traffic waters such as a port are proper utilization of the AIS system and accordingly, the user operating it as effectively as possible. It is important that the vessel not misuse the system by powering it down, putting it in mooring mode or dropping the signal power, thus diminishing the ability of the ship to be detected, monitored and ultimately verified.

This study shows that the inability to accurately match data on a more regular occurrence has resulted in the need for additional research, as this may be a security deficiency resulting in weak port resiliency. Vulnerabilities in the cyber identification

system are yet unknown. Further, the costs associated with this unknown ship cybersecurity can lead to poor decisions on ships and in ports.

5. Strategies for the "wicked problem" and the enhancement of maritime cybersecurity

The "wicked problem" of mitigating maritime cybersecurity has been largely unaddressed. Most of the world's largest ports have only limited cybersecurity strategies or cyber incident response plans in place, while the involved organizations have yet to establish company–wide cyber risk awareness programs (Masala and Tsetsos, 2015).

The transportation industry can improve cybersecurity through the common framework of risk assessment, management, and sharing experience with other stakeholders (Wong, 2015). The community approach still affords the best option. Borrowing from the financial sector, all firms should consider developing their respective cybersecurity programs in eight areas; staff training; cyber intelligence; governance and risk management for cybersecurity; cybersecurity risk assessment; technical controls; incident response planning; vendor management; and cyber insurance (FINRA, 2015). The US Department of Homeland Security has developed a national plan aimed at maritime governance in cybersecurity through achieving maritime domain awareness (Bivens, 2014). However, Heymann *et al.*, 2016 notes that although many studies have identified cyber risk in maritime shipping, most have not taken the critical (and expensive) next step of actually identifying the vulnerabilities present in these systems.

The complexity of the systems makes them extremely vulnerable. Much emphasis has been focused on the cyber infrastructure overlooking the software vulnerability including the code and remediation measures. The IMO has focused on high level recommendations. More is needed on low level in-depth vulnerability assessment (Heymann *et al.*, 2016). Further, Heymann *et al.* (2016) develop a first principle vulnerability assessment methodology where software vulnerabilities are emphasized.

Generally, the most effective solutions to protecting seaport cyber infrastructure and practices does not involve new approaches or strategies, but instead focus on rigorously applying known methodologies (Liu *et al.*, 2014). Again, the community approach should be emphasized. The focus should be on device and application configuration, monitoring, establishing steps for incident response, training and enforcing usage policies and watching trends and being prepared (Liu *et al.*, 2014). Further, it is the threat within, those with access that should be considered in all solutions.

A potential strategy to address the community approach to cybersecurity resilience is the resilience adoption curve first purport by Rothrock (2017). Rothrock emphasizes that to make your cyber systems more resilient an organization must:

- understand the entirety of the cyber infrastructure impacted by the organization;
- establish benchmarks for the system;
- measure current activity frequently again those benchmarks;
- detect anomalies; and
- response immediately to the anomalies detected.

Similar to the evaluation of risk as a function of threat, vulnerability and impact, the tension between the level of security, the cost of security and the complexity of use in the port or on the ship of cyber systems is a key factor is dealing with maritime cybersecurity. Clearly, e-navigation systems, AIS, Global Navigation Satellite System (GNSS) and other positioning systems save lives and cargo (Gunther, 2015).

Cooperation between the public and private sector is needed to identify threats and address solutions (Kolko, 2015). In the USA, partners with the government addressing risk and vulnerabilities of cyber infrastructure security and resiliency include the Chamber of Shipping of America, the American Association of Port Authorities and American Bureau of Shipping (Volpe, 2013).

Another enhancement to cybersecurity in the maritime industry are the Electro Technical Officers. The IMO has approved the training of an electronics training officer for deployment on ships. The 2010 International Convention on Standards, of Training, Certification and Watchkeeping for Seafarers (STCW) – Manila Amendments introduce standards for training Electro Technical Officers (ETO). These officers will address the needs of the ship with regard to hardware and software maintenance for automated systems and sophisticated electrical systems particularly on cruise ships (Masala and Tsetsos, 2015). This officer will further be expected to be the first line of defense in a cyberattack, thus making ships more cyber resilient (Jensen, 2015).

6. Conclusion and implication for managers

This research proposes a conceptual framework addressing this wicked problem which focuses on:

- understanding the complex driver of risks to ports and ships;
- understanding core infrastructure vulnerability of ports;
- understanding the functional vulnerability of ports including broad risk elements such as workforce and other economic elements; and
- addressing mitigation strategies.

The AIS system can be verified while underway via other trustworthy ships through cooperative communication. Thus, the use of the community for cybersecurity is an important mitigation of the "wicked problem." Sharing of data through old fashion radio communication between ships may be a way to overcome some of the challenges of digital data. The wherewithal of crew members in celestial navigation can also check overreliance on cyberspace. Automation may serve efficiency but may risk security.

However, the best way to mitigate most of the vulnerabilities of AIS systems is to use more than one system to identify vessels and location (Middleton, 2014). Celestial navigation is now being taught again at the US Naval Academy. An alert crew and a diligent captain and harbor pilot can address a cyber threat through good seamanship.

Managers of maritime organizations need to understand the use of digital information in the community. Verification of information from multiple sources through dual authentication such as Ask, JOAN can be useful and enhance security. Knowing whether cybersecurity is working is a "wicked problem" mitigated by cooperation among all stakeholders in the industry using best practices.

References

Batie, S.B. (2008), "Wickedness and applied economics", *American Journal of Agricultural Economics*, Vol. 90 No. 5, pp. 1176-1191.

BIMCO (2016), "Baltic and International Maritime Council. Cyber security seminar", available at: www.bimco.org/training/categories/security

Bivens, D. (2014), "Maritime governance: designed with security in mind", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Boin, A. and McConnell, A. (2007), "Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience", *Journal of Contingencies and Crisis Management*, Vol. 15 No. 1, pp. 50-59.

Boyes, H. (2015), "Cybersecurity and cyber-resilient supply chains", *Technology Innovation Management Review*, Vol. 5 No. 4, p. 28.

Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O'rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A. and Von Winterfeldt, D. (2003), "A framework to quantitatively assess and enhance the seismic resilience of communities", *Earthquake Spectra*, Vol. 19 No. 4, pp. 733-752.

Burton, J. (2016), "Cyber-attacks and Maritime situational awareness evidence from Japan and Taiwan", *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*.

Camillus, J.C. (2008), "Strategy as a wicked problem", *Harvard Business Review*, Vol. 86 No. 5, p. 98.

Caponi, S.L. and Belmont, K.B. (2015), "Maritime cybersecurity: a growing threat goes unanswered", *Intellectual Property and Technology Law Journal*, Vol. 27 No. 1, p. 16.

Cimpean, D., Meire, J., Bouckaert, V., Vande Casteele, S., Pelle, A. and Hellebooge, L. (2011), "Analysis of cyber security aspects in the maritime sector", *European Network and Information Security Agency*.

Clancy, E., Coonrod, J., Fossati, K., Putty, S. and Sullivan, E. (2017), Interview performed in February 2017.

Csorba, J. and Husteli, N. (2014), "Securing your control systems: overcoming vulnerabilities", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Danos, A. (2014), "Building port resilience: how cyber attacks can affect critical infrastructure", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

De Bruijne, M.L.C. (2006), "Networked reliability: institutional fragmentation and the reliability of service provision in critical infrastructures", Doctoral dissertation, Delft University of Technology, TU Delft.

De Bruijne, M. and Van Eeten, M. (2007), "Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment", *Journal of Contingencies and Crisis Management*, Vol. 15 No. 1, pp. 18-29.

Dickman, D., Locaria, D.N. and Wool, J. (2014), "Reducing cyber risk: marine transportation system cybersecurity standards", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Direnzo, J., Goward, D.A. and Roberts, F.S. (2015), "The little-known challenge of maritime cyber security", *International Conference on Information, Intelligence, Systems and Applications*, July, 1-5.

DHS – Department of Homeland Security (2017), "Critical infrastructure cyber community voluntary program (C3VP)", available at: www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience (accessed 24 January 2017).

FINRA (2015), "Financial industry regulatory authority. Cybersecurity", available at: www.finra.org/industry/cybersecurity (accessed 24 January 2017).

Fitton, O., Prince, D., Germond, B. and Lacy, M. (2015), *The Future of Maritime Cyber Security*, Lancaster University, Lancaster, Lancashire.

Frodl, M.G. (2012), "Pirates exploiting cybersecurity weaknesses in Maritime industry", *National Defense*, Vol. 96 No. 702, p. 22.

George, R. (2013), *Ninety Per cent of Everything*, Metropolitan Books, New York, NY.

Gharehgozli, A.H., Mileski, J., Adams, A. and Von Zharen, W. (2016), "Evaluating a 'wicked problem': a conceptual framework on seaport resiliency in the event of weather disruptions", *Technological Forecasting and Social Change*, Vol. 121, pp. 65-75.

Gibson, C.A. and Tarrant, M. (2010), "A 'conceptual models' approach to organisational resilience", *The Australian Journal of Emergency Management*, Vol. 25 No. 2, p. 6.

Göge, D. and Enge, H.C. (2015), *Look-Out-2016 Maritime Domain Cyber: Risks, Threats and Future Perspectives*, Lampe & Schwartze KG, Bremen.

Goldstein, E. and Kneidinger, M. (2014), "Shifting the paradigm: the DHS continuous diagnostics and mitigation program", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 714.

Gunther, C. (2015), "Design of maritime cyber security systems", *Look-Out-2016 Maritime Domain Cyber: Risks, Threats and Future Perspectives*, Lampe & Schwartze KG, Bremen.

Hayes, C.R. (2016), "Maritime cybersecurity: the future of national security", Doctoral dissertation, Naval Postgraduate School.

Head, B.W. (2008), "Wicked problems in public policy", *Public Policy*, Vol. 3 No. 2, p. 101.

Heymann, E., Miller, B.P., Alghazzawi, M.J. and Incertis, D. (2016), "Addressing the cyber-security of Maritime shipping", *2016 European Transport Conference*.

IALA - International Association of Marine Aids to Navigation (2013), "E-Navigation underway 2013 conference report", available at: www.iala-aism.org/content/uploads/2016/06/e-Navigation-Underway-2013_final-report-rev-1.pdf (accessed 24 January 2017).

Ingham, L. (2014), "Drones at sea: automated cargo ships to set sail by 2035", available at: http://factor-tech.com/connected-world/7789-drones-at-sea-automated-cargo-ships-to-set-sail-by-2035/ (accessed 24 January 2017).

International Maritime Organization (2016), "Interim guidelines on cyber risk management", MSC.1/Circ. 1526, Annex 1, 01 June, available at: www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC.1-CIRC.1526%20(E).pdf

Jensen, L. (2015), "Challenges in Maritime cyber-resilience", *Technology Innovation Management Review*, Vol. 5 No. 4, pp. 35-39.

Johnson, M. (2014), "Department of homeland security efforts: Implementing cybersecurity initiatives throughout the federal government", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Jones, K.D., Tam, K. and Papadaki, M. (2016), "Threats and impacts in Maritime cyber security", *Engineering and Technology Reference*, doi: 10.1049/etr.2015.0123.

Kaiser, L. (2013), "Transportation industrial control systems (ICS) cybersecurity standards strategy", *U.S. Department of Homeland Security*, available at: http://trbcybersecurity.erau.edu/files/Transportation-Standards-Plan.pdf

Khan, O. and Estay, D.A.S. (2015), "Supply chain cyber-resilience: creating an agenda for future research", *Technology Innovation Management Review*, Vol. 5 No. 4.

King, J. (2016), "The story you aren't being told about Iran capturing two American vessels", available at: www.mintpressnews.com/the-story-you-arent-being-told-about-iran-capturing-two-american-vessels/212937 (accessed 24 January 2017).

Klocker, G. (2015), "Cyber risks a threats: a demanding challenge for the Maritime industry", *Look-Out-2016 Maritime Domain Cyber: Risks, Threats & Future Perspectives*, Lampe & Schwartze KG, Bremen.

Koelsch, C.J. (2014), "Potential impact of changes in risk assessment to address wicked problems: a case study of British petroleum's assessment strategies", Master's thesis, A&M University, TX.

Kolko, R. (2015), "Countering the maritime cyber threat", *Coast Guard Proceedings*, Vol. 71 No. 56, pp. 55-61.

Konon, J.M. (2014), "Control system cybersecurity: Legacy systems are vulnerable to modern-day attacks", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Kramek, J. (2013), *The Critical Infrastructure Gap: US port Facilities and Cyber Vulnerabilities*, Center for 21st Century Security and Intelligence at Brookings, Washington, DC.

Labaka, L., Hernantes, J., Laugé, A. and Sarriegi, J.M. (2011), "Policies to improve resilience against major industrial accidents", in *International Workshop on Critical Information Infrastructures Security*, Springer, Berlin, pp. 187-199.

Liu, X., Burmester, M., Redwood, W.O., Wilder, F. and Butler, J. (2014), "Zero-day vulnerabilities: what to do when it's too late to prevent an attack", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Manyena, S.B. (2006), "The concept of resilience revisited", *Disasters*, Vol. 30 No. 4, pp. 434-450.

Masala, C. and Tsetsos, K. (2015), "A demanding challenge for the Maritime industry", *Look-Out-2016 Maritime Domain Cyber: Risks, Threats & Future Perspectives*, Lampe & Schwartze KG, Bremen.

MCEER - Multidisciplinary and Multi-Hazard Earthquake Engineering Research Center (2008), *Engineering Resilience Solutions*, University of Buffalo, Buffalo, New York, NY.

Middleton, A. (2014), "Hide and seek: managing automatic identification system vulnerabilities", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Morrall, T., Griffiths, D., Varelas, T., Katsoulakos, T., Koliousis, I., Furió, S., Ferrús, G. and Rødseth, ØJ. (2016), "Seventh framework programme theme 7: transport (including aeronautics) TTG4 e-Maritime: proposals for R&D road map", *Maritime Europe Strategy Action*.

Moteff, J.D. (2012), "Critical infrastructure resilience: the evolution of policy and programs and issues for congress", Congressional Research Service.

Murrison, M. (2016), "Maritime industry slowly embracing potential of IoT", *Internet of Business*, available at: https://internetofbusiness.com/iot-maritime-industry-potential/ (accessed 24 January 2017).

Nagurney, A. and Shukla, S. (2016), "Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability", *European Journal of Operational Research*, Vol. 260 No. 2, pp. 588-600.

Newberry, M.E. (2014), "Maritime critical infrastructure cyber risk: threats, vulnerabilities, and consequences", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Ng, A.K.Y. and Becker, A. (2015), "Port adaptation to the impacts posed by climate change: how can scholars, policymakers and industrial professionals contribute?", *Maritime Economist Magazine*, Fall 2015, pp. 8-14.

O'Connell, S. (2014), "The threat within: Protecting against internal enemies", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Odderstol, T. (2014), "C-Cubed: Increasing cyber resilience, awareness, and managing risk", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Parker, B. and Gray, G. (2014), "The Coast guard and cybersecurity: a legal framework for prevention and response", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Polemi, N. and Papastergiou, S. (2015), "Current efforts in ports and supply chains risk assessment", *10th International Conference for Internet Technology and Secured Transactions*.

Radgowski, J. and Tiongson, K. (2014), "Cyberspace – the imminent operational domain: a construct to tackle the Coast guard's tough challenges", *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, Vol. 71 No. 4.

Rittel, H.W. and Webber, M.M. (1973), "Dilemmas in a general theory of planning", *Policy Sciences*, Vol. 4 No. 2, pp. 155-169.

Roberts, N. (2000), "Wicked problems and network approaches to resolution", *International Public Management Review*, Vol. 1 No. 1, pp. 1-19.

Rothrock, R. (2017), "Keynote: Ray Rothrock", *Proceedings at Cybersecurity of Critical Infrastructure Summit*.

Shah, S.K. (2004), "The evolving landscape of Maritime cybersecurity", *Review of Business*, Vol. 25 No. 3, p. 30.

Smierzchalski, R. (1999), "Evolutionary trajectory planning of ships in navigation traffic areas", *Journal of Marine Science and Technology*, Vol. 4 No. 1, pp. 1-6.

Stahl, W.M. (2011), "The uncharted waters of cyberspace: applying the principles of international Maritime law to the problem of cybersecurity", *Georgia. Journal of International and Comparative Law*, Vol. 40, p. 247.

Van Eeten, M.J.G., De Bruijn, H., Kars, M., Van Der Voort, H. and Van Till, J. (2006), "The governance of cybersecurity: a framework for policy", *International Journal of Critical Infrastructures*, Vol. 2 No. 4, pp. 357-378.

Van Niekerk, B. (2016), "Analysis of cyber-attacks against the transportation sector", in *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities*, IGA Global, Hershey, p. 68.

Volpe (2013), "ICS security in Maritime transportation: a white paper examining the security and resiliency of critical transportation infrastructure", *US Department of Transportation*, No. DOT-VNTSC-MARAD-13-01.

Wilshusen, G.C. (2015), "Maritime critical infrastructure protection: DHS needs to enhance efforts to address port cybersecurity", Government Accountability Office, No. GAO-16-116T.

Wong, K. (2015), "Cybersecurity in transportation", in *Protecting Our Future: Educating a Cybersecurity Workforce*, Vol. 2, LeClair J. (ed.), Hudson Whitman/Excelsior College Press, Albany.

Xia, F., Yang, L.T., Wang, L. and Vinel, A. (2012), "Internet of things", *International Journal of Communication Systems*, Vol. 25 No. 9, p. 1101.

Zobel, C.W. (2011), "Representing perceived trade-offs in defining disaster resilience", *Decision Support Systems*, Vol. 50 No. 2, pp. 394-403.

Further reading

Kuhlman, R. and Kempf, J. (2015), "Finra publishes its 2015 'report on cybersecurity practices'", *Journal of Investment Compliance*, Vol. 16 No. 2, pp. 47-51.

Pedersen, P.V., Petersen, V.A. and Vittrup, J. (1999), "E-Navigation underway 2016", Baltic and International Maritime Council.

United States Government Publishing Office, Code of Federal Regulations (2016), CFR Part 164, available at: www.gpo.gov/ (accessed 24 January 2017).

Corresponding author
Cassia Bomer Galvao can be contacted at: cassiabgalvao@gmail.com