Journal of
Marine Science and Engineering

MDPI

Article

Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS)

Malik Shahzad Kaleem Awan [1] and Mohammed A. Al Ghamdi [2,*]

[1] Cyber Research Department, SMT-Sol, Lahore 54570, Pakistan; shahzad.awan@gmail.com
[2] Computer Science Department, Umm Al Qura University, Makkah 715, Saudi Arabia
* Correspondence: maeghamdi@uqu.edu.sa; Tel.: +966-0-541110063

Received: 10 September 2019; Accepted: 26 September 2019; Published: 2 October 2019

Abstract: The adoption of the global positioning system (GPS) within the marine industry has revolutionized the marine operations by condensing the navigation of a vessel into an integrated bridge system (IBS). An IBS acts as the main command and control of a vessel as it interconnects various digital devices used for navigation in open seas and is also connected to other on-board systems of a vessel e.g., navigation and control, propulsion and machinery management system, cargo management system and safety management system, core infra structure systems, administrative and crew welfare systems, etc. Additionally, it also provides a gateway to the Internet, thus, leaving not only an IBS vulnerable but also all the on-board systems vulnerable to cyber-attacks. We, in this study, have collected historical evidences about various vulnerable digital components in an IBS to better understand the security and privacy challenges associated with the vulnerable IBS components. Our study is the first of its kind that involves collection and review of 59 historical accidents reported in literature and has highlighted various vulnerability patterns, their causes and consequences, with geographical as well as temporal relationships for different vulnerable IBS components. The vulnerabilities of IBS components were reportedly exploited using various cyber-attack techniques e.g., jamming, spoofing, hijacking, etc. This review paper also forms a baseline for future work on vulnerabilities of IBS and maritime cyber security.

Keywords: vulnerability; maritime cyber security; integrated bridge system; cyber attacks; spoofing; hijacking; jamming

1. Introduction

Seas are used by a myriad number of users for commercial, leisure and military purposes. More than 90% of the world trade is carried through seas, as maritime transport is the most cost-effective mean of goods transportation [1]. Generally, general cargo ships, bulk carriers, container ships, auto carriers, tankers, oil industry vessels, etc. are used for goods transportation. In addition to goods transportation, specialist ships, such as anchor handling and supply vessels for oil industry, salvage tugs, ice breakers, cable layers and research vessels, are used for performing specialist activities; fishing vessels are used for fishing in deep seas; while military uses seas for coastguard ships, fireboats, frigates, corvettes, destroyers, amphibious assault ships, aircraft carrier, combat ships, submarines, etc. [1,2]. Apart from the commercial transportation vessels and other specialized ships, cruise ships and ferries for pleasure voyages also use the seas. The presence of such a diverse set of vessels requires navigational information as well as coordination with other nearby vessels, buoys and ports to ensure safer journey from the source to destination points while avoiding collisions and natural disasters.

Traditionally, mariners used Sextant measurement of the altitudes of astronomical objects e.g., sun, moon, stars, planets, etc., during navigation in open seas in order to avoid collisions with other vessels as well as natural disasters. The measurements were then used for laborious calculations to

identify the position of a navigating vessel based on latitude and longitude values [3]. The calculated positions of the vessels using this traditional method had accuracies in terms of miles. With the technological advancements and adoption of the global positioning system (GPS) within the marine industry, the marine operations have been revolutionized. GPS has helped in identifying the position of an object with significant accuracy and has resulted in condensing the vessel navigation operations into an integrated bridge system (IBS). An IBS acts as the main command and control of a vessel as it interconnects various digital devices used for navigation in open seas and is also connected to other on-board systems of a vessel e.g., navigation and control, propulsion and machinery management system, cargo management system and safety management system, core infra structure systems, administrative and crew welfare systems, etc. Additionally, it also provides a gateway to the Internet, thus, leaving not only an IBS but also all the on-board systems vulnerable to cyber-attacks. The US Government Accountability Office (GAO) has also raised security concerns for the maritime critical infrastructure from a range of evolving unaddressed threats [4]. Such behavior of not preparing well for cyber security attacks has also been reported in other industrial control systems, such as the power industry, electric grids, etc., which are well prepared for traditional threats, such as physical attacks, but not cyber security attacks [5]. Thus, need arises for better understanding of IBS and its various vulnerable components, which could be potentially exploited by cyber-attackers.

The main contributions of our work are:

(1) Collection of historical evidences about the vulnerability of IBS components.
(2) Classification of exploitation mechanism of IBS components, i.e., external vs. internal actors.
(3) Understanding the effects of geographical locations on exploitation of IBS components.
(4) Understanding the relationship of vessels' countries and the exploited IBS components.
(5) Investigating the calendar of the proposed cyber-attacks for annual trend analysis.

The rest of the paper is organized into the following sections. Section 2 presents the available literature on maritime cyber security; Section 3 describes our methodology for conducting this review study; a brief description of different digital components of an IBS and the available historical evidences on the vulnerabilities of IBS digital components are given in Section 4; Section 5 has the analyses and discussion on the collected evidences of vulnerabilities of IBS digital components; while Section 6 has the concluding remarks and the future directions of this work.

2. Related Work

The available literature on maritime cyber security domain provides a top-level but scarce information about the domain as the area is still in its infancy. This scarcity of information has hindered an extensive research and development activities in the domain and has thus presented the whole domain as a classified domain with very little information available for researchers, maritime and security experts. We have found that the available literature on maritime cyber security can be broadly classified into three areas: (1) general policy and understanding aspects of maritime cyber security; (2) challenges about maritime port infrastructure and (3) vulnerabilities of a few digital components of an IBS. A commonality found in the reported material on maritime cyber security is that generally the motivations behind cyber-attacks targeting the maritime industry include data theft and ransom, illegal movement of cargo and general disruption in the maritime operations [6]. In this section, we report the studies in the aforementioned three areas of maritime cyber security and present a comparison with our study. An emerging cold war like state between Euro-Atlantic and Sino-Russian countries has resulted in highlighted concerns about maritime cyber security. The North Atlantic Treaty Organization (NATO) Alliance and the Euro-Atlantic have repeatedly accused Russia of creating hostile environment for maritime transport and maritime infrastructure for the European countries in European waters and the Black Sea.

Realizing the challenges in maritime cyber security and the importance of safe and secure general goods transportation through deep seas, the Constanta Maritime University (CMU) has taken an

initiative to train human resources to better understand the issues associated with the maritime cyber security domain. CMU has also launched a new maritime cyber security research initiative at the Black Sea Coast in collaboration with industrial partners to offer degrees in the area of maritime cyber security [7]. Our study covers the maritime cyber security challenges faced in the deep waters during navigation and thus could be utilized by CMU for curriculum development of their degrees. Moreover, the collected evidences and results of our study could be beneficial for CMU to develop various case studies for their degree programs. A study [8] has found that modern port infrastructures tend to be highly dependent on the use of information systems to coordinate with the related agencies, port authorities and other bodies worldwide. Thus, there is a high risk of a cyber-attack on these maritime information systems to steal the maritime data. As the data in modern port infrastructures is shared across multiple ports, the modern information systems used for sharing the data become very critical and important for smooth functioning of the maritime infrastructure. The study [8] has discussed a risk management system, called MITIGATE, that has been developed for managing and protecting the dynamic nature of maritime supply chain IT infrastructure. The collected evidences and analysis also help in identifying the attack paths used in various geographical locations and for different digital components of an IBS.

Maritime Logistics and Supply Chains (MLoSCs), which include ports, maritime authorities, airports, railways, energy providers, banks, maritime logistics and transport companies, act as the blood veins of global trade and economy in the modern era [9]. Unlike [9], which focuses on inland infrastructure our study explores the historical evidences that have affected the maritime operations in deep seas and the disruption has consequential effects on the inland infrastructure mainly in terms of delay or unavailability of goods at ports. The scope of our study is limited to collection and review of existing literature on maritime cyber security as well as on the vulnerabilities of digital components of an IBS, nonetheless, the study can be extended further to develop risk assessment frameworks for marine vessels operating in deep waters.

In multicultural maritime and logistics networks, the biggest challenge lies in the existing methods and tools to dynamically respond to the frequent change of information as well as the lack of efficiently sharing security knowledge over the supply chain [10]. Our study is different than [10] as we have provided a broader overview of the maritime cyber security challenges associated with marine vessels in deep seas. Our work is also the first study of its kind to describe and report the historical evidences of malfunctioning of digital components of an IBS.

Spoofing, hacking and disrupting service availability are identified as the three threat categories normally used by cyber attackers in the maritime industry [11]. Our study has further identified human errors, software misconfigurations and malfunctioning, insiders' threats as well as the state-sponsored activities to hide any illegal or secret activities as the additional threat categories in the maritime industry.

A study found a large number of automatic identification system (AIS) receivers to be significantly insecure and could lead to numerous attack scenarios [12]. We have collected historical evidences of AIS malfunctioning and its consequences. Our study provides a broader view of AIS insecurity in the real-world. A security evaluation study of AIS has been performed using software-defined radios focusing on AIS data leakage that reported several vulnerabilities in AIS [11]. Our study has presented the real-world evidences of identified AIS vulnerabilities during penetration testing. Thus, our study reports the practical implications of reported AIS vulnerabilities of [6].

The available literature on maritime cyber security contains scarce and scattered information on the vulnerability landscape of an IBS. Our study covers this existing knowledge gap in the maritime cyber security domain by first collecting the available information from both maritime domain as well as the cyber security domain, then combining the vulnerability information with real-life evidences and presenting a detailed study of the vulnerabilities of main digital components of an IBS.

3. Methodology

For our study, we collected 59 historical accidental events of marine vessels linked with the malfunctioning of various digital components of an IBS. The data was collected from various publicly available sources, which include research papers, technical reports, white papers from security companies, product documentations, webpages, etc., While reviewing the collected literature, we focused on extracting the information about the vulnerable digital component of IBS, cause of malfunctioning, effect of the malfunctioning, geographical location where the accident event took place, month and year of the accident event, marine vessel ownership, the exploitation mechanism in terms of attack actors i.e., external or internal. We defined the following research questions for our study to get a better insight of the vulnerabilities of IBS digital components.

(1) What are the main IBS components that are vulnerable to any potential cyber-attack?
(2) How significant is each IBS component for ensuring safety of a sea journey?
(3) If uniformity in terms of vulnerability and historical accidents for all IBS components exists or they vary in ranks of vulnerability and number of historical accidents?
(4) What type of mechanism is used for exploitation of an IBS component?
(5) What could be the consequences of a compromised IBS component based on the available historical accidental events?
(6) If a relationship exists between maritime accidents and the ownership of a marine vessel?
(7) If a relationship exists between maritime accidents and the geographical location of the accident?
(8) If a relationship exists between maritime accidents and the month or year?

The extracted information was used to answer our research questions/objectives set out for this study. We used textual explanation, tabular description, graphical charts and an overall general analysis to present our findings and analysis. The results of our study helped us in presenting a broader view of the vulnerability landscape in an IBS environment.

4. Vulnerabilities in IBS Components

The digital nature of IBS components has left an IBS prone to various vulnerabilities, which could be exploited during cyber-attacks. In the following subsections, a description of each component has been presented to highlight its significance for a safer journey of a marine vessel through deep seas along with the collected historical accidental evidences.

4.1. Automatic Identification System (AIS)

4.1.1. Component Description

The automatic identification system is an automatic tracking system used by vessels navigating in open seas. AIS provides information about a ship's identity (name and call sign), type, position, course, speed, heading and position to shore stations, other ships and aircrafts [13]. The information is broadcast at a regular time interval e.g., a ship equipped with class-B-transponder when navigating at a speed of more than 23 knots has to broadcast its position every 5 seconds [11].

4.1.2. Historical Evidences

Despite the significance of AIS in navigation, collision avoidance, search-and-rescue (SAR) operations and traffic monitoring [11], its inherent vulnerabilities in both real-world scenarios as well as controlled experiments have been reported in the literature.

In November 2018, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), in collaboration with U.S. Department of State and the U.S. Coast Guard, stated that disabling the automatic identification system (AIS) is a tactic conducted by some Iranian and Russian vessels in the

Mediterranean Sea carrying petroleum to state-owned and operated ports by the Syrian Government in order to mask their movements and conceal them while heading to Syria [14].

In 2012, fourteen (14) Iranian ships, which were previously registered in the Pacific Island of Tuvalu, have reportedly counterfeited AIS information by flagging themselves to be from Zanzibar, a semi-autonomous island off the coast of Tanzania, during the time of tightened US and European sanctions relating to their nuclear program [15].

It has been reported in 2014 that Somali pirates used online AIS navigational data to identify their potential targets in the Gulf of Aden and using advanced computing techniques either prompted a targeted ship to turn off AIS as well as navigational devices or counterfeited AIS data leading the victims to believe them to be at a different geographical location [16].

In 2014, it has been reported that an Israeli firm, Windward, while analyzing AIS data found that 100 ships counterfeited AIS data and transmitted incorrect locations in one day [16].

An investigation into the sinking of the Sewol Ferry carrying 476 passengers in the sea off Korean's southern coast in April 2014 revealed that Sewol turned off its AIS for an unknown reason before capsizing in the sea. The capsizing resulted in 304 passengers getting trapped inside the ferry and drowned [17].

An experimental study conducted in 2014 identified vulnerabilities of AIS and its proneness to different types of cyber-attacks such as counterfeiting AIS data and disabling AIS communications [11].

Penetration testing of AIS by TrendMicro in 2014 revealed numerous vulnerabilities including, modification of all ship details, creation of ghost vessels, trigger false alerts and modification of signal transmission frequency [6].

In 2014, it was reported that ship owners misused AIS by shutting it down while passing through the Gulf of Aden to avoid Somali pirates so that the pirates should not be able to track the ships and later target/attack them [16].

In July 2013, a North Korean ship, Chong Chon Gang, carrying concealed cargo containing around 240 tons of weapons including two disassembled MiG-21 jet fighters hidden under more than 200,000 Cuban sugar bags reportedly turned off its AIS to hide its trip through the Gulf of Mexico and Panama Canal [18]. The vessel got caught through the Panama Canal.

A study conducted in 2013 found AIS to be vulnerable to closest point-of-approach (CPA) spoofing, which involves faked possible collision leading a ship to get off course [13].

In June 2012, a collision took place between two vessels – Josephine Maersk and Spring Glory. The watch officer on Josephine Maersk through visual observations using binoculars saw another ship—Spring Glory—approaching it at a distance of approximately 2 nautical miles, about five minutes prior to collision and also misunderstood a radio message before the collision of Josephine Maersk with Spring Glory [19].

4.2. Electronic Chart Display and Information System (ECDIS)

4.2.1. Component Description

An electronic chart display and information system is an International Maritime Organization (IMO) compliant computer navigation system and provides navigational charts. The IMO has made it mandatory for all passenger vessels to carry and use an electronic chart display and information system (ECDIS) [20,21]. ECDIS displays navigation-related information [21]; determines the quality of chart data (i.e., paper charts, Electronic Navigational Chart (ENC) or Raster Navigational Chart (RNC) data) [22] and ship's safety depth [21], and [22] apart from its integration with other navigational systems and GPS [21].

4.2.2. Historical Evidences

ECDIS is normally run on a PC having Microsoft Windows XP [20] and has inherent vulnerabilities that make it susceptible to cyber-attacks. It has been reported that an attacker can access and modify ECDIS files and charts [16]. A number of ECDIS-related incidents are reported in the literature:

On 3rd December 2016, a bulk carrier Muros was grounded on Haisborough Sand, 8 miles off the Norfolk coast in the UK due to the poor use of the electronic chart display and information system (ECDIS). There were several safety issues listed in a report related to the improper use of the e-navigation equipment on the ship [23].

An experimental study, reported in January 2014, evaluated the vulnerabilities in ECDIS running on a Windows 7 machine and found that cyber-attacks could result in directory traversals, modification or deletion of ECDIS data by exploiting HyperText Transfer Protocol (HTTP) dangerous methods as well as HTTP header injections. In addition, ECDIS was found to be vulnerable due to an outdated Apache Web Server used by the system [24].

The US Navy reported that incorrect digital charts used in ECDIS resulted in the USS Guardian running aground off the Philippines in 2013 [16]. The digital charts provided by the National Geospatial Intelligence Agency (NGA) were wrong by eight (8) nautical miles and resulted in a grounding of the $227 million minesweeper USS Guardian that also ruined 43,000 square feet of the reef in Philippines [25,26].

A Maltese oil and chemical tanker Ovit ran aground on the Varne Bank in the Dover Strait in September 2013. The investigations revealed improper configuration of ECDIS alarms, insufficient knowledge of using ECDIS as well as the reported incompetence of ECDIS [27].

In early 2012, a ship ran aground off a chartered bank in the Indian Ocean en route from Africa to South East Asia due to significant deficiencies in vessel's passage planning [28].

CSL Thames, a Maltese bulk carrier, ran aground in the Sound of Mull in August 2011 while traveling from Glensanda to Wihelmshaven due to reported failures in ECDIS functionality as a result of misconfiguration in term of setting safety contours, activation of alarms as well as insufficient knowledge of ECDIS by the bridge team [29].

4.3. Global Navigation Satellite System (GNSS)

4.3.1. Component Description

GNSS is a constellation of satellites that transmits timing and positioning data signals from space for navigation applications across the globe [30,31]. Two GNSS: 1) US global positioning system (GPS) [32]; and 2) Russian global navigation satellite system (GLONASS) [33]; are currently in operation with a European navigation system called Galileo [34] is being developed. NAVSTAR (navigation satellite timing and ranging) is another name for GPS by United States [30], and [35]. GPS is used in the maritime industry for position fixing information and it is connected to other electronic devices in an IBS.

4.3.2. Historical Evidences

The loss of GPS signals can result in failure of numerous on-board electronic systems such as AIS, dynamic positioning system, global maritime distress and safety system, etc., and can leave a ship without a positive positional fix [36,37].

On 23rd March 2017, U.S. Maritime Alert 2018-004 A "Possible GPS Interference—Eastern Mediterranean Sea" was issued by the U.S. Maritime Administration to respond to the reports of GPS disruptions and interference from multiple vessels between the Cyprus and Egypt port [38].

North Korea used GPS jamming against South Korean ships, fishing vessels and equipment on land and sea in 2010 and 2016 to create disruption in satellite signals [39,40]. The jamming campaign in March 2016 affected the signal reception of more than 700 ships [39].

In April 2014, the GPS signals of USS Donald Cook, a 4th generation guided missile destroyer, were completely jammed by a Russian Sukhoi Su-24 in the Black Sea using electronic warfare devices [41].

In 2014, a GPS jamming experiment was performed by the UK and Irish General Lighthouse Authority on a vessel called Pole Star. The experiment helped the crew of the Pole Star to understand and get trained in order to respond to a situation when a vessel enters a jamming zone [24].

A research team from the University of Texas used an electronic equipment worth $3000 to take control of an 80 million dollar 210-foot yacht in the Mediterranean Sea in July 2013 [6].

An investigative study conducted in 2005 reported that a 100-watt bulb has 1018 times more powerful signals than that of a GPS satellite signal and can result in a significant interference [42].

The malfunctioning of GPS signals during the journey caused the autopilot mode to incorrectly plan the course and resulted in grounding of Royal Majesty in June 1995 [43].

4.4. Radio Detection and Ranging (Radar)

4.4.1. Component Description

Radar is an object detection system that uses radio waves to determine the range, bearing or velocity of objects [44]. Radar signals are more difficult to jam compared to GPS signals. However, the radar signals could be jammed using advanced techniques [37].

4.4.2. Historical Evidences

Japan's Defense minister condemned the incident of locking of one of its patrol planes by South Korean destroyer's radar on 20th December 2018. This incident brought the relation of both countries to the lowest level. The minister had called it an extremely dangerous action. Japan recorded strong protest over this incident [45].

USS John McCain (named after the Senator John McCain's father and Grandfather), equipped with the advanced Radar, navigation system, GPS, AIS and radio communication. These electronic tools proved deficient when she was struck by a large oil carrier, which was carrying 12000 tons of crude oil on the midnight off coast of Malaysia in 21st August 2017 [46].

The radar signals of USS Donald Cook, a 4th generation guided missile destroyer, were completely jammed by a Russian Sukhoi Su-24 in the Black Sea using electronic warfare devices in April 2014 [41].

4.5. Navigational Telex (NAVTEX)

4.5.1. Component Description

NAVTEX has been designated by IMO to provide navigational and meteorological warnings and forecasts as well as urgent marine safety information to ships [47]. It provides an aid to safer navigation.

4.5.2. Historical Evidences

Following to the completion of Turkish Military exercise "Blue Homeland", a fresh NAVTEX (Navigational Telex) was being circulated to the Greek that a large area of Aegean Sea would again remain inaccessible for eight days from 11th March to 30th April 2019. During this time Turkish forces will conduct military exercises [48].

It was reported in June 2013 that a vessel in Chinese waters caused significant damage to a fish farm by crossing through it. The NAVTEX was not working for some time before the incident took place [49].

A formatting problem in messaging in NAVTEX resulted in failed recording of weather data transmitted from a Greek transmitter, Kerkyra, in 2007 [50].

NAVTEX signals have been reportedly received in a variable manner with signals received at high water but no signals were received at low water. In Summer 2002, cruise from Plymouth to Spanish

Basque country, the signals were not received from the journey onwards from France. The proximity of other radio emission sources adversely affected NAVTEX reception [50].

4.6. Sailing Directions

4.6.1. Component Description

Sailing directions are electronic in nature [20] and are published by the National Geospatial-Intelligence Agency (NGA) to provide planning and routes guides to sailors [51]. They contain the information about time zones, coastlines, ports, harbors, firing areas and search and rescue information [20,51].

4.6.2. Historical Evidences

Pirates attacked the container-carrying ship CONTSHIP OAK on 30th March 2019, at the Bight of Bonny, Gulf of Guinea while the ship was on anchorage. Pirates made four crews kidnap with them. Later on the ship was docked on 31st March to 2nd April at Douala [52].

The Ro-Ro cargo Vessel Neptune Hellas proceeding at the speed of 13.8 knots, collided with 'Nur', a cargo vessel, was travelling at the speed of 8 knots on a southwesterly course towards the Çanakkale strait on 21st March 2018 [53].

It was reported in June 2013 that a vessel in Chinese waters, due to incorrect information about the area, crossed through a fish farm, which was not even detected by the bridge team and resulted in paying compensation for the incurred damages [49].

In April 2008, a German-flagged containership, Pacific Challenger, with a weight of almost 13900 tons was grounded on the white reef while crossing Solomon Sea on its way from Rabaul port to Oro Bay in Papua New Guinea [54].

In 2007, the Louis Cruise liner Sea Diamond was grounded on a Greek rock, which was not shown properly on the area charts used during navigation through the area [54].

In January 2004, a Dutch stone carrier 'Rocknes' loaded with 23,243 tones of gravel and stone capsized in the south of Bergen, Norway after grounding on rocks. The investigation revealed that the charts used by 'Rocknes' were not up-to-date and did not show a shallow patch discovered a few weeks ago during a hydrographic survey [55].

In 1991 on an Australian reef, a bulk carrier Sanko Harvest was grounded and resulted in one of the worst oil spills in country's history due to inaccurate sailing directions as the charts used were not up-to-date [54].

4.7. Position Fixing

4.7.1. Component Description

Position fixing is used to determine the ship position using a variety of visual, traditional and electronic methods [56]. A loss in GPS signals will significantly affect position fixing in maritime navigation [56,57].

4.7.2. Historical Evidences

On 1st July 2017, the UK Government's Marine Accident Investigation Branch (MAIB) discovered that a failure of communications over radio was a main reason in causing a ship collision in the English Channel. MAIB exposed that the bad communication between the Tanker and Bulk Carrier's Bridge teams during an overtaking maneuver in the Dover Strait [58].

The incident report on the grounding of the cruise ship Royal Majesty reported that the disconnection of the GPS cable and antenna resulted in entering the dead reckoning mode in 9th June 1995. The autopilot of the Royal Majesty, thus, was unable to take into account the effects of the wind,

current or sea conditions and showed an incorrect position while the operational conditions in the sea had already resulted in a 17-mile error [43].

4.8. Speed Log

4.8.1. Component Description

Speed log is used to measure the speed of a vessel while navigation through deep waters [59].

4.8.2. Historical Evidences

Speed log faulty has been found in the Cargo ship Louise Auerbach (IMO 9388895) at Kiel Canal between Suchsdorf and the locks in Kiel-Holtenau. The canal was temporally blocked until it got the part replaced in 9th January 2019 [60].

In 24th March 2019, 371 people were evacuated by helicopters. The ship is still moving at a very low speed in the western direction, either under its own power or under tow. It seems like the MB initial surmise was the correct one—VIKING SKY was and most probably, still is, hampered by an anchor or anchors, being yet unable to heave them up. The weather is visibly calming down [61].

The incident report on the grounding of the cruise ship Royal Majesty reported that the disconnection of the GPS cable and antenna resulted in entering the dead reckoning mode in 9th June 1995. The autopilot of the Royal Majesty, thus, incorrectly had the calculated speed value of 12.7 knots from the speed log, which was inconsistent with the manually recorded speed in the bridge log [43].

4.9. Echo Sounder

4.9.1. Component Description

Echo-sounder is a type of sound navigation and ranging (SONAR) device, which uses the sound propagation technique for determining water depth [62].

4.9.2. Historical Evidences

Indian nuclear submarine designed by Russia INS Arihant has suffered major damage due to human error and has not sailed now for more than 10 months. Submarine's propulsion compartment was damaged after water entered it, according to details. An Indian naval source said water rushed in as a hatch on the rear side was left open by mistake while it was at harbor [63].

In February 2009, a Royal Navy nuclear submarine collided with a French nuclear submarine in the middle of the Atlantic Ocean as both the vessels were unable to detect each other. It has been anticipated that the anti-sonar devices hide both the submarines from each other [64].

4.10. Anemometer

4.10.1. Component Description

Anemometer is used for measuring wind speed [65]. The accuracy of the wind speed values depend on the shape and structure of a ship as the ship hull and superstructure could result in distortion of the airflow, which leads to biased wind speed measurements. The World Meteorological Organization (WMO) Voluntary Observing Ship (VOS) program recruits several thousand merchant ships for reporting the current meteorological conditions at the ocean surface and then, after taking care of the bias due to the shape and structure of a ship, estimates and forecasts weather conditions [66].

4.10.2. Historical Evidences

A boat sank and foundered in the middle of storm with killing 17 people in Missouri Lake in July 2018. The anemometer reading was recording 73 mph while the Hurricane-force winds are thought to begin at about 75 mph, which was stated by the National Transportation Safety Board [67].

A large passenger ship while crossing the Atlantic Ocean was affected by a hurricane and the strong winds carried away the vessel's anemometer while one of the radar scanners stopped working. The ship crew was unable to predict the wind speed and plan the journey accordingly. The vessel however arrived safely at the destination after a delay of around 8 hours in February 1997 [68].

4.11. Global Maritime Distress and Safety System (GMDSS)

4.11.1. Component Description

GMDSS has been considered as one of the basic requirements for a maritime vessel to ensure that more lives could be saved at sea during a distress condition [69,70]. Every GMDSS-equipped ship should be able to transmit and receive signals relating to ship-to-ship distress alerts; search and rescue coordinating communications; on-scene communications; maritime safety information; bridge-to-bridge communications; etc. [69].

4.11.2. Historical Evidences

Transas CEO highlighting the importance of the cyber security risk is still persisting for which solutions are to be sought from the satellite operator, service provider and hardware manufacturer. IMO should apply equal standards of compliance use for GMDSS, ECDIS and other bridge equipment to the standard communication network and equipment [71].

GMDSS is vulnerable to cyber-attacks as a malicious firmware, if installed, can allow an attacker to control devices on-board the vessel, deliver false information by spoofing and disrupt communication [69].

4.12. Ship Security Alert System (SSAS)

4.12.1. Component Description

SSAS is provided on a ship for transmitting security alert to relevant authorities in case the ship comes under treat or has been compromised [72].

4.12.2. Historical Evidences

Post the successful attack on Cosco Shipping Line's Long Beach customer service center, Sela commented that though COSCO shut down its connection as a precautionary measure but kept the ships unguided. Vessels systems are attacked by the company's shore based on information technology systems [73].

A cyber-attack can result in disabling the system remotely thereby preventing the vessel from sending alerts in case of an attempted attack; modifying or deleting distress calls and weather warnings and providing false information resulting in changing the planned route [69].

4.13. Voyage Data Recorder (VDR)

4.13.1. Component Description

IMO has made it mandatory for all passenger ships and all other ships over 3000 GRT to carry VDR for assisting in accident investigations [74]. VDR requires date, time, ship's position, speed, heading, bridge audio, communication audio, radar, AIS, depth, main alarms, wind speed, direction, etc. [75].

4.13.2. Historical Evidences

The large ore carrier Stellar Daisy sunk on 31st March 2017, suddenly leaving only two crews alive out of a total of 24. The place of accident was some 1800 nautical miles due west of Cape Town South Africa. After a 10-day search a voyage data recorder (VDR) has been recovered, for this purpose

a remote operated vehicle (ROV) was used. Reason of the accident will be clarified with the help of the VDR [76].

The VDR of EL Faro has been found in the morning of Tuesday (26th April 2016) at the depth of 15,000 feet and about 36 nautical miles northeast of Acklins and Crooked Islands, Bahamas, according to the US National Transport Safety Board (NTSB) [77].

A web article in 2015 stated that VDR has many security holes, which if exploited by attackers could lead to buffer overflow and command injection vulnerabilities [78].

It has been reported in 2015 that an Indian cargo ship's VDR files were overwritten using a USB stick [78].

In August 2008, the voyage data of the European Endeavour was not saved due to misconfiguration of VDR disk capacity and unfamiliarity of operators with the VDR type [79].

4.14. Personal Usage Software

4.14.1. Component Description

The Shipboard network has a gateway to the Internet, which is used for personal Internet usage.

4.14.2. Historical Evidences

The workstation onboard a ship connected to the Internet run Microsoft Windows and Microsoft Office, which have inherent vulnerabilities while a database of identified vulnerabilities is maintained [80].

Similarly, using email on-board could also lead to exploitation of vulnerabilities by cyber-attackers. It has been reported that an SMS sent from one ship to another can successfully exploit vulnerabilities such as multiple backdoors, weak encryption algorithms, insecure protocols and hardcoded credentials that could allow an attacker to remotely take control of the critical communication systems [69].

Facebook has been reportedly used as a pirate intelligence source in the Gulf of Aden [6]. A passenger onboard the vessel uploaded detailed images of the vessel safety measures to a Facebook account. On discovering the activity, the planned course of the vessel was changed before entering the Gulf of Aden in October 2013 [6].

5. Analyses and Discussion

We, in this section, have analyzed the dataset in order to answer the research questions that we had set in our methodology section.

5.1. Ranking of Vulnerable Digital Components of IBS

We collected a total of 59 evidences on the failure or malfunctioning of IBS components. Figure 1 shows the breakdown of the collected evidences. The vulnerability statistics about IBS components revealed that 43% of the collected evidences were related to the three components: AIS, GNSS and sailing directions; which were also considered as the vulnerable components by both maritime and cyber security experts. The remaining 57% of the collected evidence on the maritime accidents due to malfunctioning of IBS digital components showed unawareness of maritime and cyber security experts about the potential consequences of a cyber-attack on IBS digital components other than AIS, GPS and ECDIS. This identified unawareness gap about vulnerable IBS components should be addressed by the relevant stakeholders for making the IBS environment safer and reliable for navigation through deep waters. The most vulnerable component, based on the number of historical incidents and technical reports, was AIS reported in 11 events, which form 19% of the dataset. One of the possible reasons of AIS being the most reported component was its usage for coordination between vessels in deep seas for avoiding collisions and/or chaotic situations at ports. GNSS and sailing directions were found to be the most reported vulnerable components after AIS, as found in the collected evidences, with seven reported incidents for each of the component, representing a share of 12% for each of the digital

component in the dataset. Whilst ECDIS ranked fourth with 10% of the dataset collected for this study. Figure 1 presents the percentages of each IBS components based on the collected data in this study.

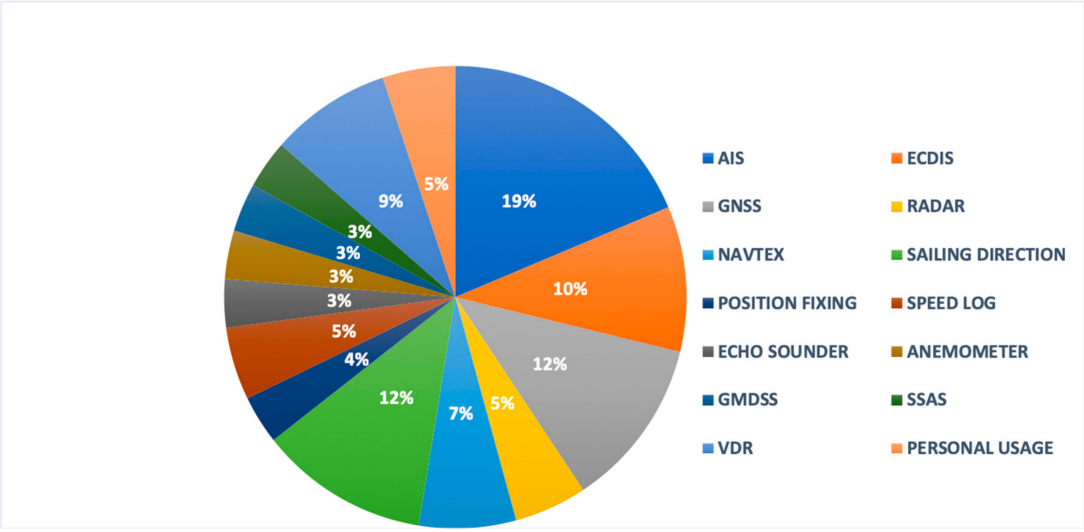

Figure 1. Composition of collected maritime vulnerability evidences.

The composition of collected evidences also provided a ranking of most vulnerable IBS components and how they have resulted in a maritime disaster. The statistics could be used by the experts to better understand the broader vulnerability landscape in an IBS environment.

5.2. Exploitation Mechanisms for IBS Digital Components and Consequences

We investigated the exploitation mechanisms for each IBS digital component as well as the reported consequences to better understand the vulnerability landscape of IBS digital components. Considering AIS vulnerabilities, the historical evidences collected for this study suggested that AIS was deliberately exploited by the crew members to: 1) Hide the real identity of the vessel and instead use a faked one, as in the case of Iranian vessels [15]; 2) carry illegal concealed cargo as in the case of a North Korean ship [18] and 3) avoid attacks from pirates as in the case of ships passing through the Gulf of Aden [16]. The investigation reports about the sinking of the Sewol Ferry [17] and collision between Josephine Maersk and Spring Glory [19] revealed that AIS was not used before the incidents happened. The groundings of the USS Guardian [16,25,26], CSL Thames [29], OVIT [27] and another ship route to South East Asia [28] were mainly attributed to incorrect digital charts being loaded and used by the ECDIS and then planning the route for navigation. An experimental study [24] showed exploiting ECDIS using software-based cyber-attacks while hardware-based exploitation of ECDIS using USB or CD is also possible [20,24].

The historical evidences [6,24,39,41,42] of jamming the GPS signals highlight the use of jamming devices to interrupt or disable GPS communication. One report [43] highlighted the breakdown of connection wires to the GPS antenna that resulted in unavailability of GPS signals. Radar signals could be jammed using electronic devices as in the incident of USS Donald Cook [41]. It is also envisaged that an insider could also disrupt the radar services by turning it off or manipulating its functionality configurations.

NAVTEX signals are subject to disruption due to interference from other electronic devices as reported in [50]. Further, a misconfiguration of NAVTEX as in [50] or unavailability of the service as in [49] could be attributed to crew negligence and could be accounted as an insider's threat for not properly working out the settings or availability of NAVTEX.

The electronic nature of sailing directions and the historical evidences of using outdated charts for navigation [49,54,55] could be associated with human negligence as well as a failure of software to get

the charts updated on time. Position fixing mainly depends on GPS signals [56], thus, a problem in GPS or by a malicious action of an insider could result in failure and accidents.

Speed log is mainly vulnerable to an insider's threat as an inappropriate speed value selected during maneuvering or for auto-pilot control can result in the vessel getting uncontrolled during maneuvering and lead to an accident. The dependency on GPS signals for calculating speed could result in accidents [43].

Echo sounder could be jammed using jamming devices such as anti-sonar, as reported in the incident of collision between two nuclear submarines [64]. While the performance of an anemometer depends on the shape and structure of a ship, thus, the measurement accuracy is based on the position of anemometer on the ship. Further an exposure to hurricanes and strong winds can result in failure of the anemometer [68]. This makes it mainly vulnerable to insider's threats.

GMDSS depends on the GPS signals for communication, which makes it vulnerable to hardware-based cyber-attacks [69]. Further, a malicious firmware installation could lead to exploiting GMDSS vulnerabilities through software-based cyber-attacks [69]. A malicious insider can also exploit the vulnerabilities of GMDSS by directly interacting with it. Similar to GMDSS, SSAS is vulnerable to both hardware and software-based cyber-attacks [69] apart from insider's threats.

VDR has been reportedly vulnerable to software-based cyber-attacks [78] as well as negligence or malicious use by an insider [78,79]. On-board personal usage of software and communication services is vulnerable to software-based cyber-attack exploitation [69,72] as well as the exploitation resulting from an insider [6].

5.3. Vessel Ownership, and Geographical and Temporal Relationship with Maritime Accidents

We have linked the vessel ownership and temporal aspects with the maritime accidents occurring due to vulnerable IBS components to investigate the significance or relationship of vessel ownership and time with the maritime accidents. In addition, the geographical location of the event is linked to highlight a wider view of the accident and identify the maritime accident hotpots occurring due to failure, malfunctioning, hacking or compromised IBS component as a result of a cyber-attack. We filtered our dataset by excluding experimental studies and penetration testing reports to only consider real-world historical evidences. This filtering resulted in 35 historical accidental events.

Table 1 presents the disruption of the occurred accidents based on the country that owned the vessels. United States of America (USA) has been affected by the cyber-attack based on the collected data in this study with 17.1% of the total accidents, followed by South Korea and United Kingdom (UK) and with 11.4% and 8.6% for each of them respectively (see Figure 2).

Table 1. The distribution of the accidents based on the vessels' own country.

-	Country	No. of Accidents	Accident Rate (%)	-	Country	No. of Accidents	Accident Rate (%)
1	USA	6	17.1	13	Spain	1	2.9
2	South Korea	4	11.4	14	China	1	2.9
3	UK	3	8.6	15	Germany	1	2.9
4	India	2	5.7	16	Australia	1	2.9
5	Hong Kong	2	5.7	17	Netherland	1	2.9
6	North Korea	1	2.9	18	Greece	1	2.9
7	Somalia	1	2.9	19	Norway	1	2.9
8	Cyprus	1	2.9	20	Panama	1	2.9
9	Italy	1	2.9	21	France	1	2.9
10	Liberia	1	2.9	22	Japan	1	2.9
11	Turkey	1	2.9	23	Iran	1	2.9
12	Denmark	1	2.9				

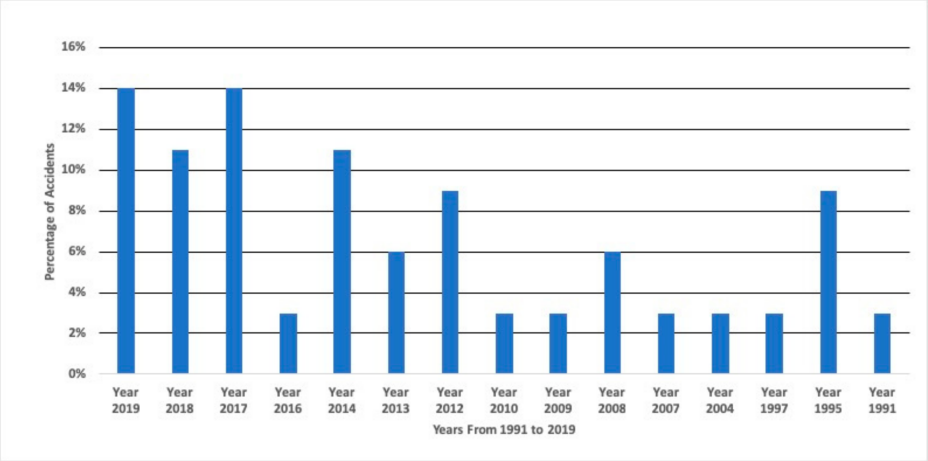

Figure 2. The distribution of accidents' percentages based on years.

The percentage distribution of the attacks based on both years and months based on the data are shown in Figures 2 and 3 respectively.

Figure 2 shows that the percentages of the incident have increased dramatically during the last three years 2017, 2018 and 2019 with 39% of the total incidents studied in this work. 2014 has also a significant increase in the number of proposed accidents comparing with the previous years.

Figure 3 states that the month of March and April are both active in terms of the numbers of incidents based on the collected data that has been conducted in this study with 22% and 19% of the total incidents respectively while there are no accidents, which have been reported during the months of May and December. The locations of the reported accidents that happened based on the IBS components are shown in Figure 4. The figure presents that 15% of the proposed incidents took place in the Atlantic Ocean. While near the coast of South Korea, there were 12% of the accidents based on the collected data in this paper. The Middle East area also has a significant number of the attacks with 15% (9% in Mediterranean Sea, 3% in Red Sea and 3% in Arabian Gulf).

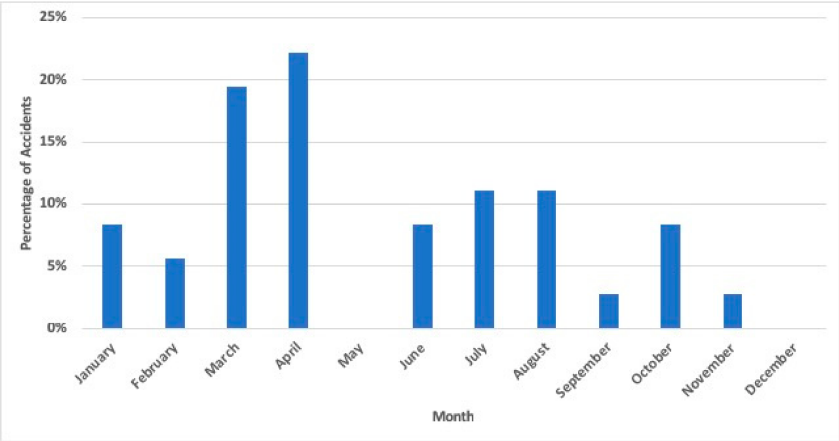

Figure 3. The distribution of accidents' number based on months.

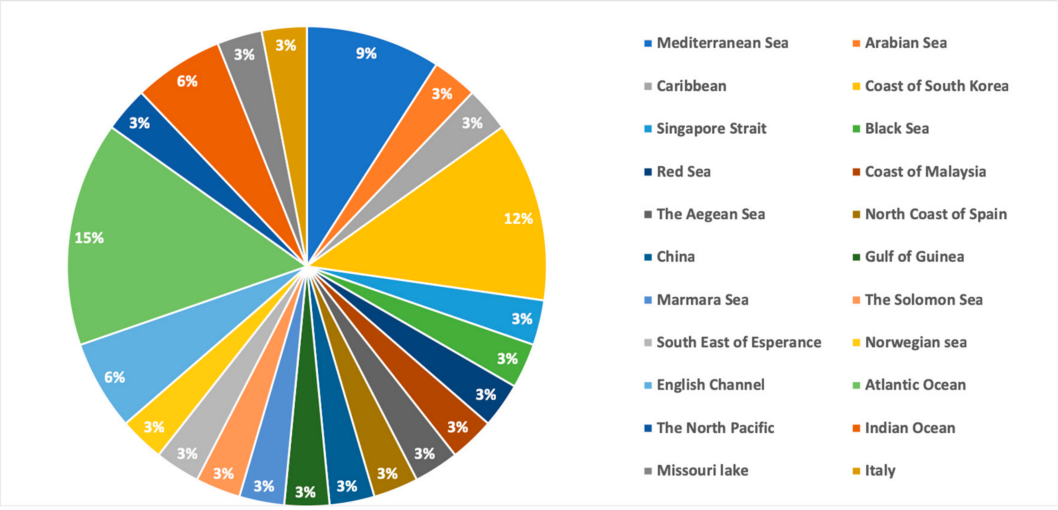

Figure 4. The locations of maritime accidents due to vulnerabilities of integrated bridge system (IBS) digital components.

6. Conclusions and Future Work

We conducted a review study to gather historical evidences about the vulnerability of IBS components. The historical evidences were collected from various publicly available resources mainly from the maritime domain as the maritime cyber security domain is still in its infancy and the available information even in the maritime cyber security domain is very little and only presents a top-level view. We found that 43% of the collected evidences were related to the vulnerabilities in AIS, GNSS and sailing directions, which should be the main concerns of experts for safer navigation through deep seas. Atlantic Ocean and the South Korean coastal areas have reportedly got 27% of the total historical evidences of failure, malfunctioning or of compromised IBS digital components. We also found that approximately 37% of the total cyber-attack are targeting three countries i.e., USA with 17.1%, South Korea with 11.4% and UK with 8.6%. Added to this, 38% of the cyber-attacks have been reported during the last three years (2019, 2018 and 2017). The months of April and March appeared to be when the most cyber-attacks took place with 23% and 20% of the total accidents respectively. We envisage that understanding a broader vulnerability landscape as described in this study will help experts take appropriate measures to make navigation safer through deep waters. Our future work includes exploring the vulnerabilities of IBS components in more detail and identifying the consequences of a compromised component in case of a cyber-attack to develop various attack paths. Further, the work would be specialized for identifying and handling various challenges associated with the different maritime industry stakeholders.

Author Contributions: The authors together collected the data, analyzed data, wrote the manuscript and reviewed the draft.

Funding: This research received no external funding.

Acknowledgments: The authors acknowledge the technical support provided by SMT-Sol and Umm Al Qura University for the research study.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Classifications of Different Naval Ships—A NAVY Guidelines. MiGFlug.com Blog. Available online: https://migflug.com/jetflights/classifications-of-naval-vessels/ (accessed on 30 September 2019).
2. Part Four—Types of Maritime Vessels. Industrial Workers of the World. Available online: http://www.iww.org/unions/iu510/yardbird/yardbird4.shtml (accessed on 30 September 2019).

3. Bhattacharjee, S. Understanding Marine Sextant—Principles, Readings and Maintenance. Available online: https://www.marineinsight.com/marine-navigation/what-is-a-sextant/ (accessed on 30 September 2019).
4. Wilshusen, G.C. *Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity*; GAO Report (No. GAO-16-116T); U.S. Government Accountability Office: Washington, DC, USA, 2015. Available online: http://www.gao.gov/products/GAO-16-116T (accessed on 30 September 2019).
5. Line, M.B.; Zand, A.; Stringhini, G.; Kemmerer, R. Targeted attacks against industrial control systems: Is the power industry prepared. In Proceedings of the 2nd Workshop on Smart Energy Grid Security, Scottsdale, AZ, USA, 7 November 2014; ACM: New York, NY, USA, 2014; pp. 13–22.
6. CyberKeel. *Maritime Cyber-Risks*; CyberKeel: Copenhagen, Denmark, 2014; Available online: https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf (accessed on 30 September 2019).
7. Zăgan, R.; Raicu, G.; Pazara, R.H.; Enache, S. Realities in Maritime Domain Regarding Cyber Security Concept. *Adv. Eng. Forum* **2018**, *27*, 221–228. [CrossRef]
8. Polatidis, N.; Pavlidis, M.; Mouratidis, H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Comput. Stand. Interfaces* **2018**, *56*, 74–82. [CrossRef]
9. Kalogeraki, E.; Papastergiou, S.; Mouratidis, H.; Polemi, N. Article A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments. *Appl. Sci.* **2018**, *8*, 1477. [CrossRef]
10. Kalogeraki, E.; Apostolou, D.; Polemi, N.; Papastergiou, S. Knowledge management methodology for identifying threats in maritime/ logistics supply chains. *Knowl. Manag. Res. Pract.* **2018**, *16*, 508–524. [CrossRef]
11. Balduzzi, M.; Pasta, A.; Wilhoit, K. A security evaluation of AIS automated identification system. In Proceedings of the 30th annual computer security applications conference, New Orleans, LA, USA, 8–12 December 2014; pp. 436–445.
12. Guarnieri, C. Security Street. Spying on the Seven Seas with AIS. 29 April 2013. Available online: https://community.rapid7.com/community/infosec/blog/2013/04/29/spying-on-the-seven-seas-with-ais (accessed on 30 September 2019).
13. Balduzzi, M.; Wihoit, K.; Pasta, A. Hey captain, where's your ship? Attacking vessel tracking systems for fun and profit. In Proceedings of the 11th annual Hack in the Box (HITB) Security Conference in Asia, Kuala Lumpur, Malaysia, 14–17th October 2013; Available online: https://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf (accessed on 30 September 2019).
14. Sanctions Risks Related to Shipping Petroleum to Syria. OFAC Releases Advisory to the Maritime Petroleum Shipping Community. 22 November 2018. Available online: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_shipping_advisory_11202018.pdf (accessed on 30 September 2019).
15. Bockmann, M. Iran Oil Tankers Said by Zanzibar to Signal Wrong Flag. Bloomberg. 19 October 2012. Available online: http://www.bloomberg.com/news/2012-10-19/iranian-oil-tankers-said-by-zanzibar-to-be-signaling-wrong-flag.html (accessed on 30 September 2019).
16. Northern California Area Maritime Security Committee. Cyber Security Newsletter. 23 April 2014. Available online: https://www.sfmx.org/wp-content/uploads/2017/03/Cyber-Security-Newsletter-2014-1.pdf (accessed on 30 September 2019).
17. Suh, J. The failure of the South Korean National Security State: The Sewol Tragedy in the Age of Neoliberalism. *Asia Pac. J.* **2014**, *12*, 1.
18. North Korean Ship Tests the Waters near America's Shores–Forbes. Available online: http://www.forbes.com/sites/claudiarosett/2014/07/13/north-korean-ship-tests-the-waters-near-americas-shres/#362d0950492a (accessed on 30 September 2019).
19. Marine Accident Report May 2013. Spring Glory/Josephine MÆrsk Collision on 5 June 2012, Danish Maritime Accident Investigation Board. Carl Jacobsens Vej 29, DK-2500 Valby, Denmark. Available online: https://dmaib.dk/media/9128/spring-glory-and-josephine-maersk-collision-on-5-june-2012.pdf (accessed on 30 September 2019).
20. Dyryavyy, Y. *Preparing for Cyber Battleships–Electronic Chart Display and Information System Security*; Technical Report; An NCC Group Publication: Manchester, UK, 2014; Available online: https://www.nccgroup.trust/uk/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/ (accessed on 30 September 2019).

21. ECDIS. What Is ECDIS. Available online: http://www.ecdis-info.com/about_ecdis.html (accessed on 30 September 2019).
22. Charts, ECDIS, International Maritime Organization (IMO). Available online: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/Charts.aspx (accessed on 30 September 2019).
23. Wingrove, M. Accident Report: Ship Damaged due to Incorrect ECDIS Use. 20 October 2017. Available online: https://www.marinemec.com/news/view,accident-report-ship-damaged-due-to-incorrect-ecdis-use_49611.htm (accessed on 30 September 2019).
24. CyberKeel. Security Risks and Weaknesses in ECDIS Systems. Marine Cyberwatch. 1 October 2014. Available online: http://www.cyberkeel.com/images/pdf-files/Oct2014.pdf (accessed on 30 September 2019).
25. Daily Mail Reporter. The $277 million minesweeper set for the scrap heap: U.S. Navy's wooden ship stuck on reef in the Philippines dismantled and hauled away. Available online: http://www.dailymail.co.uk/news/article-2299808/USS-Guardian-Wooden-ship-stuck-reef-Philippines-dismantled.html (accessed on 30 September 2019).
26. Clark, C. Untold Tale behind USS Guardian Reef Grounding: NGA's Map Was Wrong by 8 Miles. *Defense Industry News*. 26 July 2013. Available online: http://breakingdefense.com/2013/07/untold-tale-behind-uss-guardian-reef-grounding-flawed-nga-map-data (accessed on 30 September 2019).
27. Ovit: Moody Crew, Dodgy ECDIS, Inexperience and a Shy Master. 26 November 2014. Available online: http://maritimeaccident.org/2014/11/ovit-moody-crew-dodgy-ecdis-inexperience-and-a-shy-master (accessed on 30 September 2019).
28. Vandenborn, Y.; Bell, R. Standard Safety Special Edition: ECDIS Assisted Grounding, Technical Report, The Standard for service and security, London, UK. 2015. Available online: http://www.standard-club.com/media/1738472/standard-safety-special-edition-ecdis-assisted-grounding-april-2015.pdf (accessed on 30 September 2019).
29. CSL Thames Grounding: Not Enough ECDIS Training. 1 March 2012. Available online: http://maritimeaccident.org/2012/03/csl-thames-grounding-not-enough-ecdis-training (accessed on 30 September 2019).
30. Global Navigation Satellite Systems Tutorials, (2011), The University of Nottingham. Available online: https://www.nottingham.ac.uk/grace/documents/resources/glossariestutorials/globalnavigationsatellitesystems.pdf (accessed on 30 September 2019).
31. EGNOS Portal. What Is GNSS? Available online: http://www.egnos-portal.eu/discover-egnos/about-egnos/what-gnss (accessed on 30 September 2019).
32. Garmin—What is GPS? Available online: http://www8.garmin.com/aboutGPS (accessed on 30 September 2019).
33. Information and Analysis Center for Positioning, Navigation and Timing. Available online: https://www.glonass-iac.ru/en (accessed on 30 September 2019).
34. Galileo Is the European Global Satellite-Based Navigation System—European GNSS Agency. Available online: http://www.gsa.europa.eu/galileo/why-galileo (accessed on 30 September 2019).
35. Howell, E. Navstar: GPS Satellite Network. Available online: http://www.space.com/19794-navstar.html (accessed on 30 September 2019).
36. CyberKeel. GPS Jamming as Industry Threat. *Marine Cyberwatch*. 1 October 2014. Available online: http://www.cyberkeel.com/images/pdf-files/Oct2014.pdf (accessed on 30 September 2019).
37. Lanziner, H. A low-cost solution to GPS vulnerabilities. *Technol. BC Shipp. News* **2014**, 50–51. Available online: https://rntfnd.org/wp-content/uploads/BC-Shipping-News.pdf (accessed on 30 September 2019).
38. Madden, C.R. ECDIS: What Happens When the GPS Signal Goes Away? 26 March 2018. Available online: https://www.maritime-executive.com/blog/ecdis-what-happens-when-the-gps-signal-goes-away (accessed on 30 September 2019).
39. Kim, J.; Saul, J. South Korea Revives GPS Backup Project after Blaming North for Jamming [Reuters]. Available online: http://www.reuters.com/article/us-shipping-southkorea-navigation-idUSKCN0XT01T (accessed on 30 September 2019).
40. National PNT Advisory Board comments on Jamming the Global Positioning System—A National Security Threat: Recent Events and Potential Cures 4 November 2010. Available online: http://www.gla-rrnav.org/pdfs/interference_to_gps_v101_3_.pdf (accessed on 30 September 2019).

41. What Spooked the USS Donald Cook So Much in the Black Sea? US-Russian Incident. Voltaire Network. 8 November 2014. Available online: http://www.voltairenet.org/article185860.html (accessed on 30 September 2019).
42. Hoey, D.; Benshoof, P. *Civilian GPS Systems and Its Potential Vulnerabilities*; Technical Report: AAC/PA09-01-05-348; U.S. AIR FORCE: Washington, DC, USA, October 2005; Available online: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA440379 (accessed on 30 September 2019).
43. The Grounding of the Royal Majesty, Chapter 8. Available online: https://ti.arc.nasa.gov/m/profile/adegani/Grounding%20of%20the%20Royal%20Majesty.pdf (accessed on 30 September 2019).
44. Richards, M. *Fundamentals of Radar Signal Processing*, 2nd ed.; McGraw-Hill: New York, NY, USA, 2014.
45. Lee, J. South Korea Denies Warship Locked Fire-Control Radar on Japanese Plane. 24 December 2018. Available online: https://www.independent.co.uk/news/world/asia/south-korea-japan-warship-patrol-plane-lock-target-navy-a8698291.html (accessed on 30 September 2019).
46. Baraniuk, C. Why It's Not Surprising that Ship Collisions Still Happen. 22 August 2017. Available online: http://www.bbc.com/future/story/20170822-why-its-not-surprising-that-ship-collisions-still-happen (accessed on 30 September 2019).
47. NAVTEX (Navigational Telex) Forecasts. Available online: http://www.nhc.noaa.gov/pdf/TAFB_navtex.pdf (accessed on 30 September 2019).
48. Kampouris, N. Turkey Issues New NAVTEX, Blocking Large Area in Aegean. 11 March 2019. Available online: https://greece.greekreporter.com/2019/03/11/turkey-issues-new-navtex-blocking-large-area-in-aegean (accessed on 30 September 2019).
49. The Nautical Institute. Tales of the unexpected, The Navigator, Passage Planning Thinking Ahead for a Successful Voyage. Free publication in association with the Royal Institute of Navigation. Available online: https://www.nautinst.org/uploads/assets/uploaded/907a9ad0-5fb2-4c32-92f6d0875219577c.pdf (accessed on 1 October 2019).
50. Singleton, F. NAVTEX Problems in More Detail–Franks–Weather–The Weather Window. Available online: http://weather.mailasail.com/Franks-Weather/Navtex-Reception-Problems-And-Cures-Detailed (accessed on 30 September 2019).
51. Sailing Directions Planning & Enroute Guides for Foreign Waters. Available online: http://www.offshoreblue.com/navigation/sailings.php (accessed on 30 September 2019).
52. Voytenko, M. Container Ship Attacked, 4 Crew kidnapped, Gulf of Guinea. 2 April 2019. Available online: https://www.fleetmon.com/maritime-news/2019/25737/container-ship-attacked-4-crew-kidnapped-gulf-guin (accessed on 30 September 2019).
53. Saftey4sea. Ships Collision in Marmara Sea Linked to Poor Lookout. 28 March 2019. Available online: https://safety4sea.com/ships-collision-in-marmara-sea-linked-to-poor-lookout (accessed on 30 September 2019).
54. Couttie, B. The Case of the Unwatched ZOCs, Maritime Accident Casebook. Available online: http://maritimeaccident.org/library2/the-case-of-the-unwatched-zocs (accessed on 30 September 2019).
55. The Pilot Online Edition–Blog Archive–Rockness Disaster. Available online: http://www.pilotmag.co.uk/2004/10/15/rockness-disaster (accessed on 30 September 2019).
56. Sonnenberg, G. *Radar and Electronic Navigation*, 6th ed.; Butterworth-Heinemann: Oxford, UK; Available online: https://www.elsevier.com/books/radar-and-electronic-navigation/sonnenberg/978-0-408-01191-4 (accessed on 30 September 2019).
57. Brcic, D.; Kos, S.; Zuskin, S. Navigation with ECDIS: Choosing the Proper Secondary Positioning Source. *Int. J. Mar. Navig. Saf. Sea Transp.* **2015**, *9*.
58. Wingrove, M. Communications Breakdown Causes Ship Collision. 26 April 2018. Available online: https://www.marinemec.com/news/view,accident-report-communications-breakdown-causes-ship-collision_51571.htm (accessed on 30 September 2019).
59. CVE (Common Vulnerabilities and Exposures). Chapter 3: Speed Measurement. Available online: http://sbs-on-web.com/downloads/TSS/Speed_logs_description.pdf (accessed on 19 April 2019).
60. Admin. Marine Accident Round-Up: 14th January 2019. 14 January 2019. Available online: https://insurancemarinenews.com/insurance-marine-news/marine-accident-round-up-14th-january-2019 (accessed on 30 September 2019).

61. Voytenko, M. Cruise Ship VIKING SKY in Distress: Happy End Mar 24 Update. 23 March 2019. Available online: https://www.fleetmon.com/maritime-news/2019/25605/cruise-ship-viking-sky-distress-1500-people-board (accessed on 30 September 2019).
62. National Oceanography Centre. Research Ships. Available online: https://noc.ac.uk/facilities/ships (accessed on 30 September 2019).
63. Allison, G. India's first nuclear missile submarine crippled as sailor leaves hatch open. UKDJ Network. Available online: https://ukdefencejournal.org.uk/indias-first-nuclear-missile-submarine-crippled-sailor-leaves-hatch-open (accessed on 30 September 2019).
64. Nuclear Subs Collide in Atlantic. BBC News. 16 February 2009. Available online: http://news.bbc.co.uk/1/hi/uk/7892294.stm (accessed on 30 September 2019).
65. Taylor, P.; Kent, E.; Yelland, M.; Moat, B. The Accuracy of Wind Observations from Ships. Available online: http://eprints.soton.ac.uk/69541/1/Taylor_etal_coadsKiel95.pdf (accessed on 30 September 2019).
66. Moat, B.; Yelland, M.; Molland, A.; Pascal, R. The Effect of Ship Shape and Anemometer Location on Wind Speed Measurements Obtained from Ships. Available online: http://eprints.soton.ac.uk/23778/1/marinecfd-moat.pdf (accessed on 30 September 2019).
67. Chakraborty, B.; Lam, K. Sunken Duck Boat raised from Missouri Lake Days after 17 People Killed. 23 July 2018. Available online: https://www.foxnews.com/us/sunken-duck-boat-raised-from-missouri-lake-days-after-17-people-killed (accessed on 30 September 2019).
68. Marine Accident Investigation Branch (MAIB)–Safety Digest 02/1997. Available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/373821/SD_2_1997.pdf (accessed on 19 April 2019).
69. Santamarta, R. *SATCOM Terminals: Hacking by Air, Sea, and Land*; Technical White Paper; IOActive Security Services: Seattle, WA, USA, 2014; Available online: https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf (accessed on 30 September 2019).
70. IMO. International Maritime Organization. Radio Communications and Search and Rescue. Available online: http://www.imo.org/en/OurWork/Safety/RadioCommunicationsAndSearchAndRescue/Radiocommunications/Pages/Introduction-history.aspx (accessed on 30 September 2019).
71. Coles, F. Transas Calls for Regulatory Compliance for Big Data Connectivity. 19 October 2016. Available online: https://www.transas.com/transas-calls-for-regulatory-compliance-for-big-data-connectivity (accessed on 30 September 2019).
72. The Maritime Safety Committee. Performance Standards for a Ship Security Alert System, Resolution MSC.136 (76). December 2002. Available online: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Guidance/Documents/MSC.136 (accessed on 30 September 2019).
73. Wee, V. Naval Dome Warns of Continuing Threat from Cosco Cyber Attack. 27 July 2018. Available online: http://www.seatrade-maritime.com/news/americas/naval-dome-warns-of-continuing-threat-from-cosco-cyber-attack.html (accessed on 30 September 2019).
74. Voyage Data Recorders. Available online: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/VDR.aspx (accessed on 30 September 2019).
75. VDR & SDR: A Practical Guide to Marine Voyage Data Recorders for Newbuilds and Retrofits, Northrop Grumman. 2007. Available online: http://www.major-emergency-management.com/services_pdf/VDR_S-VDRGuide.pdf (accessed on 30 September 2019).
76. Hand, M. VDR Located and Recovered from the Stellar Daisy. 19 February 2019. Available online: http://www.seatrade-maritime.com/news/asia/29341.html (accessed on 30 September 2019).
77. Hand, M. VDR from the Sunken El Faro Located. 27 April 2016. Available online: http://www.seatrade-maritime.com/news/americas/vdr-from-the-sunken-el-faro-located.html?highlight=IlZEUiI (accessed on 30 September 2019).
78. Kovacs, E. Ship Data Recorders Vulnerable to Hacker Attacks. *Security Week–Internet and Enterprise Security News, Insights & Analysis*. 11 December 2015. Available online: http://www.securityweek.com/ship-data-recorders-vulnerable-hacker-attacks (accessed on 30 September 2019).

79. Marine Accident Investigation Branch Report, Electrical Failure and Loss of Starboard Engines on Ro-Ro Passenger Ferry European Endeavour Resulting in Contact with Linkspan. 29 August 2008. Available online: https://www.gov.uk/maib-reports/loss-of-power-and-starboard-main-engines-on-ro-ro-passenger-ferry-european-endeavour-resulting-in-contact-with-linkspan-at-calais-france (accessed on 30 September 2019).
80. CVE–Common Vulnerabilities and Exposures. Available online: https://cve.mitre.org (accessed on 30 September 2019).